AS

Court file No. DES-7-08

UNCLASSIFIED

Re: Mohamed MAHJOUB

OPS - 211 PROCESSING OF INFORMATION COLLECTED UNDER WARRANT (1998-2006) (REDACTED)

Prepared by the Canadian Security Intelligence Service for the Minister of Public Safety and Emergency Preparedness and the Minister of Citizenship and Immigration

February 5, 2010

Court file No. DES-7-08

UNCLASSIFIED

Re: Mohamed MAHJOUB

OPS - 211 PROCESSING OF INFORMATION COLLECTED UNDER WARRANT (1998-2006) (REDACTED)

Prepared by the Canadian Security Intelligence Service for the Minister of Public Safety and Emergency Preparedness and the Minister of Citizenship and Immigration

February 5, 2010

INDEX

TAB(S)

OPERATIONAL POLICY MANUAL

OPS-211 PROCESSING OF INFORMATION COLLECTED UNDER WARRANT

1. INTRODUCTION

Policy Objective

1.1 A Federal Court Warrant issued under Part II of the CSIS Act, empowers the Service to collect information through the interception of private communications.

1.1.1 It is incumbent on the Service to comply with the terms and conditions of the warrant; with restrictions and controls imposed by the Minister; and to account for its actions in that regard.

Scope

1.2 This policy establishes guidelines for the processing and disclosure of information obtained through the interception of private communication pursuant to a section 12 of the CSIS Act investigation, as authorized by a Federal Court Warrant.

Authorities

1.3 CSIS Act

1.4 Ministerial Direction on: Tape Retention (April 10, 1991)

1.5 CSIS - RCMP Memorandum of Understanding.

2. PRINCIPLES

Risks

2.1 Section 12 of the CSIS Act permits the Service to collect information and intelligence to the extent that it relates to activities that may on reasonable grounds be suspected of constituting threats to the security of Canada.

2.2 Part II of the CSIS Act enables the Service to make an application to obtain a warrant for the purpose of intercepting private communications when it believes, on reasonable grounds, that the warrant is required to enable the investigation of a threat to the security of Canada.

2.3 The interception of private communications is one of the most intrusive investigative techniques utilized by the Service therefore it is incumbent upon the Service to ensure communication intercept practices impair individual privacy as little as possible.

2.4 Employees involved in processing information and intelligence collected under the authority of Section 21 must comply with the terms and conditions of the Federal Court Warrant as well as any other

restrictions or conditions imposed by the Solicitor General.

2.5 Third party intercepts must be destroyed or erased at the earliest practical opportunity.

2.6 Intercepted communications must be processed as soon as possible and practical, with due regard to the nature of the particular investigation and threat.

2.7 Intelligence relating to the investigation of threats to the security of Canada may be retained in original recording, verbatim transcripts or summary format, depending on investigative necessity or practical circumstances.

2.8 Intercepted material shall be kept for a minimum of ten (10) working days but no longer than thirty (30) working days after processing.

2.9 Intercepted communications may be retained for more than 30 days after processing only when it is deemed necessary to the conduct of an investigation.

2.9.1 [redacted] or person designated must approve the request to retain communications intercepts processed within the [redacted] Unit.

2.9.2 [redacted] must approve the request to retain communication intercepts obtained by other means. (see Section 4.)

3. FUNCTIONAL RESPONSIBILITIES

Director General, Operations Support Branch

3.1 The Director General, Operations Support Branch (OS) is responsible for the policy direction and coordination of Service programs for warrant acquisition and control, [redacted] multilingual translation, [redacted] and communications intelligence production.

Regional Directors General

3.2 Regional Directors General are responsible for effecting communication interceptions within the Region in compliance with the Federal Court warrant, Ministerial Direction and Service policy.

OPERATIONAL POLICY MANUAL

[redacted]

3.5 The [redacted] conducts compliance and quality control audits of [redacted] Sections, and coordinates in-house [redacted] training courses.

