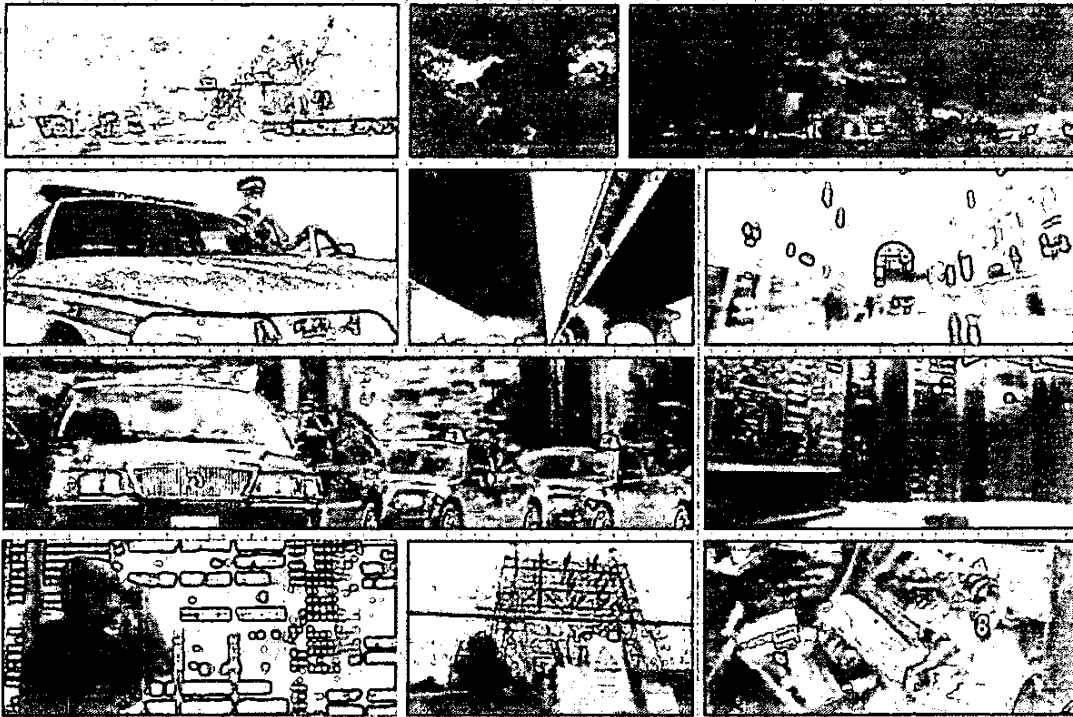




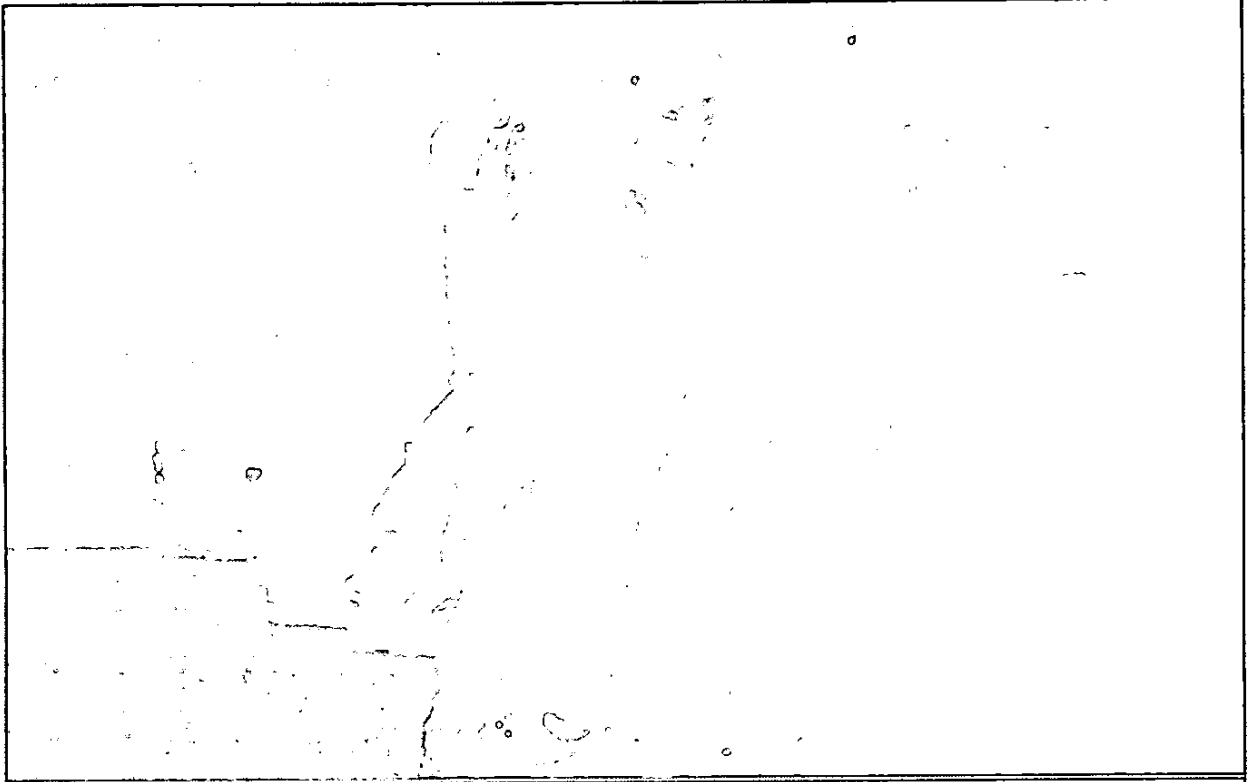
NATIONAL SECURITY  
CRIMINAL INVESTIGATIONS

ORIENTATION GUIDE  
2008

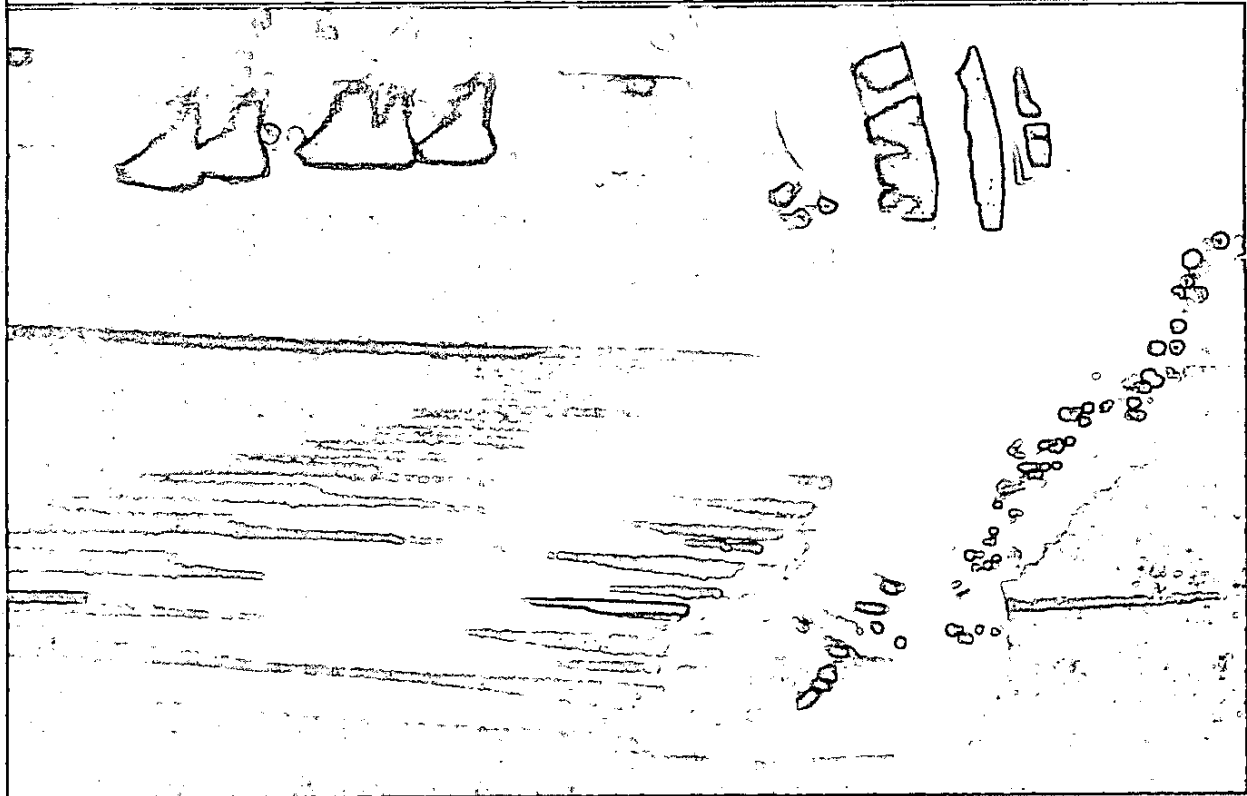


This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.





NATIONAL SECURITY CRIMINAL INVESTIGATIONS



# TABLE OF CONTENTS

**Introduction to the Orientation Guide** ..... 1

**Chapter One — About HQ** ..... 2

    General information about HQ Grounds ..... 3

    Nicholson Building ..... 4

    HQ Building and Map ..... 5

**Chapter Two — National Security Criminal Investigations** ..... 6

    NSCI Structure ..... 7

    NSCOB Structure and Duties ..... 10

    NSCOSB Structure and Duties ..... 14

    NSLAB Structure and Duties ..... 18

    SIPS Structure and Duties ..... 19

**Chapter Three — Integrated National Security Enforcement Teams** ..... 20

    Background ..... 21

    Mandate ..... 21

    INSET Unit Structure ..... 21

**Chapter Four — The Governance Model** ..... 22

    Key elements ..... 23

    Background ..... 23

    Governance structure ..... 24

    Governance Structure details ..... 25

    Human Resources ..... 27

    Defining NS Criminal Investigations ..... 28

**Chapter Five — Departmental Security** ..... 29

**Chapter Six — Document Classification** ..... 30

**National Security Criminal Investigations — Orientation Guide**

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

## TABLE OF CONTENTS

---

<b>Chapter Seven — Information and Intelligence Handling Protocols</b> .....	32
Sharing Information.....	32
General.....	32
<b>Caveats</b> .....	33
Technology.....	34
Requests to RCMP Liaison Officers (LO's).....	34
Briefing Notes.....	34
Security of Information Act.....	34
<b>Chapter Eight — Ministerial Direction on National Security</b> .....	35
Responsibility and Accountability.....	35
Arrangements and Cooperation.....	36
Investigations in Sensitive Sectors.....	37
<b>Chapter Nine — Software, Data Systems and Access</b> .....	38
Records Management System.....	38
General.....	38
Internet.....	39
ROSS.....	39
<b>Chapter Ten — Training</b> .....	40
<b>Chapter Eleven — Official Languages</b> .....	41
<b>Chapter Twelve — Relocation of National HQ</b> .....	42
<b>Chapter Thirteen — Commonly Used Acronyms</b> .....	43
Agencies.....	43
Computer Systems.....	43
RCMP Units.....	44
Miscellaneous Terms.....	44

**National Security Criminal Investigations — Orientation Guide**

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

## INTRODUCTION TO THE NSP ORIENTATION PACKAGE



*Welcome.*

*The purpose of this orientation guide is to provide an initial introduction for new employees — whether they are new to the RCMP, new to Headquarters, new to the National Security Program (NSP), or even all three.*

*As part of your orientation it would be useful to explore the RCMP INFOWEB site, an internal site which contains lots of valuable information. Particularly valuable is the package put together on the Chief Information Officer (CIO) Website for the information of new employees. While some information there is outdated and is specifically geared to new members of that program, it contains links to areas that will be of interest to all new employees of the RCMP — [http://infoweb.rcmp-grc.gc.ca/cio/seclms/learning\\_services/orientation/index\\_e.htm](http://infoweb.rcmp-grc.gc.ca/cio/seclms/learning_services/orientation/index_e.htm)*

*When using the NSP orientation guide please keep in mind that the specifics of your orientation are still the responsibility of your supervisors.*

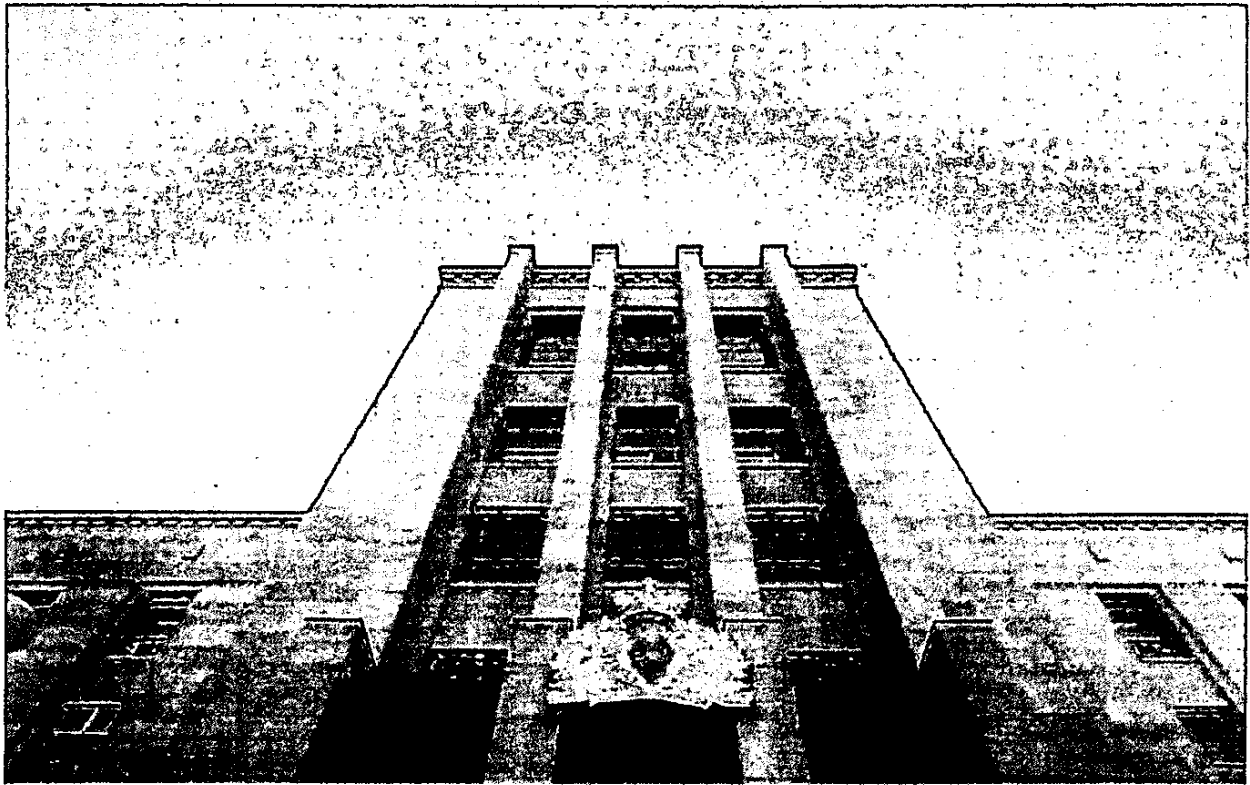
*If you have suggestions for the orientation guide please contact us via e-mail at [NSCI\\_ECSN@rcmp-grc.gc.ca](mailto:NSCI_ECSN@rcmp-grc.gc.ca) and let us know. We would be pleased to include any information that will assist in integrating new employees.*

