CSIS POLICY: CONDUCT OF OPERATIONS

Secret

Effective Date: 2014-01-10	**Approved by:** DDO	**French version**
Policy Centre: DDO Sec	**Supported by:** Chief, DDO Sec	
Version No: 1	**File No:** 305-3	
Replaces: OPS-201 and OPS-801		

1. INTRODUCTION

Objective

1.1 The objective of this policy is to ensure the Service achieves its mission by conducting operations in a manner consistent with the Service's Policy Framework and the additional principles outlined in this policy.

Scope

1.2 This policy describes the Service's stance regarding operations conducted pursuant to its national security mandate pursuant to ss.12, 15 and 16 of the *Canadian Security Intelligence Service Act* (*CSIS Act*). It also provides additional principles and requirements that the Service and its employees will adhere to while working to achieve the commitments outlined in this policy.

Policy Centre

1.3 The Deputy Director of Operations (DDO) Secretariat is the policy centre for all matters related to the conduct of operations such as the use of operational tools and techniques, the application for and execution of warrant powers, and related policy documents.

Definitions

1.4 For definitions of specific terms used in this policy, readers should refer to the Policy Glossary.

Guidance and Information

1.5 Additional guidance and information (*e.g.* templates, forms, guides *etc.*) required to carry out this policy can be found on the DDO Secretariat's website. Links to procedures related to the use of specific operational tools and techniques to support operations can be found in the

2. PRINCIPLES

2.1 The Government and the people of Canada expect a high level of performance by the Service in its discharge of responsibilities under the *CSIS Act*. It is also expected that the Service will perform its duties and functions with due regard for the rule of law and respect for the rights and liberties as guaranteed under the *Charter of Rights and Freedoms*. Consequently, CSIS operations will be governed by the Service's Policy Framework, meaning that they will be **lawful** and **authorized**, **necessary**, **proportionate** and will represent an **effective** and **efficient** use of public resources.

Lawful and Authorized

2.2 All CSIS Operations will comply with Canadian law and will be conducted pursuant to the Service's national security mandate as defined in ss.12, 15 and 16 of the *CSIS Act*.

2.3 Prior to conducting an operation, CSIS employees will obtain the appropriate approvals and for s.12 of the *CSIS Act* investigations, ensure that the appropriate targeting authority is in effect.

2.4 When there is uncertainty concerning the lawfulness of an operation, technique or action, employees are expected to consult with their supervisor for direction. Supervisors, in turn, may consult with their managers.

Necessary

2.5 The Service will conduct operations as necessary to fulfill its national security mandate and Government of Canada intelligence requirements pursuant to ss. 12, 15, and 16 of the *CSIS Act*. The collection of information and intelligence will be limited to that which is necessary for the purpose at hand, and is carried out only through such techniques as are necessary in the circumstances. The privacy of individuals will not be infringed unless there are valid reasons to do so, and then only to the extent that is necessary.

Proportionate

2.6 The Service's use of operational tools and techniques will be proportionate to the gravity and imminence of the threat being investigated. Additionally, the greater the risk associated with a particular activity, the higher the authority required to approve the activity.

Effective and Efficient Use of Public Resources

2.7 The Service will evaluate its operations to ensure that they are effective and that the resources dedicated to them are being used as efficiently as possible.

Safety of Employees and Public is Paramount

2.8 The Service will ensure during the planning and conduct of operations that potential risks to employees and/or members of the public are identified and mitigated to the extent possible.

Enhancing Future Capability

2.9 The Service will establish a mechanism to learn from our operational experiences to increase the efficiency of future operations. Service employees will be encouraged and expected to submit suggestions for improving operational tools.

Need to Know

2.10 Service employees will adhere to the "need-to-know" principle and mitigate the risk of unauthorized disclosure or compromise of classified information and assets.

3. USE OF OPERATIONAL TOOLS AND TECHNIQUES

3.1 The operational tools and techniques available to the Service vary greatly and their use will depend on the nature of the potential threat. In general, the Service will use the least intrusive techniques first, except in emergency situations or where less intrusive investigative techniques would not be proportionate to the gravity and imminence of the threat, or if it appears they are unlikely to succeed.

3.1.1 The use of certain operational tools and techniques to support an operation conducted pursuant to s.12 of the *CSIS Act* will require a valid targeting authority. A list of operational tools and techniques and the targeting authority required for their use can be found in CSIS Procedures: Targeting.

3.2 The Service will establish procedures and approval authorities for requesting the use of operational tools and techniques. The level of authority required for approving the use of operational tools and techniques will be commensurate with their intrusiveness and with any risks associated to using them.

3.4 the Director will notify the Minister when there is a potential that a CSIS activity may have significant adverse impact on Canadian interests, such as:

a) discrediting the Service or the GoC;

b) giving rise to public controversy;

c) a clear risk to human life;

d) affecting domestic interdepartmental or intergovernmental relations;

e) affecting Canadian relations with any country or international organization of states; and/or

f) contravening any of the directives with respect to the management of the Service in existing Ministerial Direction or a policy.