[redacted]

4. SPECIAL CIRCUMSTANCES

Warrant

4.1 A Federal Court warrant may empower the Service to conduct non- electronic communications intercepts, [redacted] obtain records [redacted] as well as electronic communication intercepts. [redacted]

[redacted]

Intercepts

OPERATIONAL POLICY MANUAL

4.3 A non-electronic communication intercept is normally coordinated by the [redacted] in concert with the operational responsibility centre, [redacted] and the Regional Warrant Coordinator.

General Principles

4.4 Material collected in these special circumstances is subject to the general principles and retention standards of this policy.

NOTE: The method of processing will depend on the type of communication intercepted.

4.5 Regional Warrant Coordinators are responsible for monitoring the execution of powers involving special circumstance communication intercepts, and maintaining the necessary records to ensure compliance with the established guidelines.

5. INTERCEPTIONS INVOLVING A SOLICITOR, OR A SOLICITOR'S EMPLOYEE AT A SOLICITOR'S OFFICE (hereafter referred to as "solicitor")

5.1 The Federal Court, when authorizing warrants, specifies conditions the Service is obligated to follow when faced with an intercepted communication involving a solicitor.

[redacted]

5.2 Where a party to an intercepted communication is a solicitor, [redacted] shall make an initial determination as to whether the communication relates to a threat to the security of Canada.

5.2.1 Where the communication is deemed not related to a threat, it shall be destroyed or erased at the earliest practical opportunity; and,

5.2.2 Where the [redacted] believes the communication may relate to a threat, the communication shall be forwarded to the Regional Director General.

Restricted

5.3 An intercepted communication involving a solicitor requiring a determination by the Regional Director General, shall remain in its original format, or in a translated summary version without wider distribution.

5.3.1 A Solicitor Communication form [redacted] must accompany the communication requiring the determination.

Regional Director General

OPERATIONAL POLICY MANUAL

5.4 The Regional Director General must review the communication and decide if it relates to a threat and shall be retained.

Records

5.5. A designated person in each Region shall be responsible for maintaining a record of the disposition of all Solicitor communications where the Regional Director General has made a determination.

6. INCIDENTAL (SPIN OFF) INFORMATION

6.1 Under subsection 19(2) of the CSIS Act, the Service may retain, for the purpose of disclosure, information which:

-- may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province;

-- relates to the conduct of the international affairs of Canada;

-- relates to the defense of Canada; or

-- relates to the public interest as determined by the Solicitor General.

6.2 Incidental information retained under subsection 19(2) of the CSIS Act shall be reported to the appropriate operational branch.

6.3 Refer to OPS-601 to OPS-603, Disclosure of Operational Information and Intelligence, for policy governing the disclosure of information retained under subsection 19(2) of the CSIS Act.

7. ASSISTANCE TO THE RCMP

7.1 Assistance and cooperation with the RCMP is governed by a MOU between the Service and the RCMP and is reflected in OPS-601 to OPS-603, "Disclosure of Operational Information and Intelligence".

7.2 Through the Liaison Officer program, the RCMP has access to all CSIS information, except:

-- information provided to the Service which prohibits disclosure to a third party; and,

-- information that identifies a source.

OPERATIONAL POLICY MANUAL

Access to Communications Intercepts

7.3 The RCMP may, based on information disclosed to them by the Service, request access to the relevant communications intercept to ascertain if there may be further material which could relate to a criminal investigation.

7.3.1 The RCMP has ten working days, after the intercepted communication has been processed, to request further access to the interception to identify intelligence which may be suitable for investigative leads. After this time the intercepted material may be destroyed.

7.3.2 Intercepted communications shared with the RCMP must be destroyed after thirty (30) working days.

7.3.3 Should the RCMP request an extension of the retention period, the Regional or Branch DG may agree to a further extension.

7.3.4 A record must be maintained of all intercepted communications shared with the RCMP.

Serious Crime

7.4 In exceptional circumstances where the RCMP, when performing their duties under the Security Offences Act, are unable to obtain their own independent evidence, they may request access to communications intercepts held by the Service.