*Again, welcome to the National Security Program.*

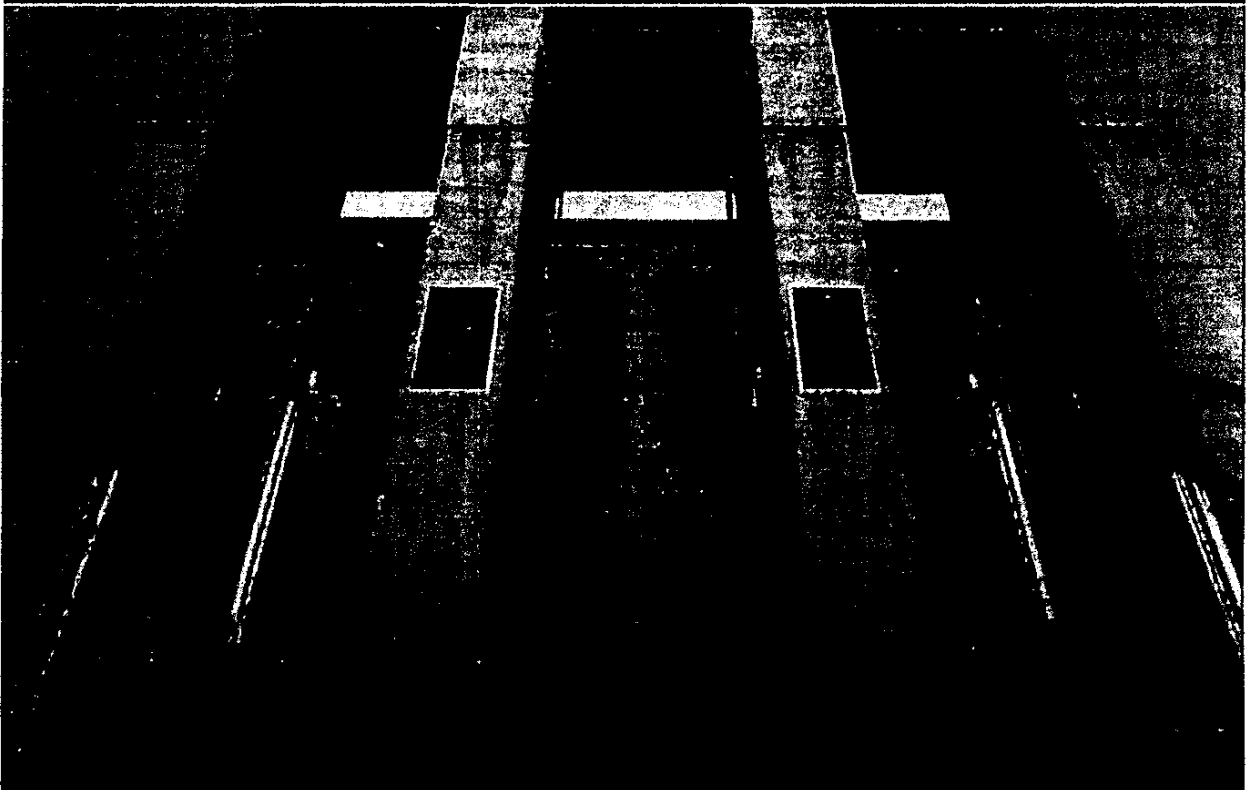
*Bob Paulson  
Assistant Commissioner  
National Security Criminal Investigations*

### National Security Criminal Investigations — Orientation Guide

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.



## Chapter One — About Headquarters



## GENERAL INFORMATION ABOUT HQ GROUNDS

### **Commissioner's Flag**

The Commissioner's flag is included on the flagpole near the front door of the Nicholson Building. If it is raised, the Commissioner is present at HQ. All flags flying at half-mast denotes a death within the Force.

### **Picnic Area**

Located in between the Canadian Police Information Centre (CPIC) and National Police Services (NPS) Buildings, the picnic area is an area where all employees may relax while enjoying a coffee or meal break.

### **Smoking Areas**

Smoking is allowed on campus in areas indicated by "Butt Stop" boxes. Please be aware that smoking directly in front of the doors of any building is not permitted.

### **Parking Lots**

Parking lots are located around the entire campus. Please see campus map for their various locations.

The parking lots at the HQ complex are currently full to capacity. Waiting lists for all areas have been established. Should you require a parking space, you must complete form 2613, which can be found on the Infoweb (see the Web Forms Catalogue: [http://infoweb.rcmp-grc.gc.ca/cio/bs/im/bpas/Forms/lics\\_index/index\\_e.htm](http://infoweb.rcmp-grc.gc.ca/cio/bs/im/bpas/Forms/lics_index/index_e.htm)), and be placed on a waiting list.

To obtain complete parking information, please visit Room B212 in the Nicholson Building.

RCMP employees may also park at the RCMP Building located at 295 Coventry Rd. for \$69.00 per month for outside parking or \$80.50 for inside parking. For more information, please call 613-842-8612.

If you would like an alternative to parking on the RCMP lots, consider parking in the church lot adjacent to our campus for \$45.00.

You may also park at The Canadian Tire on Coventry Rd for a monthly fee of \$50 (about a 10 minute walk from HQ).

### **Public Transportation Information**

OC Transpo operates bus and light rail service in the Ottawa area. Two buses service the RCMP campus: the #3 and the #103.

For more transit information, consult the OC Transpo Information Line, at 613-741-4390 or <http://www.octranspo.com>

### **Entering Campus**

Whether you are walking, biking or in a car, please slow down and show your security badge to one of the commissionaires on duty at the entrance to the campus.

### **Obtaining your Building Security Badge**

You will be issued a building security badge. You must wear this badge at all times and it must remain visible.

Your building security badge allows you access to various buildings on campus. Please notify your Security coordinator if you need access to more than one building or if you need access outside of normal office hours.

Please note that HQ personnel take security extremely seriously. If your badge is not visible, do not be surprised or offended if your identity is challenged by another RCMP employee.

### **Visitors**

When you have a visitor who is not an RCMP employee, it is your responsibility to meet them at the commissionaire's desk and register them as a visitor. All visitors must wear a visitor's badge and it must be visible at all times. You must accompany your visitor at all times.

When your visitor leaves, you must escort them back to the commissionaire's desk where they must drop off their visitor's badge.

### **Emergencies**

Should you need to call an ambulance or the fire department, please do not dial 911 directly.

Instead, call 613-993-1204 to alert the commissionaires at the main desk. They will assist you with all further emergency needs and will facilitate the entrance of emergency vehicles through the front gate.

Please remember to provide the commissionaires with your exact location, so that they may relay this information to the emergency workers

Protected "A"

## **The Nicholson Building**

### **Commissionaires' Desk**

The commissionaires' desk is located at the main entrance to the building. This is the desk at which you must sign in your visitors, obtain a temporary security pass should you forget yours, and ask other questions about the building and its security.

Should you have any questions, and would like to contact the commissionaires, they can be reached at 613-993-RCMP (7267).

### **Mail Room/Mail Slot**

The mail room is used to send outgoing mail, both external and internal. Please ensure that all outgoing external mail has correct postage and a return address on it or else it will not be processed.

The mail room is situated on the first floor, Room G-110.

Should the mail room be closed, please feel free to insert your mail through the various sizes of slots on the walls. It will be mailed at the next earliest mailing.

### **Cafeteria**

The cafeteria is situated on the first floor. It is open Monday-Friday from 6:30 a.m. until 3 p.m.

Breakfast is served from 6:30 a.m. until approximately 9:30 a.m. and a full lunch service is available at midday.

### **The HQ General Mess**

The licensed Officer's Mess facility is situated in the basement of the building. It is open on Thursday, Friday and Saturday nights until 2 a.m.

### **Gym**

The gym is located in the basement of the Nicholson Building. It is free for all employees of the RCMP. It is open 24 hours a day; seven days a week.

If you would like some assistance in creating a workout plan for yourself, feel free to contact Pierre Drouin at 613-993-0283. He can arrange a meeting with you and help you design a fitness training plan with specific objectives tailored to your personal wishes.

If you are interested, you may also inquire if you are eligible for a personal body fat and/or nutritional analysis.

To help you obtain your fitness objectives, the gym offers the following cardiovascular equipment: treadmills, elliptical machines, stair climbing machines, and stationary bicycles. It also has a weight room that features many machines, free weights and full length mirrors. Furthermore, there is a fully sprung floor for aerobics and other activities, a large and a small punching bag, mats for doing floor work, and exercise balls. For information on class schedules, please visit the infoweb at [http://infoweb.rcmp-grc.gc.ca/bulletin/hq/fitness/index\\_e.htm](http://infoweb.rcmp-grc.gc.ca/bulletin/hq/fitness/index_e.htm)

The locker room is available to anyone accessing the gym. Showers, towel racks, sinks, lockers, mirrors, benches and a medical grade scale can be found in the change rooms.

### **RCMP Store (also known as "the canteen")**

The canteen is located in the basement of the Nicholson building. It is open Monday to Friday, from 9:00 a.m. - 3:30 p.m. It stocks an array of RCMP branded merchandise along with candy and sundries. It also offers a pick-up and drop-off service for dry cleaning.

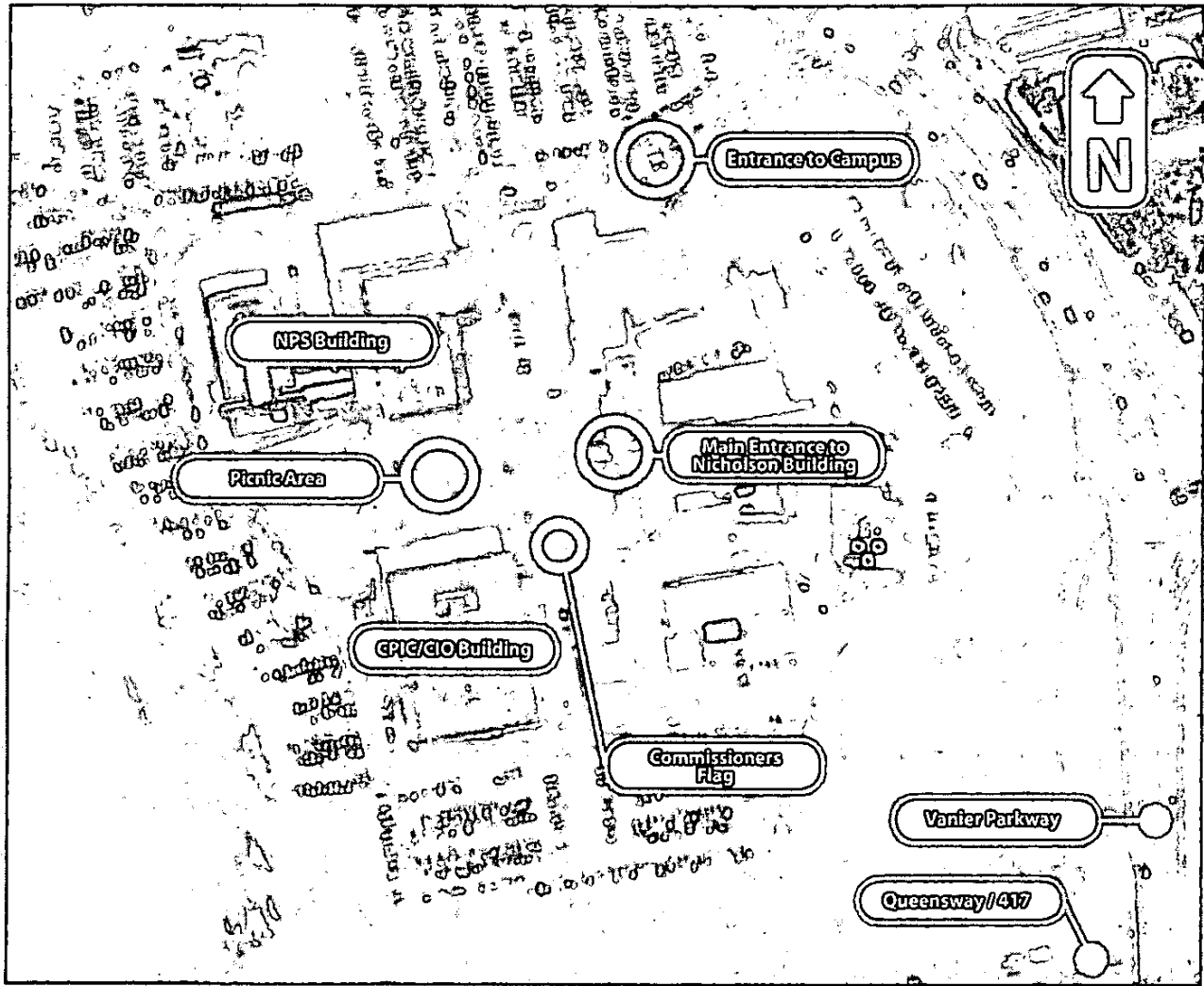
### **CS-COOP ATM Machine**

The ATM machine is located in the basement.

### **Vending Machines and Newspapers**

There are vending machines offering cold drinks and snacks, as well as various newspapers on the 1st floor of Nicholson Building, right outside the cafeteria doors.





### Emergencies

Should you need to call an ambulance or the fire department, please do **NOT** dial 911 directly.

Instead, call 613-993-1204 to alert the commissionaires at the main desk. They will assist you with all further emergency needs and will facilitate the entrance of emergency vehicles through the front gate.

Please remember to provide the commissionaires with your exact location, so that they may relay this information to the emergency workers.

#### National Security Criminal Investigations - Orientation Guide

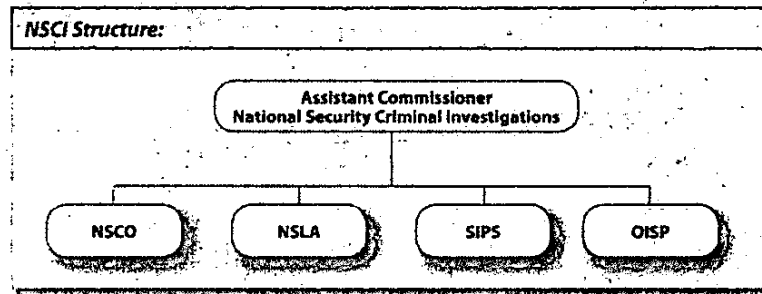
This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

5

## Chapter Two — National Security Criminal Investigations

National Security Criminal Investigations (NSCI) provides a national program for the management of national security criminal intelligence and operations that will permit the RCMP to detect, prevent and disrupt criminal activity having a national security dimension domestically or internationally, as it affects Canada. NSCI was established to ensure that all national security criminal resources and functions were aligned and controlled from within a single organizational structure. The Assistant Commissioner is responsible for the overall operation, administration and coordination of all the components of NSCI.