Execution of Warrant Powers

3.6 The execution of warrant powers is considered an operational tool that the Service may use to further an investigation into a threat to the security of Canada, to perform its duties and functions under s.16 of the *CSIS Act*,

3.7 When executing warrant powers the Service will comply with the terms and conditions contained in the warrant and with any additional direction issued by the Federal Court and/or the Minister of Public Safety.

3.8 The Service recognizes that there is a heightened risk or potential for controversy given the intrusiveness of some warrant powers. To minimize this risk, the decision to execute warrant powers will be based on the principles outlined in this policy and will be made following established procedures.

Warrant Acquisition and Coordination

3.9 Service employees will employ rigour while engaging in the warrant or production order acquisition process to ensure accuracy and completeness, and that sources of information are not inadvertently disclosed in the application for a warrant.

3.10 The Warrant Acquisition, Control and Requirements (WACR) unit of the DDO Secretariat will be responsible for the overall coordination of Service's Federal Court warrant applications. To reflect the importance of warrants in regards to furthering investigations, WACR will develop and continually review warrant acquisition best practices and procedures to ensure effectiveness and efficiency. The unit will ensure that required documentation in support of the application is prepared and reviewed prior to filing the warrant application with the Court.

Warrant Committees

3.11 The Warrant Review Committee (WRC), chaired by the Director, will be responsible for ensuring that the application for a warrant is both necessary and proportionate and that if the warrant is granted, its execution would constitute an effective and efficient use of the Service's resources.

3.12 The DDO Review Committee, chaired by the Chief, DDO Secretariat, will be responsible for reviewing the affidavit and exhibits
to ensure the documents are consistent with Ministerial Direction, Service standards, and the principles outlined in this policy before the warrant application is filed.

Pretexts

3.13 While in certain circumstances, parallel investigations might be necessary (for example investigations mandated in accordance with ss. 12, 15, or 16 of the *CSIS Act*), operations conducted to support an investigation under one section of the *CSIS Act* will not be used as a *pretext* for conducting operations pursuant to another section of the *Act*.

Use of information collected pursuant to s.15 of the *CSIS Act*

3.14 The Service may use information, collected pursuant to s.15 of the *CSIS Act,* to the extent that it is necessary to support specific investigations pursuant to s.12 of the *CSIS Act*.

4. COOPERATION WITH CANADIAN AND FOREIGN AGENCIES

4.1

To facilitate this cooperation, the Service may enter into arrangements with Canadian and foreign partners in accordance with s.17 of the *CSIS Act,* Ministerial Direction and the principles outlined in this policy.

4.1.1 In emergency circumstances where no s.17 of the *CSIS Act* arrangement exists, the Service may undertake whatever exchanges or cooperation as are necessary. In these cases, the Service will advise the Deputy Minister of Public Safety as soon as possible.

Joint Operations

4.2 The Service considers a joint operation to be an activity that seeks to advance an investigation of mutual interest to the participants by combining resources and sharing the product.

Operational Assistance

4.8 The Service considers Operational Assistance as an activity undertaken by the Service on behalf of a requesting organization, or vice versa,

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Foreign Operational Activity

4.14 In addition to complying with the principles outlined in this policy, CSIS operational activities conducted outside Canada will:

a) hold potential benefit for Canada and its national interests;

b) be considered for their impact on Canadian foreign policy interests and objectives; and

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

5. INDIVIDUALS AND ORGANIZATIONS DEEMED OF SPECIAL CONSIDERATION

5.1 The Service will weigh the need to use intrusive operational tools and techniques against potential damage to civil liberties or the activities of a Canadian Fundamental Institution (CFI). CFIs include, but are not limited to, post-secondary, political, religious and media institutions.

6. EMPLOYEE CONDUCT

6.1 CSIS Employees are expected to conduct themselves in a manner consistent with the Service's Code of Conduct and the following standards during the performance of their duties:

a) their actions will be impartial and in compliance with the *CSIS Act* and established CSIS procedures;

b) their deportment will be professional, courteous and respectful when dealing with the public;

c) they will be discreet, apply the need-to-know principle, and abide by established standards of security during the performance of their duties and functions so that sensitive sources of information, collection programs and operational methodologies are not compromised;

d) they will report in a timely, accurate, complete and objective manner all information pertinent to a collection program;

e) they will clearly distinguish between fact, analysis, and opinion in their reports; and

f) they will refrain from offering personal opinions on sensitive issues which could lead to unnecessary confrontation or controversy.

6.2

Unlawful Activity

6.3 When an employee learns of unlawful activity during the performance of his or her duties and functions, he or she will advise his/her supervisor or manager as soon as possible. The employee may also make an internal disclosure in accordance with ADM-406, "Internal Disclosure of Wrongdoing and Reprisal Protection" to the Senior Officer of Disclosure of Wrongdoing.

7. REPORTING AND RETENTION OF OPERATIONAL INFORMATION AND MATERIALS

7.1 All information, intelligence and materials collected during an operation will be reported and retained in accordance with the Service's existing policies and procedures for reporting and retaining operational information and materials.