7.4.1 The following criteria, established in the Memorandum of Understanding (MOU) between the Service and the RCMP, shall be used to assess what are exceptional circumstances:

-- the seriousness of the crime;

-- the importance and uniqueness of the information; and,

-- the potential effects of disclosure on CSIS sources of information, methods of operation and third-party relations.

7.5 When requested by the RCMP to retain information that meets the above criteria, [redacted] or person designated must ensure an accurate copy of the communication is made.

7.5.1 Requests to retain intercepted communications collected under circumstances as described in Section 4, Special Circumstances, must be brought to the attention of the Deputy Director, Operations (DDO), for a decision.

7.6 For possible use in future judicial proceedings, the [redacted] or person designated must verify the accuracy of the copy, when possible, against the original communications intercept and must identify the copy by target name, date and time of the interception as well as the time and date the copy

OPERATIONAL POLICY MANUAL

was made.

7.6.1 The copy and any accompanying translated summary must be stored in a place where access is limited to the [redacted] or person designated (ie: a cabinet rated for storing Top Secret material).

7.7 Where the RCMP intend to present the communications intercept as evidence, the recording must be retained by the Service for a time mutually agreed upon by the Service and the RCMP.

7.8 Where the communications intercept information relates to serious criminal activity, unrelated to a threat to the security of Canada, the same procedures as 7.6 shall apply; however, the recipient of the information will be the police of jurisdiction.

7.8.1 The communication will only be retained until its potential use has been decided upon in consultation with officials of the Office of the Attorney General of Canada.

[redacted]

OPERATIONAL POLICY MANUAL

[redacted]

OPERATIONAL POLICY MANUAL

[redacted]

~~2004-09-01~~
OPS-211 PROCESSING OF MATERIALS OR COMMUNICATION INTERCEPTS COLLECTED UNDER WARRANT - SECTION 12

1. INTRODUCTION

Objective

1.1 To manage the processing of materials or communication intercepts collected under warrants issued pursuant to sections 12, 21 and 22, *CSIS Act*.

Scope

1.2 To provide direction on the analysis, reporting, retention or destruction of materials or communication intercepts.

Authorities and References

1.3 *CSIS Act*

1.4 *Security Offences Act*

1.5 Memoranda of Understanding (MOU):

i) CSIS-REVENUE CANADA, (Taxation) (August 1987) Canada Revenue Agency (formerly Revenue Canada)

ii) CSIS - RCMP, (April 1990)

iii) CSIS-CSE Section 12 Operations, (November 1990)

1.6 OPS-211-1, "Procedures - Processing of Solicitor - Client Materials or Communication Intercepts"

1.7 OPS-211-2, "Procedures - Processing / Retention / Disposition of Materials Collected Under Warrant - Section 12"

1.8 OPS-211-3, "Procedures - Transfer / Retention / Disposition of Communication Intercepts - Section 12"

1.9 OPS-211-4, "Procedures - Incidentally Collected Communication Intercepts - Section 12"

1.10 OPS-211-5, "Procedures - Security Offences and Criminal Offences - Section 12"

1.11 OPS-501, "Operational Reporting"

1.12 OPS-601, "Authorized Disclosure of Operational Information or Intelligence - General"

1.13 OPS-602, "Disclosure of Security Information or Intelligence"

1.14 OPS-603, "Disclosure of Operational Information or Intelligence - Caveats"

1.15 SEC-402, "Physical Safeguarding of Information"

[redacted]

Definitions

1.18 **Communication intercept:** Oral or telecommunication intercepts processed by [redacted]

1.19 **Incidentally collected information:** Any communication intercept of a person other than the target obtained pursuant to a warrant.

1.20 **Information:** Materials, communication intercepts or data from any source which has not been analysed but may produce intelligence, once processed.

1.21 **Long Term Retention (LTR):** The retention of materials or communication intercept(s) after the expiration date of the warrant, for security and intelligence purposes consistent with the "strictly necessary" requirement.