## NATIONAL SECURITY CRIMINAL INVESTIGATIONS



Four areas within NSCI report directly to the Assistant Commissioner:

- > National Security Criminal Operations (NSCO)
- > National Security Legislative Affairs (NSLA)
- > Strategic Integration & Program Support (SIPS)
- > National Office of Investigative Standards and Practices (OISP)

### **National Security Criminal Operations (NSCO)**

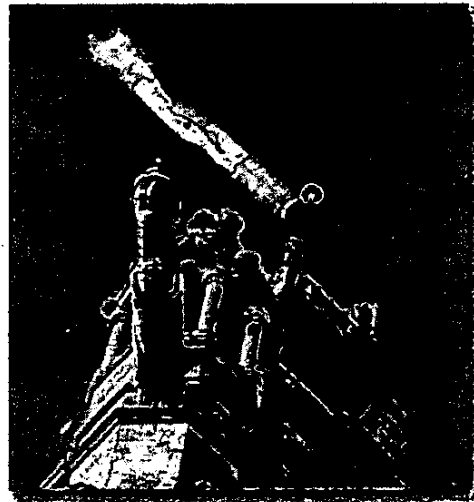
National Security Criminal Operations centrally controls all investigations relating to national security and consists of two units: National Security Criminal Operations Branch (NSCOB) and National Security Criminal Operations Support Branch (NSCOSB). These two units are composed of several sub-units.

### **National Security Legislative Affairs (NSLA)**

National Security Legislative Affairs provides a centrally controlled response to issues arising from public inquiries and civil litigation related to national security criminal investigations. It analyzes events on the public and political horizon that have implications for the RCMP's national security criminal investigative activities, particularly concerns emerging from government stakeholders, security and intelligence partners, the legal community and civil society. A key NSLA activity is providing advice to senior managers on national security issues with legislative and legal implications.

### **Strategic Integration & Program Support (SIPS)**

Strategic Integration and Program Support provides strategic direction and client services in the areas of program/policy development, intelligence research and development, HR, Training, creative design, alternative analysis, business planning, performance management, report on program management and expenditures, and briefing of senior management. Through consultation, feedback, quality assurance and communication processes, it ensures that obligations to internal partners, RCMP divisions and senior government and international bodies are met. A key component of this branch is its capability to act and respond in a visionary and proactive capacity.



#### National Security Criminal Investigations — Orientation Guide

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

Protected "A"

**National Office of Investigative Standards and Practices (OISP)**

NSCI is in the process of developing a National OISP to heighten oversight, raise accountability and manage civilian oversight for NS criminal investigations across the RCMP. A key function of the OISP will be to institute and manage a program for accreditation of team commanders. Team commanders, or case managers, are the single point of responsibility and accountability for major cases.

OISP's responsibilities would include ensuring field compliance with the principles of Major Case Management (MCM). MCM is a methodology for managing and leading major investigations; this provides accountability, clear goals and objectives, planning, utilization of resources and control over the speed, flow and direction of the investigation.

*Through the OISP, NSCI hopes to:*

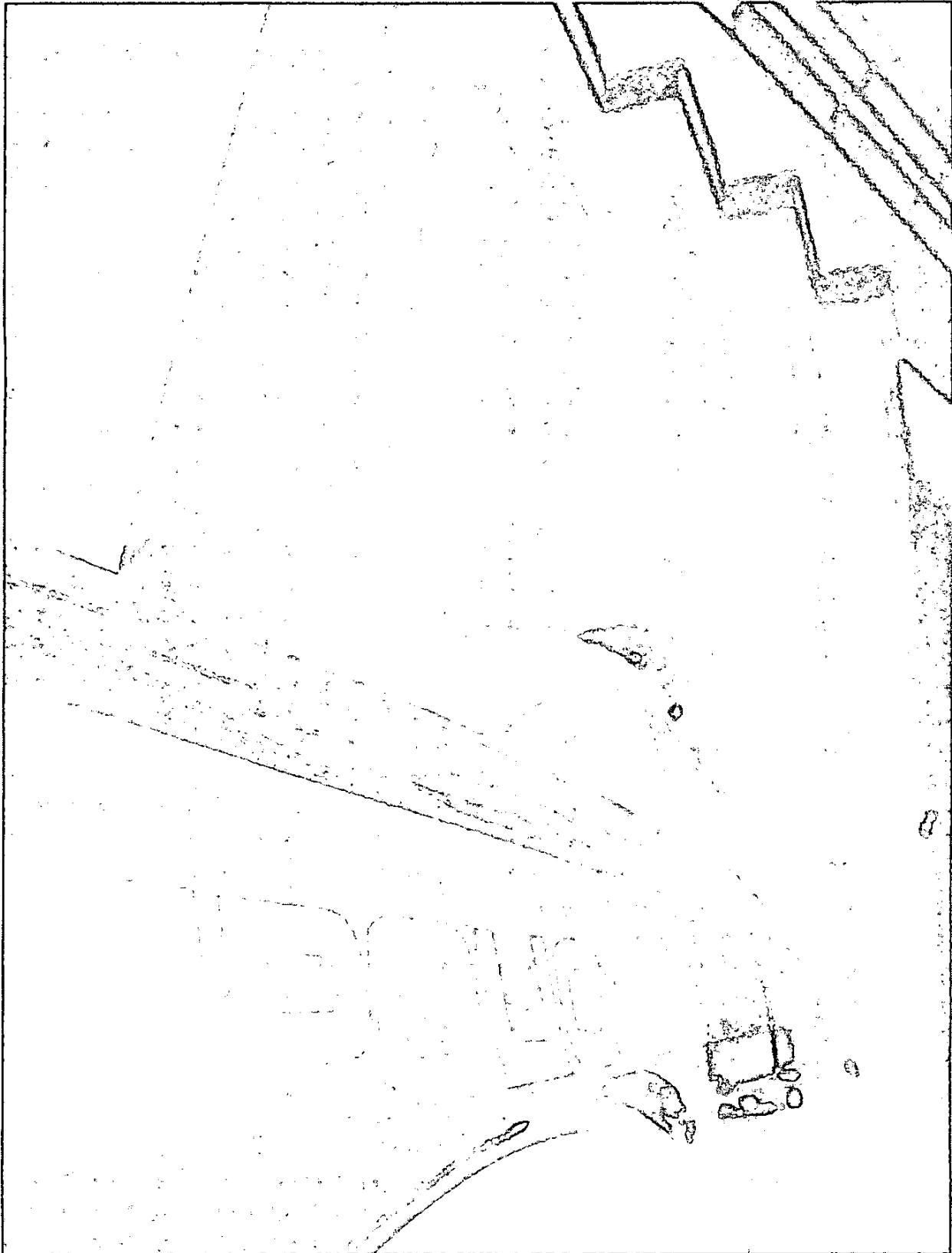
- > elevate operational oversight and accountability for major cases to those who are best positioned to both enable and enforce the consistent application of the principles of MCM;
- > develop a pool of accredited Team Commanders within National Security Criminal Operations to lead major investigations;
- > mitigate loss of public trust in law enforcement arising from failed major cases;
- > develop and sustain excellence in investigative practices;
- > develop active review of high-risk activity;
- > conduct critical debriefs and after-action reporting on best practices / challenges;
- > respond pro-actively to civilian oversight of NS criminal investigations; and,
- > demonstrate transparency and impartiality through civilian oversight.



**National Security Criminal Investigations — Orientation Guide**

8

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.





## NSCOB: STRUCTURE AND DUTIES

National Security Criminal Operations Branch (NSCOB) monitors, assesses, coordinates and directs all RCMP national security criminal investigations from a national and international perspective. It supports field operations by reviewing, analyzing and disseminating information from all sources, including the Canadian Security Intelligence Service (CSIS), various domestic and international partners, and RCMP field investigations. NSCOB also prepares subject profiles, case briefs and briefing notes for senior management, ensures compliance with RCMP policy, and tasks RCMP Liaison Officers in Canada and abroad in support of RCMP national security criminal investigations. It also co-ordinates the National Counter-Terrorism Plan on behalf of the RCMP.

### National Security Criminal Investigations — Orientation Guide

10

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

**The units within NSCOB are:****Intake Unit (IU)**

The Intake Unit is a critical point for initial contact and is responsible for processing all national security related requests for assistance/inquiries. These requests originate from, but are not limited to, domestic and foreign law enforcement agencies, domestic and foreign government and non-government agencies, RCMP Liaison Officers, other RCMP business lines, and information/tips received from the public. The Intake Unit ensures that the requests and related reports are gathered, assessed, entered onto the secure file management database (SCIS/SPROS) and disseminated to the appropriate unit or section in order to be dealt with as per the prescribed policy.

The role of the Intake Unit is integral to meeting the requirement that all national security criminal investigations be centrally coordinated by HQ.

**Intake Unit Reviewers:**

- > review and assess correspondence to determine if the information is related to an ongoing SCIS/SPROS investigation;
- > review and assess new information to determine its relevancy to the national security mandate;
- > conduct indices checks;
- > create supplementary reports including the results of basic indices checks;
- > create new SPROS occurrences when appropriate;
- > process correspondence related to ongoing SCIS/SPROS investigations;
- > task the relevant unit/team within NSCOB.

**National Response Team (NRT)**

NRT is the primary unit for oversight of the majority of national security criminal investigations. It supports field operations conducted by the National Security Enforcement Sections (NSES) and Integrated National Security Enforcement Teams (INSET) and tasks RCMP Liaison Officers abroad, in support of RCMP national security related criminal investigations. NRT also prepares subject profiles, case briefs and briefing notes for senior management and ensures compliance with RCMP policy, mandate and law. It acts as a critical control point for ongoing investigations. NRT also provides necessary Headquarters approvals (i.e., International Travel, including travel of foreign police officers to Canada).

**Emerging Trends Unit (ETU)**

The ETU establishes an enhanced capacity to systematically collect, evaluate, analyze and disseminate information, from a multitude of internal and external clients and partners, designed to identify and predict emerging trends in national security criminal investigations. ETU regularly reports to senior management and to the Divisions with respect to a variety of topics. Due to its location within NSCOB, the Emerging Trends Unit has the capability to provide a national perspective. It provides monthly reporting to the Divisions in order to keep them abreast of investigations occurring in other regions of Canada. ETU links commonalities in an effort to identify emerging trends and provides Sensitive Case Reporting to the Deputy Commissioner, Operations and Integration (DCOI), including empirical analysis of data, such as case load and resource allocation, and mapping of significant events or trends. ETU is responsible for updating and disseminating Litigation Reports and Monthly Case Synopsis Reports to INSET and NSES management. The Unit monitors quality assurance of files in NSCOB and supports Critical Infrastructure Criminal Intelligence (CICI) Section in regular reporting to partners in the private and public sector. ETU collects, evaluates and analyzes information with respect to major events worldwide relative to national security and terrorism.

The Unit also responds to various taskings on issues of concern and emerging trends within Canada and abroad, such as the use of the Internet by extremists for propaganda and recruitment, new trends in domestic and foreign terrorist training, radical imams, etc.

**National Priorities Project Team (NPPT)**

NPPT assesses, monitors, and provides operational support and direction as appropriate on established national priorities, at the national and international level, related to major case priority projects. Other responsibilities include coordinating approvals for major projects such as Undercover Operations, Part VI Investigations (electronic surveillance), Sensitive Case Investigations, Preventative Arrest, Investigative Hearings, the laying of *Anti-Terrorism Act* charges, and foreign operational travel.

NPPT provides analytical reports and key advice to senior management and is responsible for handling Canadian Security Intelligence Service (CSIS) disclosure and advisory letters (for use in affidavits and search warrants). CSIS often gathers parallel security intelligence related to RCMP national security criminal investigations. As a result, RCMP and CSIS efforts related to major operations require coordination and reporting to senior management and government. NPPT is a critical point for ongoing investigations. The team also facilitates contact with foreign law enforcement agencies.

**National Security Criminal Investigations — Orientation Guide**

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

11

Protected "A"

### **Anti-Terrorist Financing Team (ATFT)**

Responsible for the assessment, coordination, monitoring, operational support and progress reporting of established national priorities at the national and international level with respect to financing activities associated with terrorism; ensures that operations conform with legislation; implements approved new operational support mechanisms and strengthens existing ones.

The ATFT supports counter-terrorism strategies with respect to terrorist financing, financial intelligence gathering, investigations, and enforcement. ATFT provides operational anti-terrorism financing support to national priority projects as well as all ongoing national security criminal investigations by providing advice, and making recommendations based on the examination of financial information received from various sources specific to terrorist financing offences. It is also responsible for preparing documentation for the *Criminal Code* listing process in respect to terrorist entities (see <http://publicsafety.gc.ca/prg/ns/le/index-eng.aspx>). ATFT also assists the Department of Foreign Affairs and International Trade in relation to the United Nations/Office of the Superintendent of Financial Institutions list (see [http://www.osfi-bsif.gc.ca/osfi/index\\_e.aspx?DetailID=525](http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?DetailID=525)) and Certificates of Mistaken Identity.

ATFT has enhanced its role and participates within national and international forums such as the Financial Action Task Force, the G8 Law Enforcement Projects Subgroup (Roma/Lyon Group), the International Working Group on Terrorist Financing, as well as, the Terrorist Financing Working Group of the Canadian Bankers Association, Five Eyes (Canada, US, UK, Australia, New Zealand) Terrorist Financing Working Group, and the Bi-lateral (US-Canada) Anti-Terrorist Financing Working Group.

### **Terrorist Entity Listing Group (TELG)**

Prepares cases for adjudication under existing legislation that provides for terrorist entities to be identified, thereby restricting the capabilities and activities of extremist organizations and individuals. TELG also implements and supports counter-terrorism and anti-terrorist strategies, activities, procedures, policies and standards.

### **Extra-Territorial Investigations**

Provides the RCMP with the capability to respond to terrorist activity committed outside of Canada, where the act is committed against a Canadian citizen or by a Canadian citizen. A member will be required to travel to conduct investigations outside of Canada. The member

will also be responsible to establish protocols with client partners to ensure an integrated interdepartmental approach to extra-territorial jurisdiction. The ensuing investigation will be conducted as per Canadian standards and the RCMP could be tasked to participate and/or conduct these investigations. Therefore, the duties of the Extra-territorial Unit are to enforce the legislation enacted by the Canadian government.

### **Analytical Component:**

Analysts are assigned to each of the above noted units to provide key support for all investigations. The analyst performs the following key activities:

- a) Researches subjects related to international events, groups, or political/ideological/religious dynamics in order to provide appropriate context and relevant material for all national security criminal investigations and briefings. Analysts are considered subject matter experts.
- b) Researches, collates, evaluates and analyzes information from a variety of closed and open sources in order to develop a complete and accurate picture of specific elements of criminality that are national and international in scope.
- c) Supports investigations by providing link charts, associative charts, diagrams, maps, target profiles, summaries, briefs, time-lines, and all other related analytical products as deemed appropriate for a given topic or file.
- d) Acts as the bridge between investigations and intelligence, gathering all relevant and available material and determining what may be included in a given analytical product depending on need, dissemination, classification or eventual end-purpose.
- e) Identifies and evaluates extremist organizations, extremist targets, illicit commodities and trends that are national or international in scope in support of the RCMP National Security Program.

