OPS-100 TARGETING - SECTION 12 *CSIS ACT*

1. INTRODUCTION

Objective

1.1 To state the principles and directives governing the approval process for an initial request, a renewal, an upgrade, a downgrade or a termination of a targeting level pursuant to the *CSIS Act*.

Scope

1.2 This policy and related procedures outline the principles, as well as the organizational and functional responsibilities, pertaining to targeting.

1.3 Procedures for the preparation of an Assessment Report to initiate, renew, modify, or terminate a targeting level are covered in OPS-100-1, "Procedures - Targeting - Assessment Report".

Policy Centre

1.4 The policy centre for this policy is the Targeting and Warrants Section (TWS) of the Deputy Director of Operations (DDO) Secretariat.

Authorities and References

1.5 *CSIS Act*

1.6 *Anti-terrorism Act*

1.7 Ministerial Direction - CSIS Operations (2008 10 29)

1.8 OPS-201, "Conduct of Operations - General"

1.9 OPS-209, "Warrant Acquisition - Section 12"

1.10 OPS-501, "Operational Reporting"

1.11 OPS-601 to OPS-603, "Authorized Disclosure of Operational Information and Intelligence"

Definitions

1.13 For definitions of specific terms used in this policy, readers should refer to OPS - "Glossary of Terms and Definitions".

1.14 For the purpose of targeting policies and procedures, the term "targeting decision" refers to the final determination made by the approving authority of an Assessment Report requesting to initiate, renew, upgrade, downgrade or terminate a targeting level.

Temporary Authority

1.15 Unless otherwise specified, when a specific position or title is mentioned in this policy, the authorities

and responsibilities bestowed on that position or title apply to any employee performing the duties of the position or title in an acting capacity.

2. POLICY STATEMENT

2.1 The Targeting Policy is established under the authority of the Director pursuant to subsection 6(1), *CSIS Act*, and directs the Service's targeting process.

2.2 Further to a Memorandum from Cabinet of national intelligence collection priorities the Minister of Public Safety issues a Ministerial Directive outlining general collection requirements. The DDO then provides a strategic directive to operationalize the Ministerial Directive.

2.3 Targeting will be governed by the following fundamental principles:

a) the rule of law must be observed;

b) the means must be proportional to the gravity and imminence of the threat;

c) the greater the risk associated with a particular activity, the higher the authority required for approval; and

d) with regard to the use of intrusive techniques:

i) the need for their use must be weighed against possible damage to civil liberties and to Canadian fundamental institutions, such as political, religious, post-secondary and media establishments;

ii) the least intrusive techniques must be used first, except in emergency situations or where less intrusive techniques would not be proportionate to the gravity and imminence of the threat; and

iii) the level of authority required for approving their use must be commensurate with their intrusiveness and with any risks associated to using them.

2.4 Lawful advocacy, protest or dissent may not be investigated unless such activities are carried out in conjunction with threats as defined in section 2, *CSIS Act*.

2.5 When there is uncertainty concerning the lawfulness of an operation, technique or action, the issue must be referred to the appropriate Director General (DG) for direction.

2.6 When approving an Assessment Report, a Headquarters (HQ) DG or Regional Director General (RDG) must consider the intrusiveness of each technique allowed under the approved targeting level and may impose special restrictions if deemed appropriate considering the gravity and imminence of the threat.

2.7 Recognizing that special considerations should be given when dealing with underage persons, all Assessment Reports concerning an individual under the age of eighteen (18) will be sent to the DDO for approval.

3. RESPONSIBILITIES

Directors General

3.1 An HQ DG or RDG is responsible for:

a) approving a targeting decision with the exception of the targeting of an underage person;

b) ensuring targeting decisions are consistent with the Service's mandate and policies, and current Government of Canada (GoC) intelligence requirements;

c) ensuring that consultation between Regions and the appropriate HQ Branch(es) has taken place on all targeting decisions;

d) assessing the intrusiveness of the techniques to be used to collect information and intelligence;

e) assessing the reliability of the information in an Assessment Report;

f) assessing the implications, magnitude, seriousness and immediacy of the activities suspected of constituting the threat; and

g) appointing a Targeting Coordinator.