1.22 **Materials:** Items [redacted] collected by [redacted] Regional Warrant Coordinator (RWC) or [redacted]

1.23 **Need-to-know:** The principle whereby employees/consultants/contractors are provided with access to classified or designated information to properly carry out their current duties or responsibilities. Employees/consultants/contractors must be satisfied of their legitimate need-to-know before seeking access to classified or designated information. Before providing another person with access to classified or designated information, employees/consultants/contractors must be satisfied of that person's legitimate need-to-know. (SEC-402, "Physical Safeguarding of Information")

1.24 **Processing:** Method by which materials or communication intercepts are analysed to determine if they are to be reported, retained and/or destroyed.

1.25 **Retention:** The holding or storage of materials, communication intercepts or data from any source, more than 30 days up to the expiration date of the warrant.

1.26 **Solicitor-client information / communication:** Any materials or communication intercepts of a confidential nature, between a client and a solicitor or any person employed in a solicitor's office, directly related to the seeking, formulating or giving of legal advice or assistance.

2. RESPONSIBILITIES

Deputy Director Operations

2.1 The Deputy Director Operations (DDO) will issue policy to ensure compliance with the terms

and conditions of the warrant and Ministerial Direction.

2.2 The DDO or designate will:

i) approve the further retention of materials or communication intercepts collected under a warrant which has expired and has not been renewed; and

ii) identify investigations and/or warrants wherein Long Term Retention (LTR) will be used.

Director General, Operations Support

2.3 **The Director General, Operations Support (DG OS), issues procedures for the processing of materials or communication intercepts obtained under the authority of a warrant.**

2.4 [redacted] **is responsible** for:

i) **reviewing the handling of materials or communication intercepts obtained under warrant;**

ii) **reviewing compliance with the terms and conditions of the warrant, Ministerial Direction and Service policies; and**

iii) **advising Regional Directors General (RDG) regarding best practices and the management of material or communication intercepts collected under warrant.**

Directors General

2.5 Directors General (DGs) or designate are responsible for:

i) ensuring materials or communication intercepts collected pursuant to a warrant are processed in compliance with the terms and conditions of the warrant, Ministerial Direction and Service policy;

ii) ensuring employees responsible for processing materials or communication intercepts have read the warrant, the affidavit and the letter of instruction from th[redacted]

iii) determining the disposition of solicitor-client materials or communication intercepts;

iv) reviewing incidentally collected information;

v) determining the disposition of materials or communication intercepts in relation to the *Security Offences Act* and criminal offences;

vi) approving the retention of materials or communication intercepts when held for more than 30 calendar days after processing;

vii) approving the retention of unprocessed materials when held for more than 90 calendar

days:

[redacted]

ix) designating [redacted] and

x) ensuring that compliance and quality control reviews are performed.

[redacted]

2.6 The [redacted] is responsible for performing compliance and quality control reviews [redacted] within 90 calendar days of executing the powers of a warrant to confirm:

i) employees have read the warrant and understood the terms and conditions imposed by the warrant;

ii) written tasking and priorities were provided to employees within 30 calendar days of executing the powers of the warrant;

iii) materials or communication intercepts are being processed within policy time frames;

iv) operational reports conform with the terms and conditions of the warrant, written tasking and priorities, and Service policy; and

v) compliance with the terms and conditions of the warrant, Ministerial Direction, and Service policy and procedures.

2.6.1 The [redacted] will report findings of the compliance and quality control review to the RDG or designate.

Regional Warrant Coordinator

2.7 The Regional Warrant Coordinator (RWC) is responsible for:

i) maintaining information on powers and conditions for all warrants including approval designations [redacted]

ii) tracking and recording of powers executed, including:

a) materials collected, processed, retained or disposed/transmitted (OPS-211-2, "Procedures - Processing / Retention / Disposition of Materials Collected Under Warrant - Section 12") [redacted]

b) communication intercepts collected, retained or disposed/transmitted (OPS-211-3, "Procedures - Transfer / Retention / Disposition of Communication Intercepts - Section 12") [redacted]

[redacted]

[redacted]

3. PROCEDURES

3.1 Procedures concerning solicitor-client materials or communication intercepts are located in OPS-211-1 "Procedures - Processing of Solicitor-Client Materials or Communication Intercepts".