Please remember to engage analysts within your section AS SOON AS A FILE gains importance. The analyst is a key component in all investigations, particularly national security criminal investigations, which are often more complex and critical than other law enforcement domains.



CBC News: the fifth estate - Microsoft Internet Explorer provided by Bell Business ISP

File Edit View Favorites Tools Help

Address http://www.cbc.ca/fifth/

**cbc.ca** RADIO TV RADIO-CANADA.ca SHOP Search Links

**the fifth estate**

CBC-TV: Wednesdays at 8pm & midnight on CBC-TV  
CBC Newsworld: see times at right

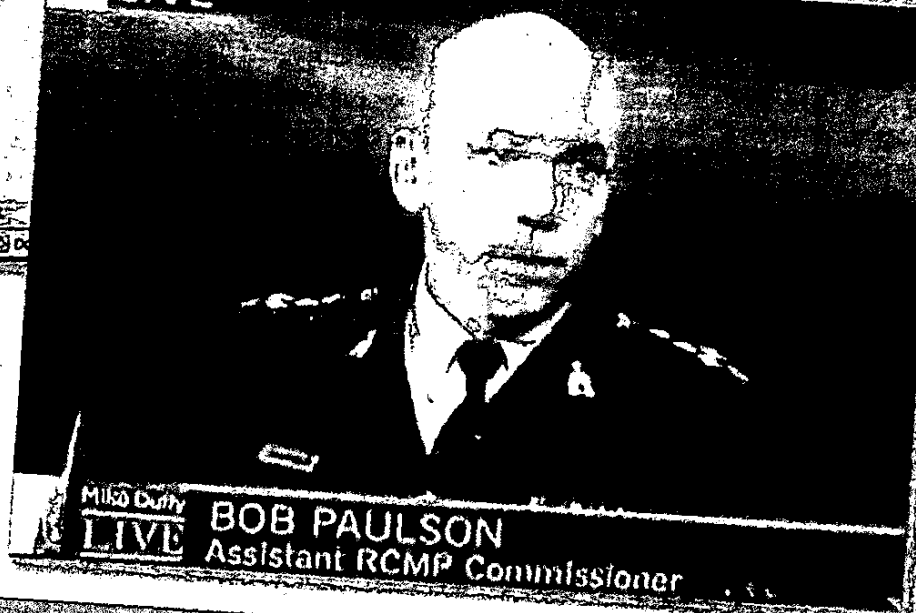
**AMONG THE BELIEVERS: CRACKING THE TORONTO TERROR CELL**  
Wednesday January 17 at 9pm on CBC-TV  
see CBC Newsworld times at the right

Last summer, Toronto's mostly moderate Muslim community found itself in the glare of unwelcome public attention from the international media when eighteen men were charged with plotting terrorist attacks on Canadian soil.

In a special co-production with PBS Frontline, the fifth estate goes inside the alleged terror cell.

**ON CBC NEWSWORLD**  
AMONG THE BELIEVERS: CRACKING TORONTO'S TERROR CELL  
Friday January 19 at 10pm  
Saturday January 20 at 10pm

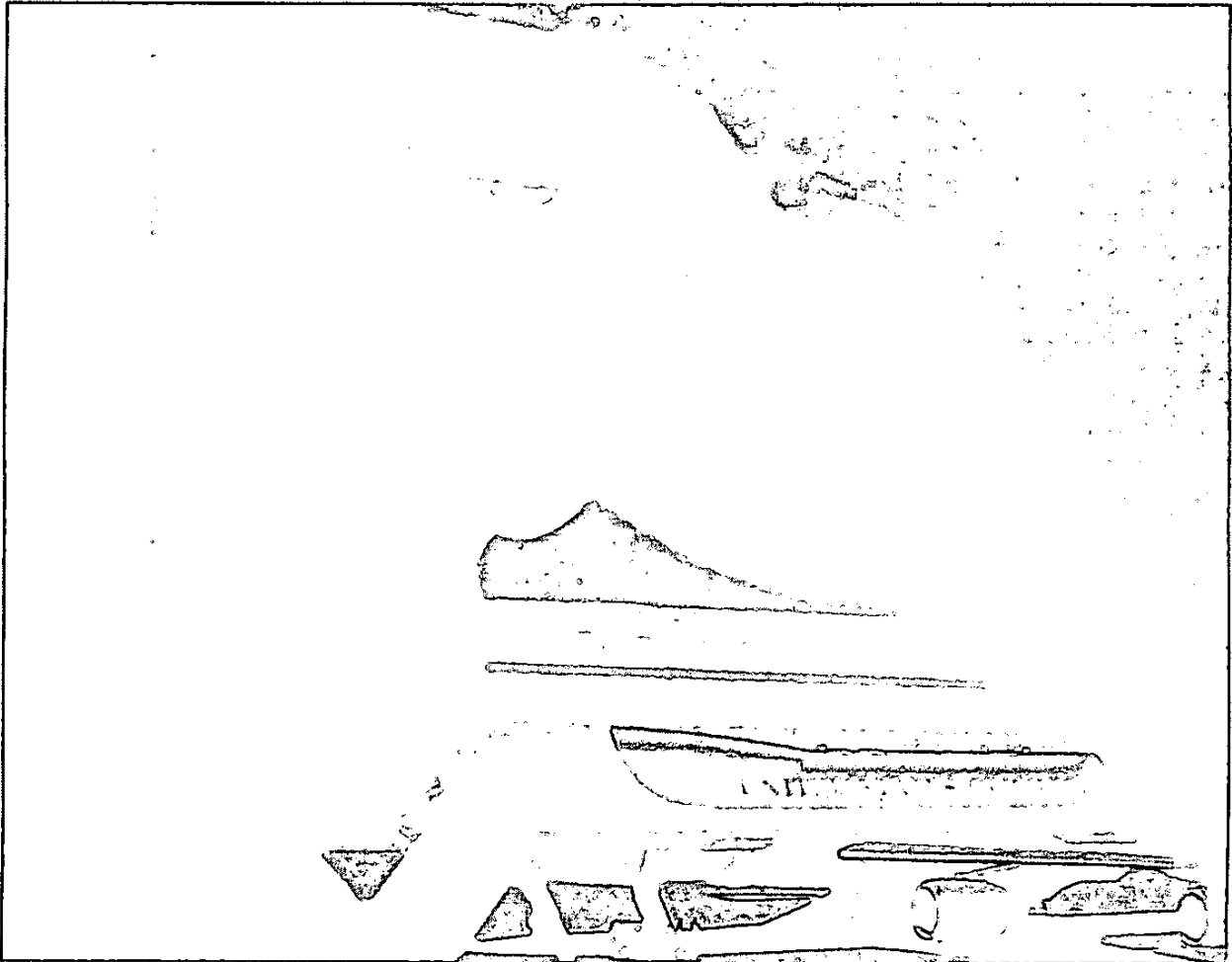
**LIVE**



**Mission Duty LIVE** **BOB PAULSON**  
Assistant RCMP Commissioner

National Security Criminal Investigations - Orientation Guide

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.



NSCOSB: STRUCTURE AND DUTIES

### **NSCOSB: Structure and Duties**

National Security Criminal Operations Support Branch (NSCOSB) provides support to NSCOB in the following capacity:

#### ***National Security Threat Assessment Section (NSTAS)***

NSTAS monitors events, investigations and intelligence reports and prepares threat assessments on national security issues which may pose a threat to Canada. Internationally Protected Persons or to Canadian interests abroad. It's legislative mandate and primary responsibility is to identify and evaluate potential threats associated to subjects, events and locations regarding Protective Policing clients. Five units within the section are responsible for various aspects of the program.

##### **1 Canadian Executive Protective Intelligence:**

Conducts tactical Threat Assessments (TAs) and monitors events regarding Canadian Executives such as the Governor General, the Prime Minister, Cabinet Ministers and certain other Members of Parliament, as well as Supreme Court, Federal and Tax Court Justices. These products can be general in nature or be focused on a particular event or travel within Canada or abroad. The unit also conducts Threat Assessments for Parliament Hill, the Supreme Court, as well as other prominent federal buildings. It is also responsible for developing TAs on Security Certificate Detainees (for information on security certificates see <http://publicsafety.gc.ca/prg/ns/seccert-eng.aspx>) and in support of Federal and International Operations in regards to the potential deployment of RCMP resources abroad.

**2 International Protective Intelligence:** Conducts Tactical Threat Assessments for foreign missions in Canada, including embassies, consulates and foreign visitors (Internationally Protected Persons) traveling to Canada. It also conducts TAs for major events taking place in Canada and abroad such as the Olympic and Commonwealth Games, the G8 and other political summits.

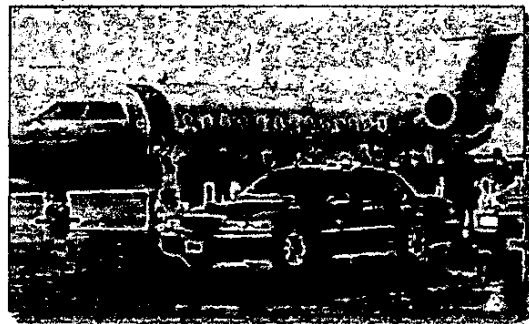
**3 Civil Aviation Protective Intelligence:** Identifies flights/routes in Canada that represent a risk of terrorist action or other aviation threats. Provides threat assessments to Canadian and international airports and carriers. The unit supports the Canadian Air Carrier Protective Program (CACPP), which assigns RCMP Aircraft Protective Officers (APO's) to Canadian flights and provides intelligence support for a range of clients. The unit also produces bulletins on aviation and security related matters.

##### **4 Threat Management Protective Intelligence:**

Coordinates and maintains the Protective Policing Persons of Interest Program which identifies, investigates and monitors individuals who have shown a criminal or abnormal interest in public figures who fall within the Protective Policing mandate.

##### **5 Intergovernmental Coordination:**

Conducts criminal checks and security checks on behalf of the Commissioner for the Privy Council Office and Department of Justice to assist the Prime Minister with suitability of candidates for certain public office positions (Senior positions within the Government of Canada and Federal Judiciary).



#### ***Protective Intelligence and Threat Assessment Section (PITAS)***

Monitors events and prepares threat assessments on national security issues which may pose a threat to Canada, or to Canadian interests abroad. Three units within the section are responsible for various aspects of the program.

#### ***Airline Passenger Assessment and Security Project (APAS)***

Provides an RCMP contribution to a horizontal initiative involving Public Safety Canada (PS), Transport Canada (TC), Canadian Security Intelligence Service (CSIS), Canada Border Services Agency (CBSA) to implement the provisions of Sections 4.81 and 4.82 of the Aeronautics Act. Section 4.81 forms the basis of Passenger Protect as announced jointly by the Minister of Transport and Deputy Prime Minister in August 2005. Section 4.82 authorizes the Commissioner to designate persons who can request information listed in the schedule of the Act from air carriers and air reservations system operations. This information will be matched with information under the control of Transport Canada, the RCMP and CSIS to identify threats to transportation security.

**Critical Infrastructure Criminal Intelligence (CICI)**

CICI examines physical and cyber threats to critical infrastructure in support of the RCMP's and Government of Canada's critical infrastructure protection mandates. CICI collaborates closely with domestic (such as Public Safety Canada, CSIS, ITAC, provincial government agencies, and private sector stakeholders) and international (such as security and police partners in the US, UK, and Australia) partners to acquire, assess, analyze and share information to prevent, detect, deter and respond to actual and potential national security criminal threats to Canada's critical infrastructure.

CICI projects are intelligence-led and priority based. CICI produces criminal threat, risk, and intelligence assessments and indications and warnings related to physical and cyber threats to critical infrastructure through comprehensive analysis, research and evaluation of information from a variety of classified and open sources. CICI also participates in joint threat, vulnerability and risk assessments with public and private sector partners. To support this work, CICI researches analytical and risk assessment methodologies to identify, develop, and implement tools and best practices.

CICI members provide subject matter expertise to NSCI investigations and other RCMP supporting programs, and participate as subject matter experts in Interdepartmental Expert Groups (IEG) (including the IEG Domestic Security, which is developing a national all-hazards risk assessment), as well as domestic & interdepartmental working groups, meetings and conferences.

CICI coordinates the development of a robust, centrally coordinated, Canada-wide framework to: (i) collect, analyze and share suspicious incident criminal information; (ii) enhance inter-jurisdictional police co-operation, intelligence and information sharing amongst government, law enforcement and the private sector; and (iii) support the comprehensive identification and examination of national security threats to critical infrastructure.

This framework will consist of a secure web-portal to: (a) allow the rapid collection of suspicious incident reports from private sector security stakeholders, and (b) provide access to a library of finished intelligence products by government, law enforcement and industry security stakeholders. The reports of suspicious incidents with a possible nexus to national security will be analyzed using a new streamlined approach and innovative analytical tools to better support operational and tactical decision-making.

**National Security Community Outreach Program (NSCOP)**

The program employs proactive and consultative measures to forge and enhance links with communities and groups impacted by national security issues.

**Mandate**

In keeping with the Government of Canada's goal of Safe Homes and Safe Communities, Canada's Action Plan Against Racism, the RCMP's Bias-free Policing Strategy and its national terrorism and youth priorities, the RCMP National Security Program (NSP) established the National Security Community Outreach Program (NSCOP) in April, 2005.

The program is a comprehensive effort to engage all Canadian communities, including the diverse ethnic, cultural and religious communities in protecting Canada's national security. This is accomplished in part by increasing the understanding of mutual goals and concerns and ensuring appropriate and informed communications should a crisis arise.

**Sensitive Information Handling Unit (SIHU)**

Develops, implements and manages procedures and protocols for the handling and release of sensitive national security information.

SIHU has been established in the National Security Criminal Operations Support Branch to provide for the centralized processing and control of foreign and sensitive information and criminal intelligence.

SIHU supports the National Security Criminal Operations Support Branch (NSCOSB), the Integrated National Security Enforcement Teams (INSETs), the National Security Enforcement Sections (NSES), the Integrated Border Enforcement Teams (IBETs), Threat Assessment, Critical Infrastructure Criminal Intelligence Section, Liaison Officers (LO's), Peacekeeping operations and Criminal Intelligence Major and Serious Organized Crime.

SIHU also supports National Security Criminal Operations Branch by providing intelligence received from sensitive intelligence sectors in the form of intelligence analysis reports, summaries and officer safety alerts.

**National Security Border Integrity Unit**

Provides analysis and draws linkages between national security threats to protect Canadian borders from extremist groups.

**Mandate**

To facilitate cooperation and provide a link between all programs responsible for protecting our borders and those overseeing investigations related to national security.

To explore and report on the nature and extent of affiliations between terrorist groups and their activities and other forms of cross border criminal activities, including organized crime.

**Role and Responsibilities**

Collection, collation, evaluation, analysis and dissemination of information and intelligence pertaining to the affiliations of terrorist groups and activities, and their association with cross border criminal activities.

Produce strategic and tactical criminal intelligence reports to provide management and field units with insight into cross border criminal activities and trends.

**Open Source Criminal Intelligence Section (OSCIS)**

OSCIS specializes in collecting and retrieving open source information available through the Internet in order to develop and turn this information into meaningful and actionable criminal intelligence.