Chief, Deputy Director Operations Secretariat

3.2 The Chief DDO Secretariat is responsible for:

a) providing the DDO, Assistant Director Operations (ADO), and the Assistant Director Legal Services, within five (5) working days from the date of approval, written confirmation of all targeting decisions pursuant to this policy;

d) providing advice and guidance to the Targeting Coordinators in HQ and the Regions to ensure the consistent application of the targeting policy;

f) maintaining statistical information and producing, on request, accounts of targeting decisions;

h) performing other administrative functions as directed by the DDO.

Deputy Director Operations

3.4 The DDO is responsible for:

a) managing the application of this policy and providing direction to resolve issues arising from its implementation; and

b) ensuring that targeting decisions are consistent with the Service's mandate and policies, and current GoC intelligence requirements.

Director

3.5 Only the Director can approve targeting pursuant to subsection 2(d), *CSIS Act*.

3.6 The Director is responsible for reporting to the Minister of Public Safety where:

a) there is a well-founded risk of serious violence;

b) there is a potential that a CSIS activity may have significant adverse impact on Canadian interests, such as:

i) discrediting the Service or the Government of Canada;

ii) giving rise to public controversy;

iii) a clear risk to human life;

iv) affecting domestic interdepartmental or intergovernmental relations;

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

vi) contravening any of the guidelines set out in the Ministerial Direction on CSIS Operations with respect to the management of the Service.

4. TARGETS OF THE SERVICE

4.1 Information from a foreign state or agency may be used when submitting an Assessment Report, taking into consideration the human rights record of that foreign state or agency and the specific circumstances under which the information was obtained.

Persons

4.2 A targeting level may be approved by an RDG or an HQ DG to collect information and intelligence on the activities of persons who may on reasonable grounds be suspected of constituting a threat to the security of Canada pursuant to s. 2, *CSIS Act*.

Groups and Organizations

4.3 A targeting level may be approved by an HQ DG to collect information and intelligence on the activities of a group of persons or an organization, including its general membership, where there are reasonable grounds to suspect:

a) the objectives or activities of the group or organization constitute a threat to the security of Canada pursuant to s. 2, *CSIS Act*; and

b) participants in the group or organization understand and sympathize with threat-related objectives or activities.

4.3.1 Collection of information and intelligence on a group of persons or an organization may be used to determine:

Issues or Events

4.5 A targeting level may be approved to collect information and intelligence on the activities associated with an issue or event in relation to which the Service has reasonable grounds to suspect these activities constitute a threat to the security of Canada.

5. GENERAL AUTHORITY

5.1 The following activities do not require a targeting level and are exempt from this policy:

a) collecting incidental information which may be disclosed pursuant to subsection 19.2(a) to (d), *CSIS Act*;

b) collecting information pursuant to s. 15 and s. 16, *CSIS Act*;

d) conducting investigations in support of the execution of a warrant pursuant to s. 21 and s. 23, *CSIS Act*. Refer to OPS-210, "Execution of Warrant Powers and Non-warranted Special Operations";

e) conducting internal investigations pursuant to s. 8 and s. 20, *CSIS Act*;

f) researching and using internal records and databanks;

g) researching and using open information;

h) accepting and reporting unsolicited information; and

5.1.1 Employees reporting unsolicited information are responsible for ensuring the information is reported on the appropriate file and retained in the appropriate database. It is also the employees' responsibility to assess the origin and reliability of the information and the need to report it if the information originates from a foreign organization with a poor human rights record (see OPS-501 "Operational Reporting").

6. USE OF HUMAN SOURCES

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

8. COOPERATION WITH DOMESTIC OR FOREIGN AGENCIES

8.1 Collection of information and intelligence by the Service pursuant to s.12, *CSIS Act*, in cooperation with a Canadian federal, provincial or a territorial government department, a Canadian law enforcement authority, or a foreign police, security or intelligence organization, will only be undertaken when approved under the terms of this policy.

8.1.1 The collection of information and intelligence described above will be in compliance with all other Service policies.

Top

2010-10-04

SECRET