3.2 Procedures concerning materials collected pursuant to a warrant are located in OPS-211-2, "Procedures - Processing / Retention / Disposition of Materials Collected Under Warrant - Section 12".

3.3 Procedures concerning communication intercepts collected pursuant to a warrant are located in OPS-211-3, "Procedures - Retention / Disposition of Communication Intercepts - Section 12".

3.4 Procedures concerning incidentally collected communication intercepts are located in OPS-211-4, "Procedures - Incidentally Collected Communication Intercepts - Section 12".

3.5 Procedures concerning security or criminal offences are located in OPS-211-5, "Procedures - Security Offences and Criminal Offences - Section 12".

2006-05-01

OPS-211 PROCESSING OF MATERIALS OR COMMUNICATION INTERCEPTS COLLECTED UNDER WARRANT - SECTION 12

1. INTRODUCTION

Objective

1.1 To manage the processing of materials or communication intercepts collected under warrants issued pursuant to sections 12, 21 and 22, *CSIS Act*.

Scope

1.2 To provide direction on the analysis, reporting, retention or destruction of materials or communication intercepts.

Authorities and References

1.3 *CSIS Act*

1.4 *Security Offences Act*

1.5 Memoranda of Understanding (MOU):

i) CSIS-REVENUE CANADA, (Taxation) (August 1987) Canada Revenue Agency (formerly Revenue Canada)

ii) CSIS - RCMP, (April 1990)

iii) CSIS-CSE Section 12 Operations, (November 1990)

1.6 OPS-211-1, "Procedures - Processing of Solicitor - Client Information / Communication"

1.7 OPS-211-2, "Procedures - Processing / Retention / Disposition of Materials Collected Under Warrant - Section 12"

1.8 OPS-211-3, "Procedures - Transfer / Retention / Disposition of Communication Intercepts - Section 12"

1.9 OPS-211-4, "Procedures - Incidentally Collected Communication Intercepts - Section 12"

1.10 OPS-211-5, "Procedures - Security Offences and Criminal Offences - Section 12"

1.11 OPS-501, "Operational Reporting"

1.12 OPS-601, "Authorized Disclosure of Operational Information and Intelligence - General"

1.13 OPS-602, "Disclosure of Security Information or Intelligence"

1.14 OPS-603, "Disclosure of Operational Information or Intelligence - Caveats"

1.15 SEC-402, "Physical Safeguarding of Information"

[redacted]

Definitions

1.18 **Communication intercept:** Oral or telecommunication intercepts processed by [redacted]

1.19 **Incidentally collected information:** Any intercepted communications of a person (s) other than the target (s) obtained pursuant to a warrant.

1.20 **Information:** Materials, communication intercepts or data from any source which has not been analysed but may produce intelligence, once processed.

1.21 **Long Term Retention (LTR):** The retention of materials or communication intercept(s) after the expiration date of the warrant, for security and intelligence purposes is consistent with the "strictly necessary" requirement.

1.22 **Materials:** Items [redacted] collected by [redacted] Regional Warrant Coordinator (RWC) or the [redacted]

1.23 **Need-to-know:** The principle whereby employees/consultants/contractors are provided with access to classified or designated information to properly carry out their current duties or responsibilities. Employees/consultants/contractors must be satisfied of their legitimate need-to-know before seeking access to classified or designated information. Before providing another person with access to classified or designated information, employees/consultants/contractors must be satisfied of that person's legitimate need-to-know. (SEC-402, "Physical Safeguarding of Information").

1.24 **Processing:** Method by which materials or communication intercepts are analysed to determine if they are to be reported, retained and/or destroyed.

1.25 **Raw Product:** Unprocessed product in its original state.

1.26 **Retention:** The holding or storage of materials, communication intercepts or data from any source, more than 30 days after processing or up to the expiration date of the warrant.

1.27 **Solicitor-client information/communication:** Any materials or communication intercepts of a confidential nature, between a client and a solicitor or any person employed in a solicitor's office, directly related to the seeking, formulating or giving of legal advice or assistance.