The section supports all national security criminal investigative and support sections within the RCMP. As part of its mandate, it also provides related training to the RCMP National Security Program and many of its domestic and international partners.

**Independent File Review Unit (IFR)****Mandate**

Under the direction of the A/Commr. National Security Criminal Investigations and the DG National Security, an IFR procedure was requested to enhance the service delivery of the National Security Program.

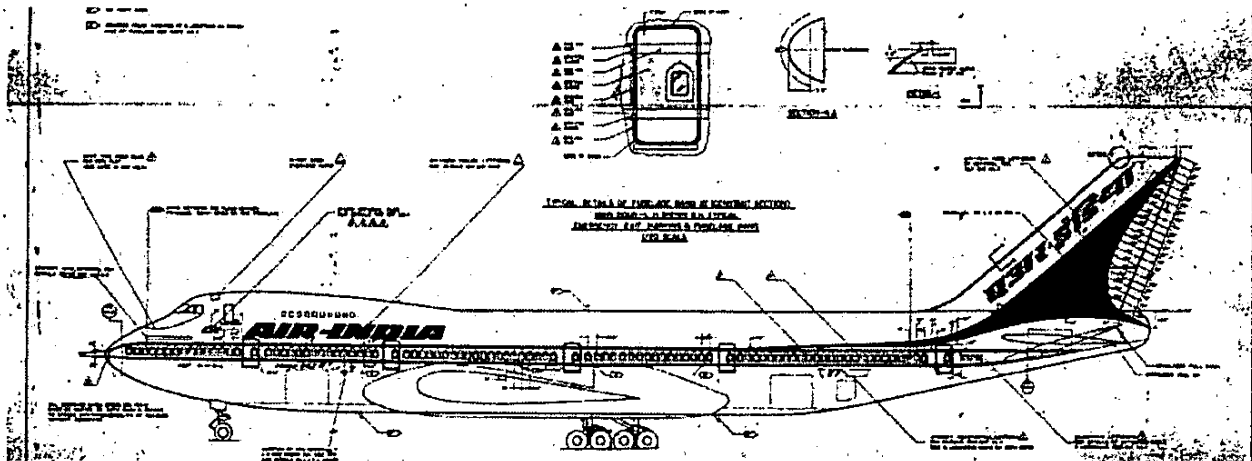
**Role and Responsibilities**

- > The DG National Security will make the final decision of when to implement this process
- > Reviews are conducted under the supervision of an experienced Major Case practitioner, not involved in the investigation
- > Working in conjunction with the INSET and NSES commanders, the review is guided by the principle of cooperation
- > The results of the review are documented and reported to the DG National Security or his/her delegate
- > The review teams' reporting or recommendations in relation to the file is subject to disclosure
- > The assessment of resources includes the appropriate intra and inter-agency response when applicable
- > A peer review should be considered in *all* National Security investigations where there is an Operation/Project name
- > Major cases are serious in nature, which by virtue of their need, complexity, risk, and resources, require the application of the principles of Major Case Management
- > Major cases will be submitted for an independent review if an investigation has become prolonged, complex, difficult or stalled

**National Security Criminal Investigations — Orientation Guide**

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

17



## NSLAB: STRUCTURE AND DUTIES

### General Description

National Security Legislative Affairs provides a centrally coordinated response to issues arising from public inquiries and civil litigation stemming from national security criminal investigations. It also analyzes events on the public and political horizon that have implications for the RCMP's national security criminal investigative activities, particularly concerns emerging from government stakeholders, security and intelligence partners, the legal community and civil society. A key NSLAB activity is providing advice to senior managers on national security issues with legislative and legal implications.

### Inquiry Liaison

Presently, NSLAB personnel are engaged with two public inquiries: Air India and Iacobucci. The team has produced thousands of documents for Commission counsel, responded to numerous requests for information, and attended regular weekly meetings to coordinate work and plan strategy with Government of Canada counsel. NSLAB has also notified, scheduled and prepared more than 50 witnesses (from the RCMP and integrated police forces) for testimony at the inquiries. Redacting RCMP documents for public disclosure purposes and protecting investigative methods and sources has been a key activity throughout. During the final phase of these inquiries, NSLAB personnel have been collaborating with counsel to prepare the Government's final submission to the Commission.

### Litigation and Parliamentary Response

Team members working in this area have coordinated responses to ongoing and prospective civil litigation against the RCMP stemming from actions with respect to national security criminal investigations. This includes the preparation of briefing material for senior officers,

responding to questions emanating from the Department of Justice, and developing a coordinated response with other agencies and departments.

NSLAB also prepares briefing material for appearances by senior RCMP officers at a number of Parliamentary committees such as the Special Senate Committee on Anti-Terrorism, the Senate Committee on National Security and Defence, and the Standing Committee on Public Safety and National Security.

NSLAB personnel have also prepared material and participated in discussions (both internal and at the inter-departmental level) on the review of the *Canada Evidence Act* (i.e., protecting confidential information from disclosure), contributed material to the reviews by the House and Senate of the *Anti-Terrorism Act*, and provided input on behalf of the RCMP to reform the security certificate process within the *Immigration and Refugee Protection Act*.

### National Security Review

NSLAB coordinates the RCMP's response to government-led initiatives with respect to enhancing public accountability in the national security sphere. Its activities include providing feedback on proposals for new review models, collaborating on an inter-departmental working group to enhance the current review process, and developing critical discussion papers on proposals to strengthen the Commission for Public Complaints Against the RCMP (CPC). It also collaborates with the Public Complaints Unit of the RCMP when there is a complaint in the national security area.

### Major Case Management

This team within NSLAB centrally coordinates NSCI investigative files for public inquiries and ongoing litigation, public complaints and civilian review in the national

## SIPS: STRUCTURE AND DUTIES

security domain. Its key activities are collating, organizing, classifying, vetting, formatting and centrally storing information for use by any of the processes noted above. This unit is modernizing and more broadly improving NSCI's ability to respond to the requirements of external agencies (e.g., the Commission for Public Complaints Against the RCMP) or *ad hoc* bodies such as public inquiries. Work being done in this area will evolve into standard file management practices employed by the National Security Operations Branch.

### General Description

Strategic Integration & Program Support (SIPS) provides strategic direction to NSCI by developing policies, programs and processes to ensure that NSCI is meeting its obligations to internal partners, RCMP divisions, senior government and international bodies. Through the application of consultative feedback and quality assurance processes, and the provision of research, analysis and communication services SIPS ensures NSCI is equipped to meet current and future criminal intelligence requirements. SIPS is also responsible for providing direction and support to NSCI for the implementation of the O'Connor Commission recommendations (see [http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher\\_arar/07-09-13/www.ararcommission.ca/eng/index.htm](http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/index.htm) for the Commission report).

### Alternative Analysis (AA)

AA conducts analysis of the strategic environment in order to provide in depth understanding of issues that may affect the RCMP. Its focus is the global context from which crime and national security threats emerge. Its primary clients are the Deputy Commissioner of Operations and Integration, Assistant Commissioners, the Operations Council, the Senior Management Team (SMT) and the Senior Executive Committee (SEC).

Intelligence Research and Development (IR&D) IR&D researches, develops and updates criminal intelligence processes, methods and techniques to assist and enhance intelligence analysis and management processes. Projects include updating SLEIPNIR (a threat-measurement technique), developing the Disruption Attributes Tool (DAT) and Priority Rating of Operational Files (PROOF) techniques for National Security, and writing Criminal Intelligence Doctrine.

### National Security Criminal Investigations Support Services:

Strategic Integration & Program Support (SIPS) provides strategic direction to NSCI by developing policies, programs and processes to ensure that NSCI is meeting its obligations to internal partners, RCMP divisions, senior government and international bodies. Through the application of consultative feedback and quality assurance processes, and the provision of research, analysis and communication services SIPS ensures NSCI is equipped to meet current and future criminal intelligence requirements. SIPS is also responsible for providing direction and support to NSCI for the implementation of the O'Connor Commission recommendations (see [http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher\\_arar/07-09-13/www.ararcommission.ca/eng/index.htm](http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/index.htm) for the Commission report).

### Briefing Co-ordination (BC)

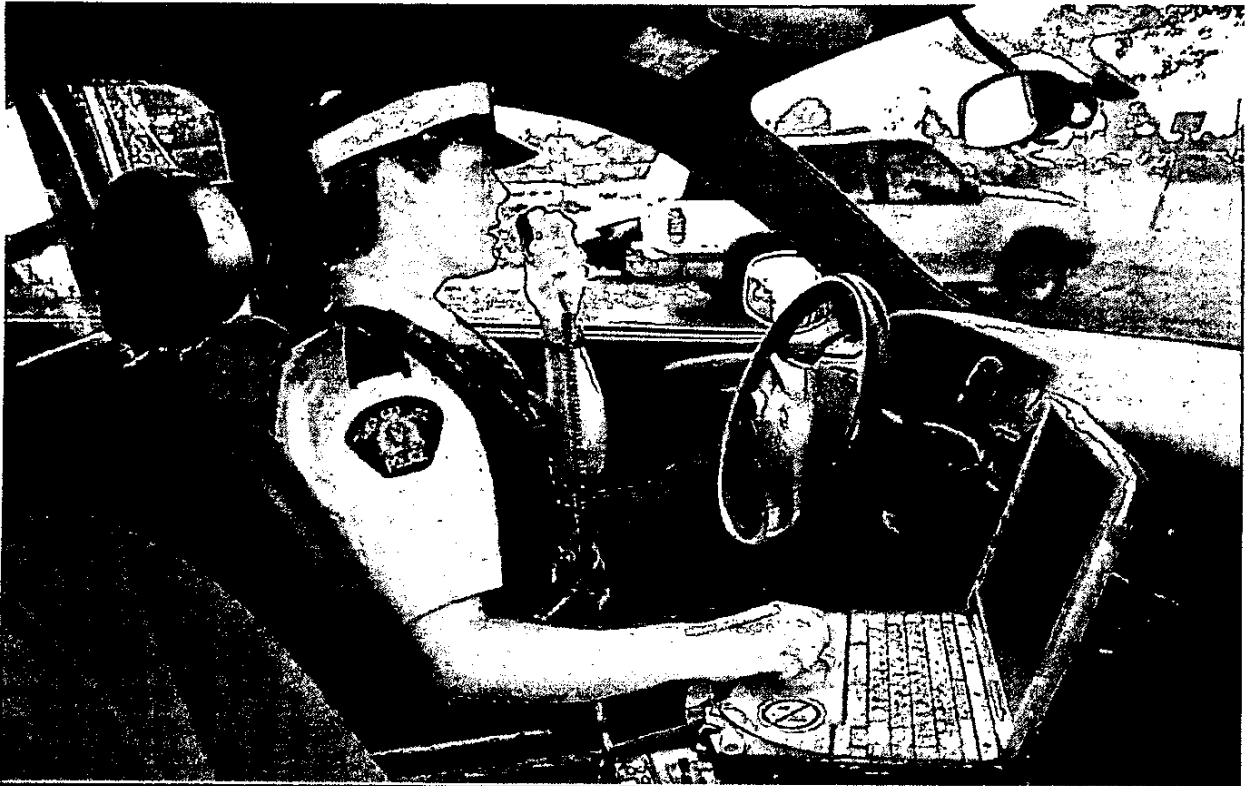
Co-ordinates and produces comprehensive and timely responses to requests for NSCI information and briefing materials from internal and external partners. BC works closely with Integrated Operations Support (IOS) to respond to briefing requirements for the Commissioner and Deputy and Assistant Commissioners.

### Client Services Section (CSS)

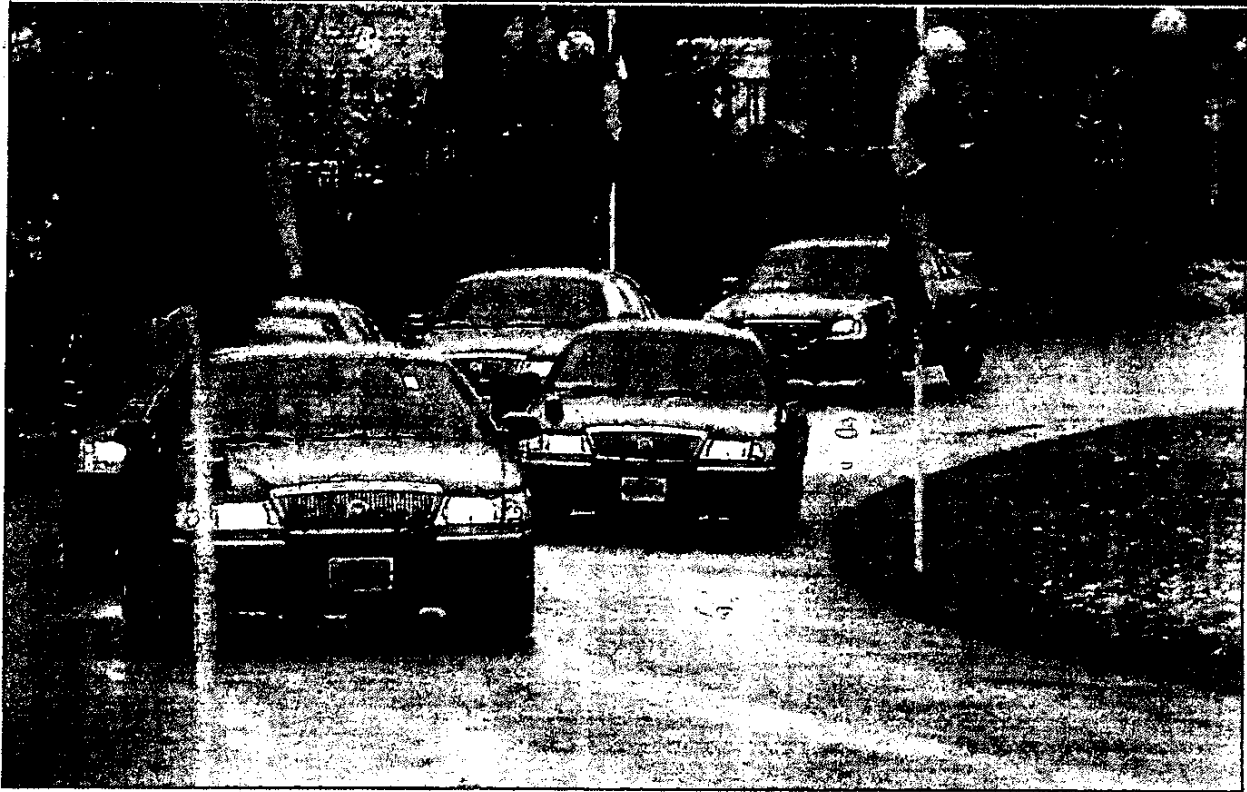
Provides professional expertise in the area of creating a better understanding and awareness of all aspects of national security policies, practices, processes and products. This includes creating national security-specific documents, presentations and products. CSS is also responsible for establishing production and graphic standards for NSCI products, and the ongoing development of related sections of the Infoweb, RCMP public web site and secure government network.

### Policy and Program Development (PPD)

PPD ensures that policy relative to national security is current and addresses issues related to program co-ordination. This includes developing Memoranda of Understanding (MOU), secondment and information sharing agreements with outside agencies, and the monitoring of quality assurance processes on critical issues, such as co-operation with foreign security intelligence agencies. Other responsibilities include managing the Balanced Scorecard (a performance measurement tool), contributing to business planning and the Departmental Performance Report, financial administration, security, training co-ordination and employee accommodations.



**Chapter Three — Integrated National Security Enforcement Teams (INSET)**





### Background

- > The Royal Canadian Mounted Police is the legislated, designated lead agency for investigating criminal acts of terrorism within Canada (see the *Security Offences Act* — <http://laws.justice.gc.ca/en/showtdm/cs/S2Z>). There is also a memorandum of understanding (MOU) in place with Health Canada for the RCMP to lead investigations into Chemical, Biological, Radiological and Nuclear (CBRN) incidents. Historically, the RCMP's National Security Enforcement Sections (NSES) — formerly called National Security Investigation Sections — was the unit assigned to the national security file.
- > Integrated National Security Enforcement Teams (INSET), which are made up of representatives of the RCMP, federal partners and agencies such as Canada Border Services Agency, Citizenship and Immigration Canada, Canadian Security Intelligence Service, and provincial and municipal police services, were created in the Post 9/11 environment to address the issue that no single agency can investigate terrorism in isolation.
- > There are currently four INSET's in Canada: Vancouver, Toronto, Ottawa and Montreal with a unit planned for Edmonton. RCMP NSES units still exist in the other provinces.

### Mandate

- > Increase the capacity to collect, share and analyze intelligence among partners, with respect to suspects that are threat to national security.
- > To create an enhanced enforcement capacity to bring such suspects to justice
- > Enhance partner agencies' collective ability to combat national security threats and meet specific mandate responsibilities.

### INSET Unit Structure

#### Support Unit

Public Service Employees: duties include — records management, exhibit management, finances, pay and compensation, kit, equipment procurement and upkeep, transcriptions, mail, secure faxes.

#### General Enforcement Unit (GEU)

Investigates complaints received via phone or fax, from internal and external partners and requests from foreign agencies. Generally, short term investigations are assigned to individual team members.

#### Protective Intelligence, Threat Assessment Unit (TA)

Working in conjunction with the RCMP VIP unit, Municipal and Federal agencies, the team conducts regional assessments on potential threats to Internationally Protected Persons (IPP's), VIP's and at functions that might have international visitors, VIP's or involve international relations and trade.

#### Anti-Terrorist Financial Investigation Unit (ATFIU)

ATFIU's role is to investigate financial leads relating to terrorist financing and support. The unit supports other INSET investigations and conducts its own projects as well.

#### Project Teams

The team conducts long term investigations of a complex nature using the principles of Major Case Management (MCM), Part VI's and Undercover Operations.

#### Major Case Management Support Unit

Using Evidence and Reports (E&R) III as the primary tool, the MCM Support Unit provides the necessary support for the effective management of the investigation up to and including court document preparation and disclosure.

#### Community Outreach Program

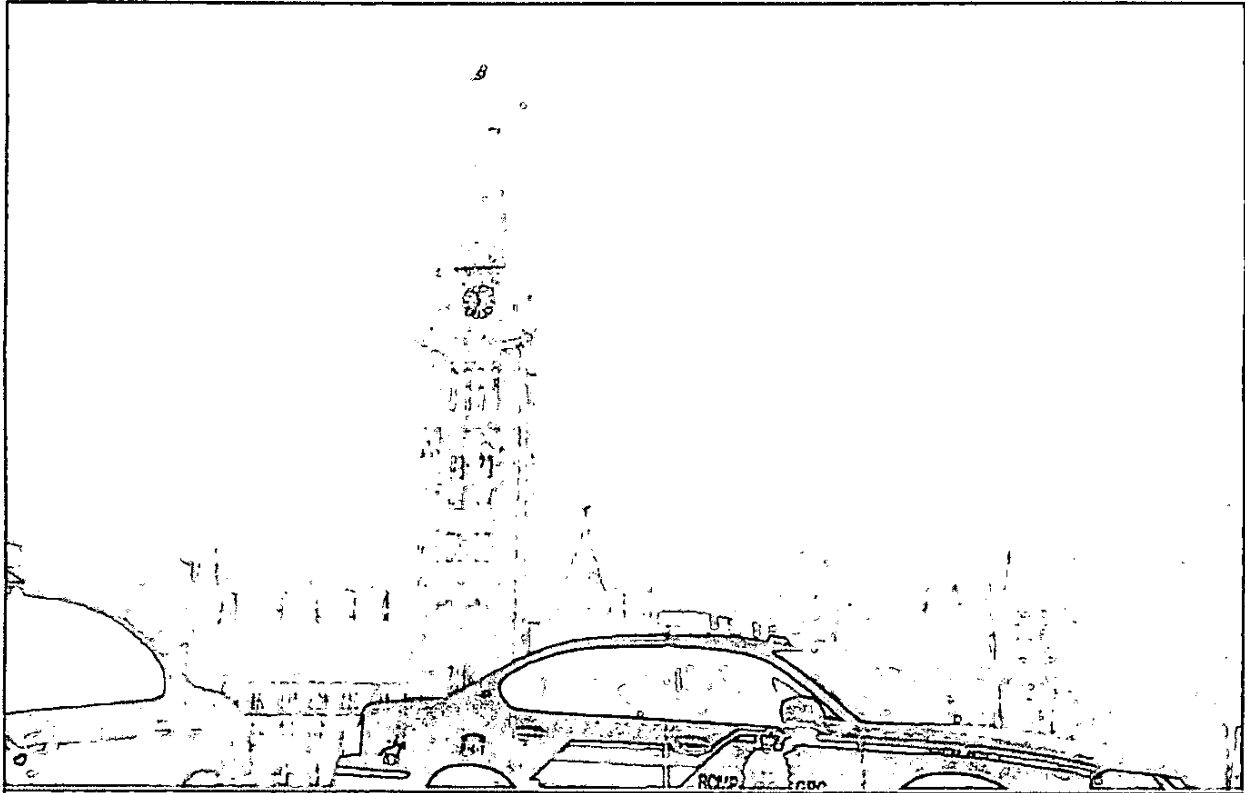
Working in conjunction with all partner agencies, provides a method for effectively sharing information, providing education on current and pending issues (relating to national security and terrorism) affecting the communities we serve. This includes creating and maintaining Community Consultative Groups, providing training with law enforcement, government and non-governmental agencies that have a role or service that is or would be affected by terrorism.

#### Analyst Program

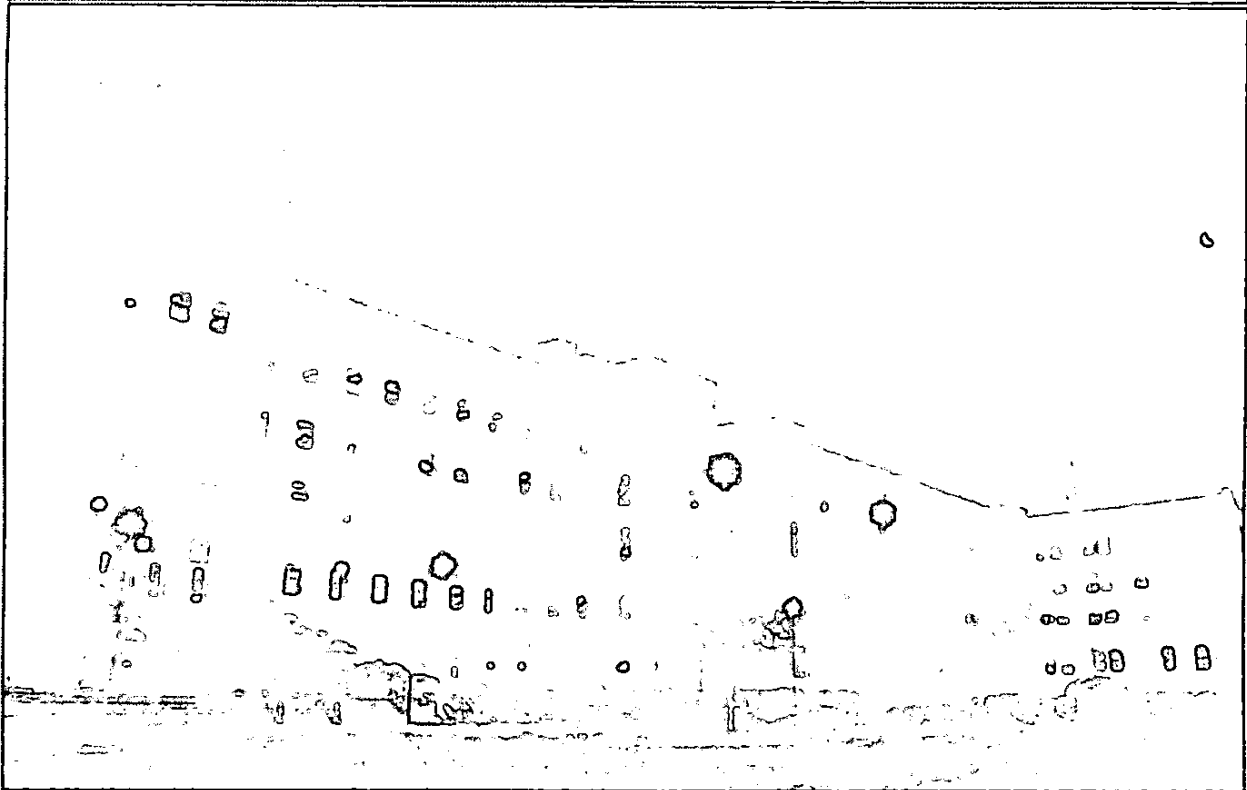
The Analyst's role is the research, review and assessment of incoming information (multi-source), and then creating intelligence (through an analytical process) that can be applied to the investigations. At the unit level this is normally Tactical Analysis (what is happening now or in the very near future) but may include Strategic (the big picture, long term). Some Analysts are assigned to one specific project and others may be multi-tasked through the Operations NCO.

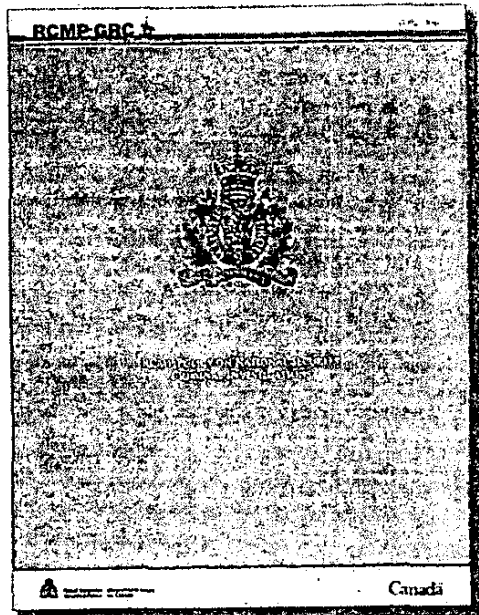
#### Source Development Unit (SDU)

Supports INSET enforcement operations by recruiting Human source assets, assists in major operations, provides training and support to Divisions on Human source issues.



## Chapter Four — The Governance Model





This chapter presents the governance structure for National Security (NS) criminal investigations.

#### Key Elements

*NS criminal investigations will be centrally controlled by:*

- Increasing National Headquarters' capacity to monitor and oversee all NS criminal investigations;
- Delineating to the Assistant Commissioner National Security Criminal Investigations (NSCI) final authority over all NS criminal investigations;
- Delineating to the Commanding Officers (COs) responsibility for conducting NS criminal investigations within their respective Divisions in compliance with Ministerial Directives, RCMP priorities and policy;
- Ensuring that the NS Program has sufficient human resources, with the training and tools required, to effectively investigate NS criminal investigations;
- Creating a NS Strategic Operations Council to support the Assistant Commissioner NSCI in executing his responsibility with respect to the NS program,
- Completing a revised NS policy framework and its periodic review.

#### Background

Commissioner Zaccardelli directed the RCMP to implement Justice O'Connor's recommendations and central control of NS criminal investigations.

The goal of central control is to create a governance structure for NS criminal investigations that fits with the realities of the current environment. To paraphrase Justice O'Connor's Part I report, centralization will be valuable in supporting the effectiveness and propriety of NS criminal investigations. It will ensure that relevant information is shared internally, assist in discerning trends, and facilitate briefing the Minister of Public Safety, when necessary. Also, it will ensure that persons involved in NS criminal investigations adhere to the RCMP's mandate, follow Ministerial Directives and policy, respect individual liberties, and share information appropriately.

The successful implementation of central control of the RCMP's NS criminal investigations depends on how central control is operationalized. This could be done in a number of ways encompassing different structures, processes and models.

The governance structure to implement central control (outlined below) has been the product of extensive consultation and discussion at a variety of levels across the RCMP.

The rationale for the centralization of NS criminal investigations is often cited. Namely, NS criminal investigations are unique:

- They are often integrated investigations with links to other agencies in the security and intelligence community, are preventative in nature and are subject to Ministerial Directives by virtue of their high profile and sensitivities;
- The human rights issues, privacy concerns and international dimensions involved may create risk to the RCMP, the Government and the people of Canada that must be centrally mitigated;
- Their complexity and international scope requires a national perspective, lead and response that is beyond any one part or Division of the RCMP;
- There is a critical requirement that they stay within the RCMP's mandate, an objective best monitored from HQ;
- They are alone in attempting to prevent and/or investigate incidents where the state itself (and not necessarily any citizen in particular) is the direct target, demanding a nationally-led effort to conduct these investigations;

#### National Security Criminal Investigations — Orientation Guide

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

Protected "A"

- > There is a demand for enhanced accountability to government and to the public requiring centralized leadership; and,
- > The additional scrutiny on these investigations requires significantly more central effort and resources to support disclosure and review than other major investigations.<sup>1</sup>

Centralization of NS criminal investigations is consistent with the governance models of our domestic and international security and intelligence partners.

Together, these factors remain the root rationale behind greater centralized control.

One of the RCMP's greatest strengths, even in an area that needs as much centralization as NS criminal investigations, is the ability of the RCMP's personnel to develop on-the-ground knowledge of communities and to exercise their individual responsibilities to conduct investigations.

As Justice O'Connor's Part I Report states: "The RCMP should maintain its current approach to centralized oversight of national security investigations."<sup>2</sup> Further, the report highlights the "important steps [that] have been taken in recent years by both the RCMP and the Solicitor General, the minister responsible for the RCMP, to provide for greater centralization and oversight of RCMP national security investigations."<sup>3</sup>

The crux of Justice O'Connor's comments on centralization is that there must be greater vigilance and control exercised on NS criminal investigations. Some might differ on where in the chain of command that increased vigilance and control must occur, but the truth of the matter is – and the core principle underlying this governance framework is – that *it must occur at all levels of the RCMP*.

Therefore, it was decided that NS criminal investigations would operate under a governance structure that allows them to remain responsive to the communities where such investigations take place, while retaining and augmenting the critical elements and levers of national control that have developed in recent years.

This structure will demand increased vigilance at the Unit, Division and HQ level. At the same time, it will place a greater onus on the Divisions to consult and keep HQ informed on NS criminal investigations while enhancing

the authority of National Headquarters to direct NS criminal investigations when necessary.