2. RESPONSIBILITIES

Deputy Director Operations

2.1 The Deputy Director Operations (DDO) will issue policy to ensure compliance with the terms

and conditions of the warrant and Ministerial Direction specific to the warrant.

2.2 The DDO or designate will:

i) approve the Long Term Retention (LTR) of materials or communication intercepts collected under a warrant which has expired and has not been renewed; and

ii) identify investigations and/or warrants wherein LTR will be used and advise HQ and Regional Directors Generals (RDGs) with a copy to [redacted]

[redacted]

2.3 The [redacted] or designate is responsible for:

i) issuing procedures for the processing of materials or communication intercepts obtained under the authority of a warrant;

ii) advising RDGs regarding best practices and the management of material or communication intercepts collected under warrant.

iii) reviewing the handling of materials or communication intercepts obtained under warrant; and

iv) reviewing compliance with the terms and conditions of the warrant, Ministerial Direction and Service policies.

Directors General

2.4 Directors General (DGs) or designate are responsible for:

i) ensuring materials or communication intercepts collected pursuant to a warrant are processed in compliance with the terms and conditions of the warrant, Ministerial Direction and Service policy;

ii) ensuring employees responsible for processing materials or communication intercepts have read the warrant, the affidavit and the letter of instruction from the [redacted]

iii) determining the disposition of solicitor-client materials or communication intercepts;

iv) reviewing incidentally collected information;

v) determining the disposition of materials or communication intercepts in relation to the *Security Offences Act* and criminal offences;

vi) approving the retention of materials or communication intercepts when held for more than 30 calendar days after processing;

vii) approving the retention of unprocessed materials collected by [redacted] Regional Warrant Coordinator when held for more than 90 calendar days;

[redacted]

ix) designating a [redacted] and

x) ensuring that compliance and quality control reviews are performed.

[redacted]

2.5 The [redacted] or designate is responsible for performing compliance and quality control reviews [redacted] within 90 calendar days of executing the powers of a warrant to confirm:

i) employees have read the warrant and understood the terms and conditions imposed by the warrant;

ii) written tasking and priorities were provided to employees within 30 calendar days of executing the powers of the warrant;

iii) materials or communication intercepts are being processed within policy time frames;

iv) operational reports conform with the terms and conditions of the warrant, written tasking and priorities, and Service policy; and

v) compliance with the terms and conditions of the warrant, Ministerial Direction, and Service policy and procedures.

2.5.1 The [redacted] will report findings of the compliance and quality control review to the RDG or designate.

Regional Warrant Coordinator

2.6 The Regional Warrant Coordinator (RWC) or designate is responsible for:

i) maintaining information on powers and conditions for all warrants including approval designations [redacted] and

ii) tracking and recording of powers executed, including:

a) materials collected, processed, retained or disposed/transmitted (OPS-211-2, "Procedures - Processing/Retention/Disposition of Materials Collected Under Warrant - Section 12") [redacted] and

b) communication intercepts collected, retained or disposed/transmitted (OPS-211-3, "Procedures - Transfer/Retention/Disposition of Communication Intercepts - Section 12") [redacted]

[redacted]

[redacted]

3. PROCEDURES

3.1 Procedures concerning solicitor-client materials or communication intercepts are located in OPS-211-1 "Procedures - Processing of Solicitor-Client Information / Communication".

3.2 Procedures concerning materials collected pursuant to a warrant are located in OPS-211-2, "Procedures - Processing / Retention / Disposition of Materials Collected Under Warrant - Section 12".

3.3 Procedures concerning communication intercepts collected pursuant to a warrant are located in OPS-211-3, "Procedures - Retention / Disposition of Communication Intercepts - Section 12".

3.4 Procedures concerning incidentally collected communication intercepts are located in OPS-211-4, "Procedures - Incidentally Collected Communication Intercepts - Section 12".

3.5 Procedures concerning security or criminal offences are located in OPS-211-5, "Procedures - Security Offences and Criminal Offences - Section 12".