To that end, roles, responsibilities, accountability and authorities will be clarified throughout the chain of command to ensure the effective and proper conduct of NS criminal investigations. This has been done in the governance structure that follows based on deliberations between Divisions, NSCI and the Operations Management Board.

### Governance Structure

This new framework will implement Justice O'Connor's recommendations and central control of NS criminal investigations by:

- > Increasing the capacity of NSCI to monitor, supervise and direct NS criminal investigations, when necessary;
- > Increasing responsibility and accountability at all levels throughout the program to ensure compliance with policy and ministerial directives especially as it pertains to information sharing and mandate;
- > Increasing the capacity of Integrated National Security Enforcement Teams (INSETs) / National Security Enforcement Sections (NSESs) / Source Development Units (SDUs) to undertake investigations;
- > Increasing the capacity of Divisions to manage investigations; and,
- > Improving NS training and setting national NS training standards.

Accountability and responsibility for all aspects of the NS program including NS criminal investigations ultimately rests with the Assistant Commissioner NSCI.

To that end, NSCI at National HQ will monitor NS criminal investigations and will provide oversight, guidance and direction where appropriate to the Divisions.

The Commanding Officer (CO) is accountable and responsible for overseeing, managing and directing NS criminal investigations within his/her Division and for ensuring adherence to Ministerial Directives, RCMP priorities and policy. The Division will also ensure a local

1 This is in part because of the disclosure burden placed on investigators by R vs Stinchcombe and the need to utilize Section 37 and Section 38 of the Canada Evidence Act to protect sensitive information, and the involvement of multiple agencies with disclosure interests at stake.

2 The Commission of Inquiry Into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Government of Canada, 2006), p. 327.

3 Ibid, p. 378.

#### National Security Criminal Investigations – Orientation Guide

24

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

perspective is provided, advise on potential impact on other programs/priorities, task operational support as necessary, and contribute to the "rich picture" of NS-related criminal activity within the division.

Under this governance framework, CROPs officers will assume a more active role in overseeing NS criminal investigations to ensure compliance with Ministerial Directives, RCMP policy, and priorities and to ensure that NSCI at National HQ is appropriately consulted and informed on all aspects of investigations, especially any that may give rise to media coverage or controversy.

To support this reemphasized role, it is proposed that six new officer positions dedicated solely to NS criminal investigations be created (in A, C, E, and O Divisions, the NW and Atlantic Regions). This proposed position will be detailed further in the NS Criminal Investigations Structural Template.

A NS Strategic Operations Council will be created to support the Assistant Commissioner NSCI in the execution of his/her responsibilities for NS criminal investigations. The Council's role will be to:

- > Consult on select major issues and National Tactical Criminal Investigative priorities;
- > Provide a broader view of strategic issues related to NS criminal investigations;
- > Form an advisory group to assist in strategic NS decision-making on issues impacting partners; and,
- > Provide a forum for the discussion of NS criminal investigation issues that affect provinces and partners.

The Council will serve to enhance the RCMP's provincial and municipal partnerships and reinforce that, though NS criminal investigations are nationally controlled, they are conducted locally.

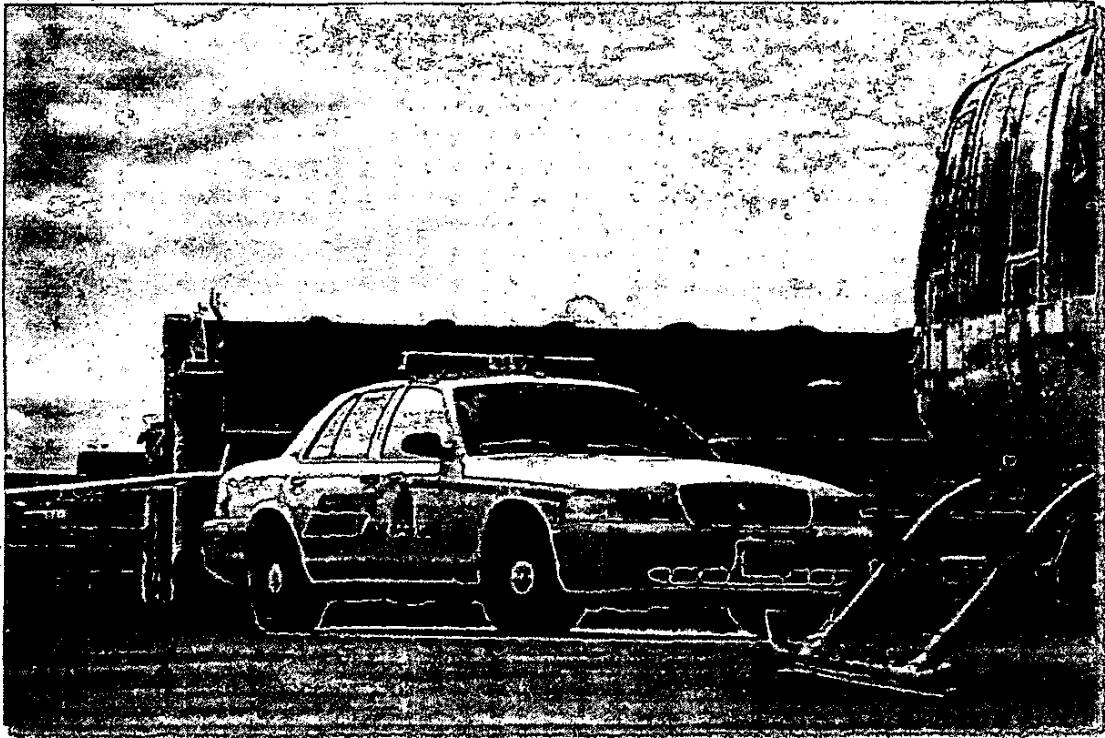
### Governance Structure Details

#### **Role of HQ-NSCI**

NSCI at National HQ will add value and be an integral part of operations. As opposed to being a policy centre peripheral to operations, NSCI at National HQ will be responsible for oversight, and direction when necessary, of NS criminal investigations.

Practical elements of HQ's role under central control will include:

- > Monitoring every NS file;
- > Staying current on their progress through reporting from CROPs officers;
- > Providing guidance, tasking, and direction to the CROPs officers in writing, particularly with regard to information sharing, sensitive sectors, NS-related foreign travel and relations with foreign agencies;
- > Providing input on NS-related elements of the Commissioner's Performance Agreements with Deputy Commissioners;
- > Verifying that the Division has adequate systems and controls in place to ensure compliance with RCMP policy;
- > Identifying high-risk activities for Divisions;
- > Administering domestic and international partnerships;
- > Controlling foreign information sharing;
- > Conducting extra-territorial investigations that do not have a clear venue to a geographic location in Canada, and continuing to further develop the capability and capacity to do so;
- > Coordinating disclosure of information to Judicial Inquiries and civil litigation proceedings related to NS criminal investigations;
- > Coordinating work with civilian review mechanisms related to NS criminal investigations;
- > Coordinating and supporting disclosure responsibilities to cases before the Court, especially with respect to Section 38 of the *Canada Evidence Act* claims;
- > Establishing clear and comprehensive policies for all facets of NS criminal investigations;
- > Providing the national analysis of trends, "connecting of dots," and communication of such information to NS personnel and integrated partners;
- > Outlining best practices with regard to NS criminal investigations, standards, human resource strategies, training, information systems, and technology in consultation with other policy centres;
- > Increasing the number of knowledgeable and experienced personnel in the NS program;
- > Increasing HQ's capacity to support NS criminal investigations nationwide; and,
- > Improving NS training.



### **Role of Divisions**

Commanding Officers (COs) are responsible and accountable for overseeing NS criminal investigations and their adherence to Ministerial Directives, and RCMP priorities and policy within their respective Divisions. Recognizing the traditional role and responsibilities of COs, they will be responsible for ensuring there are adequate controls and procedures in place to ensure:

- > Compliance with all policy, especially as it relates to Ministerial Directives, and information sharing and mandate
- > The mitigation of the risks posed by high-risk activities;
- > The implementation of quality assurance processes to monitor NS high-risk activities;
- > Managerial reviews, internal audits and evaluations take place; and,
- > Sufficient divisional resources are dedicated to investigate NS criminal investigations, in accordance with RCMP's mandate and priorities.

CROP's officers will be responsible and accountable for the operational management of NS criminal investigations within their respective divisions. As part of that responsibility, CROP's officers will:

- > Conduct NS criminal investigations in a bias-free manner, in keeping with the RCMP's mandate and core values;
- > Comply with Ministerial Directives and RCMP policy, particularly with regard to information sharing, sensitive sectors, NS-related foreign travel and relations with foreign agencies;
- > Provide oversight and direction to INSET, SDU and NSES personnel, under the direction of NSCI, where applicable;
- > Conduct NS criminal investigations in keeping with the principles of Major Case Management;
- > Keep NSCI at HQ informed of all NS criminal investigations and appropriately consulted;

- > Comply with direction from NSCI on NS criminal investigations;
- > Contribute to the development of the national picture of NS-related criminal activity by providing input from their Division;
- > Advise NSCI at HQ of the impact of NS criminal investigations on other Divisional priorities and programs;
- > Conduct critical incident management with respect to crisis and consequence management where the RCMP is the police service of jurisdiction;
- > Engage with partner agencies, particularly municipal and provincial police services, and NSCI to develop relationships and networks for conducting effective and successful NS criminal investigations;
- > Comply with NS criminal investigations-related training requirements;
- > Lead engagement with citizens and communities particularly affected by NS criminal investigations (e.g., Citizen Advisory Groups);
- > Monitor high-risk activities through Quality Assurance processes; and,
- > Ensure local perspective is provided.

As stated earlier, the enhanced role for the Division to provide oversight and ensure central control of NS criminal investigations would likely require six new positions dedicated solely to the management of NS criminal investigations. It is envisioned that: the four Divisions with INSETs would each receive one position; the Northwest and Atlantic Regions would each receive one position to service the region.

Personnel in these new positions would support the CROPs officers in the execution of their responsibility for divisional management of NS criminal investigations and reporting to NSCI.

Dedicating an officer solely to NS criminal investigations would increase the capacity of Division leadership to manage these types of investigations. Considering the scope of this task, it is expected that increased resources, in addition to this officer, would be required to effectively implement this framework.

An additional officer dedicated to NS criminal investigations would have the added benefit of allowing INSET, NSES and SDU Commanders to focus, as much as possible, on day-to-day operations. They would also facilitate senior-level linkages between Divisions, NSCI and provincial/municipal partners.

They would operate within the Divisional command structure and report directly to their respective CROPs officer.

These officers would be responsible for INSET/NSES units within their respective areas of responsibility, including all source development and national security-related threat assessment units.

#### **Human Resources**

The Deputy Commissioner Human Resources (DCHR) is developing a Human Resources strategy, in partnership with NSCI and Corporate Management & Comptrollership, to meet the short-term needs of the immediate reallocation of personnel.

The longer-term human resources requirements to sustain the NS criminal investigations program will be met by the current model in place.

## Defining National Security Criminal Investigations

The Integrated National Security Enforcement Teams (INSETs) and National Security Enforcement Sections (NSES) undertake NS criminal investigations into the following:

- > Terrorist activities as defined in the anti-terrorism provisions of the *Criminal Code* (<http://laws.justice.gc.ca/en/showdoc/c/c-46/bo-ga-1-11-1/cn#anchorb-ga-1-11-1>) — i.e. the *Anti-Terrorism Act*;<sup>4</sup>
- > Any offence arising out of a threat to the security of Canada as defined in Sec. 2 of the *CSIS Act* (<http://laws.justice.gc.ca/en/showtdm/c/c-23>), which includes:
  - > espionage or sabotage that is against Canada or is detrimental to the interests of Canada;
  - > foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;
  - > activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, or religious or ideological objective within Canada or a foreign state; and,
  - > activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada;
- > An offence where the victim is an Internationally Protected Person as per Section 2 of the *Criminal Code* or designated per Section 17 of RCMP regulations;
- > The unlawful release of sensitive or classified information dealing with NS, including information that could constitute a breach of the *Security of Information Act* or similar provisions in other federal statutes and the *Criminal Code of Canada*, or information originating from CSIS, other domestic originators of intelligence, or our foreign partner agencies in this area; and,

- > Terrorist financing investigations under the provisions of *The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*.

For the purposes of this governance framework, these investigations and all other operational files managed by INSET/NSES units as well as all NS-related threat assessments will be under central control of NSCI:

NS criminal investigations aim to reduce the threat of criminal terrorist activity in Canada and abroad through preventing, disrupting, detecting, investigating, and gathering evidence to support prosecuting those involved in NS-related criminal acts. Specifically, these investigations target offences related to: terrorist activities as defined in the anti-terrorism provisions of the *Criminal Code*; terrorist financing activities as defined by *The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*; offences arising out of conduct constituting threats to the security of Canada as defined by *The CSIS Act*; offences against Internationally Protected Persons; and, unlawful release of sensitive or classified information.

NS criminal investigations represent a subset of the RCMP's larger NS activities. In addition to NS criminal investigations (which are often related to other NS activities), the larger envelope of National Security also includes Protective Policing designated protected persons and internationally protected persons, elements of the Integrated Border Enforcement Teams (IBET), the Coastal and Airport Watch Program, and the Canadian Air Carrier Protective Program (CACPP). In addition, key operational support activities to NS criminal investigations are provided by a wide range of other program areas, including: Special I, Special O, Tech Crime, Air Services, Critical Incident Program (including Emergency Response Teams), Witness Protection Program, Forensic Science Services, CPIC, etc. For the purposes of NS criminal investigations governance, NS criminal investigations also includes liaison and outreach functions related to national security.

<sup>4</sup> This remains an active area of the law and the RCMP is mindful of the impact of recent judicial decisions and their impact on future national security investigations.





## Chapter Five — Departmental Security

In your role within the National Security Program, you will be dealing primarily with investigations that are Protected "B", Protected "C", Confidential, Secret and Top Secret (most detachments and units work in the Protected realm, "A", "B" and "C").

In light of the security rating of these investigations, you will have to change the way and manner that you handle information:

- > Sensitive information cannot be sent over regular faxes or through e-mails.
- > Cell phones and personal digital assistants (PDAs) cannot be used to share information or talk about sensitive investigations.
- > Lap tops are generally not permitted for use on our investigations.
- > Sensitive files cannot be taken out of the office.
- > You cannot talk about the sensitive investigations you work on with friends or family (this includes police officers not assigned to the unit).
- > Secret and Top Secret information cannot be shared with law enforcement officials or persons that do not have the appropriate security clearance, or that do not have a "need to know" the information.

Upon your arrival, please familiarize yourself with the RCMP Security Handbook ([http://infoweb.rcmp.gc.ca/to/dsb/handbook/handbook\\_e.pdf](http://infoweb.rcmp.gc.ca/to/dsb/handbook/handbook_e.pdf)).

### No Wireless Devices in Secure Zones

**USE OF WIRELESS DEVICES IN SECURITY ZONES WHERE TERMINALS ARE PROCESSING PROTECTED C, SECRET OR TOP SECRET MATERIAL IS PROHIBITED.**

Laboratory tests easily demonstrated that information emitted by video monitors can inadvertently be re-transmitted far beyond the controlled perimeter by wireless electronic devices located nearby.

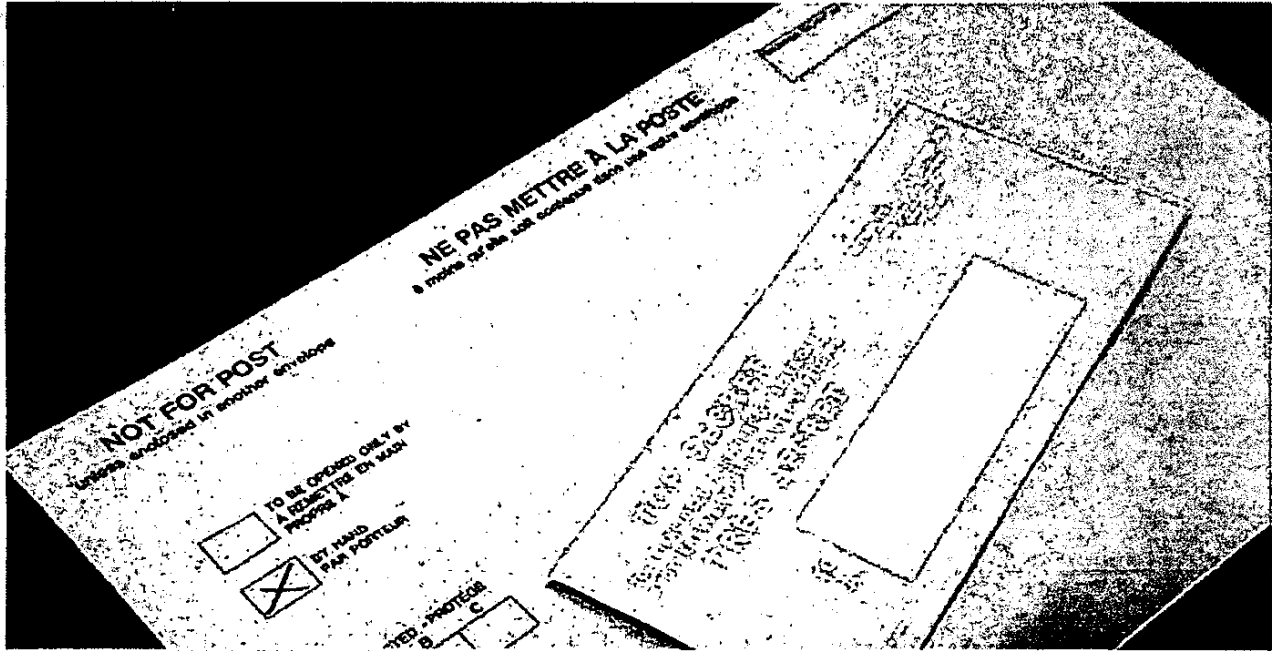
The cost of technology used to perform an interception has steadily declined and apparatus required are more sophisticated than ever, making it more attractive to subscribe to this activity.

To pro-actively prevent unintentional interception of RCMP extremely sensitive or classified information, it is imperative that the use of radio frequency transmitting devices such as: PDAs, wireless LANs, cellular telephones, Blackberries, etc., be banned from security zones where terminals are processing Protected "C", Secret or Top Secret information unless the technology has been approved by Departmental Security Branch.

National Security Criminal Investigations - Orientation Guide

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning this information, please contact the originator of the document.

20



## Chapter Six — Document Classification

Most RCMP information is protected or classified to ensure its safe handling and appropriate storage. When determining whether to classify or protect new information/intelligence the following injury tests must be applied. The determined level dictates how that information is stored, including the appropriate data system, how it is shared and how it is transported.

### **Protected information includes:**

- > All sensitive information (Classified and Protected) must be marked with the level of sensitivity in the top right corner, of every page, in each document.
- > Do not Classify or Protect information to: conceal violations of law; conceal inefficiency or administrative error; avoid embarrassment; or restrain competition.
- > Written agreements, noting the required safeguards, must be entered into when sharing sensitive information outside the Government of Canada.

### **For more information regarding information security, please visit the following Infoweb links:**

[http://infoweb.rcmp-grc.gc.ca/to/dsb/oas/definitions\\_c.htm](http://infoweb.rcmp-grc.gc.ca/to/dsb/oas/definitions_c.htm)

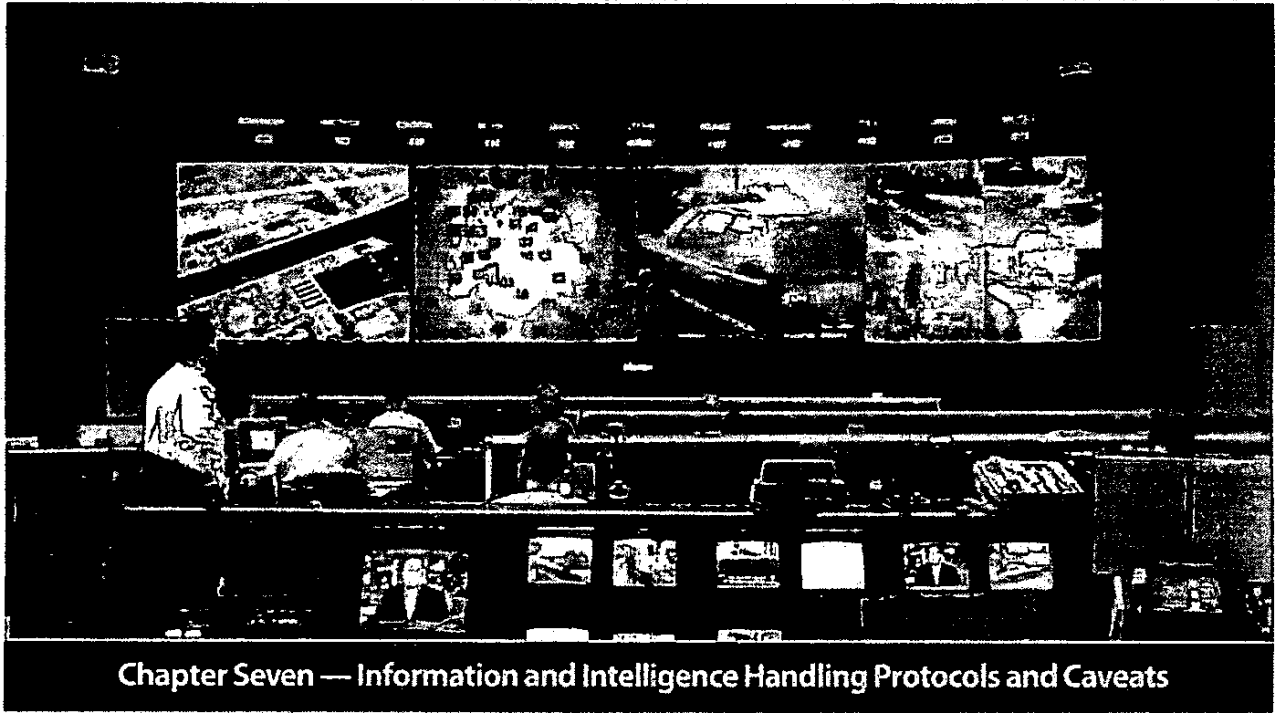
<http://infoweb.rcmp-grc.gc.ca/english/rcmpmanuals/am/xi/amX1-1/amX1-1.htm>

## Classify or Protect Your Sensitive Information

<b>Classify: National Interest Information</b>	<b>Protect: Non-National Information</b>
<p><b>Confidential:</b> Compromise is expected to cause injury to the National Interest. Most of the information meriting classification should fall in this level.</p>	<p><b>Protected A:</b> Routine information of low sensitivity that requires protection eg. routine complaints, general information.</p>
<p><b>Secret:</b> Compromise is expected to cause serious injury to the National Interest.</p>	<p><b>Protected B:</b> Particularly sensitive information that requires more stringent protection, e.g. medical descriptions, organized crime intelligence, drug operations.</p>
<p><b>Top Secret:</b> Compromise is expected to cause exceptionally serious injury to the National Interest.</p>	<p><b>Protected C:</b> Extremely sensitive information requiring special stringent safeguards, e.g. information concerning life threatening situations.</p>
<p><b>Classified information includes:</b></p> <ul style="list-style-type: none"> <li>• information on federal-provincial relations, international affairs, defense, or the economic interests of Canada;</li> <li>• advice and recommendations connected with the above information;</li> <li>• information on investigations into threats to the security of Canada;</li> <li>• information under the Cabinet Paper System; and</li> <li>• other Cabinet Confidences, that contain information sensitive in the national interest.</li> </ul> <p>Classified Information is information related to the national interest, that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act and the compromise (unauthorized disclosure, destruction, removal, modification or interruption) of which could reasonably be expected to cause injury to the national interest (for examples of national interest and other sensitive information see <a href="http://infoweb.rcmp-grc.gc.ca/english/rcmpmanuals/am/xi/amXI-1/a11-1-3/a11-1-3.htm">http://infoweb.rcmp-grc.gc.ca/english/rcmpmanuals/am/xi/amXI-1/a11-1-3/a11-1-3.htm</a>).</p>	<p><b>Protected information:</b> Information related to other than the national interest, that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise (unauthorized disclosure, destruction, removal, modification or interruption) of which could reasonably be expected to cause injury outside the national interest, or when its integrity or availability warrants safeguarding.</p> <p><i>Protected information includes:</i></p> <ul style="list-style-type: none"> <li>• law enforcement investigations;</li> <li>• the safety of individuals;</li> <li>• the government's competitive position;</li> <li>• research and testing procedures;</li> <li>• business information from a third party;</li> <li>• solicitor-client privilege;</li> <li>• information from other levels of government (when given in confidence);</li> <li>• medical records;</li> <li>• individual members of the public or federal employees; and</li> <li>• information that other laws, such as the Income Tax Act, prohibit disclosing.</li> </ul>

### National Security Criminal Investigations — Orientation Guide

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.



## Chapter Seven — Information and Intelligence Handling Protocols and Caveats



### Sharing of Information

The RCMP is committed to sharing intelligence with its partners. Given the nature of national security criminal investigations, there is a requirement to safeguard the manner in which the sharing takes place. The policies and processes for the sharing and exchange of information and criminal intelligence with external partners differ from other areas within the RCMP.

#### General

- Only the originator of a document can reclassify it.
- Confidential, Secret and Top Secret information cannot be shared with any person that does not have the appropriate security clearance, or that does not have a "need to know" the information.
- All investigational correspondence leaving NSCOB must have the signature/approval of the OIC or designate.
- Information to be shared with foreign agencies must be transmitted through NSCOB (Ottawa). INSET and NSES units must forward these types of requests through NSCOB.
- The Director General, National Security Criminal Operations is the **SOLE AUTHORITY** for determining whether or not criminal intelligence and/or information related to National Security may be shared with foreign external partners.
- The Director General, National Security Criminal Investigations will centrally coordinate all national security criminal investigations through monitoring, supporting and tasking.

## Caveats

In addition to the classification and protection of documents, they will often have an additional caveat which must be respected. It is common, for example, to see the caveat, particularly on documents from the United States, Law Enforcement Use Only'. The classification of the document may be quite low and the information can be widely shared in law enforcement but could not, for example, be used in a presentation to a high school class.

Caveats must be included on all national security-related information shared within and outside the RCMP. A common caveat is the designation Third Party Rule (or more correctly Third Party Information). Included in all *Classified* or *Protected* outgoing messages and documents being passed to other domestic and foreign law enforcement agencies/departments is the following caveat (<http://infoweb.rcmp-grc.gc.ca/rcmpmanuals/eng/om/12/om12-3/om12-3.htm>):

"This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Branch, RCMP."

All information and criminal intelligence that was collected from sensitive sources or where further disclosure may reveal RCMP sources, operational methodology or investigative techniques, and thereby potentially engage the provisions of the Security of Information Act designed to prevent or deter injury to national security as the result of the disclosure of special operational information, must include the following caveat in addition to the caveat stated in sec. 7.2 of the RCMP Policy on National Security Criminal Investigations.

"This document may be subject to mandatory exemption under the Access to Information and Privacy Acts. If access is requested under this legislation, the decision to disclose will not be made without prior consultation with the Departmental Privacy Coordinator of the Royal Canadian Mounted Police (RCMP). This document may constitute special operational information as defined in the Security of Information Act. This information may also be protected by the provisions of the Canada Evidence Act (CEA). The RCMP National Security Program may take all steps pursuant to the CEA or any other legislation to protect this information from production or disclosure, including the filing of any necessary notices with the Attorney General of Canada."

All internal correspondence that contains national security-related information must include the following caveat:

"This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is provided to your section/unit and should not be disseminated, in whole or in part, without the prior consent of the originator. This document will not be declassified without the written consent of the originator. This document may constitute "special operational information" as defined in the Security of Information Act. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If you cannot apply these guidelines, please read and destroy this document. Failure to comply with this caveat will constitute a breach of RCMP policy and federal legislation. For any enquiries concerning the information, please contact the originator of the document."

The following is the standard caveat for all *Protected* outgoing correspondence, messages and documents being passed to another Canadian or foreign law enforcement agency or investigative agency (<http://infoweb.rcmp-grc.gc.ca/english/rcmpmanuals/am/xi/amXL-1/a11-1-5/b11-1-5.htm>):

"This document is the property of the Government of Canada. It is loaned to your agency on the understanding that it is not to be further disseminated without the consent of the originator. Distribution within your agency is to be done on a need-to-know basis. The document is to be protected in accordance with normal safeguards for law enforcement information."

### National Security Criminal Investigations — Orientation Guide

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

33

Protected "A"

## Technology

### **ROSS Email — ENTRUST**

You will need an Entrust key (Form 5098) in order to send Protected "B" information via e-mail on ROSS (Groupwise). Failing to do so consists of a breach of security and can have serious repercussions.

### **Secure Fax**

The Secure Fax is for sending information that is Protected "B" or "C" and for information classified Confidential, Secret and Top Secret. There is a log book to record all outgoing faxes.

### **Classified Environment Computer System Email (SCIS/SPROS)**

Information rated up to Top Secret can be sent securely over the Classified Environment Computer system Groupwise e-mail.

### **STU III Phone (Secure Telephone Unit)**

The STU Phone is for conversations about information that is Secret or Top Secret (Requires both persons in the conversation to have a STU phone).

### **Encrypted Radios**

Conversations up to Top Secret when on an encrypted channel.

### **Hardline Telephones**

Caution should be exercised when having any conversation related to an investigation.

### **Cell Phones**

Cell phones should never be used to discuss information that is sensitive.

### **Requests to RCMP LO's (Liaison Officer's)**

There are many times in an investigation when information is requested or is to be passed on to a foreign government. This is done through the Liaison Officer (LO) program. The RCMP maintains LO's in many of Canada's Embassy and Consular offices around the world.

All requests to LO's must be made through NSCOB to ensure central control. This is usually done through a Secure Fax (Form 2875). In some countries technology is very basic and a simple request may take between six and 12 months.

Responses to requests from foreign government agencies are handled in the same fashion. Please quote the foreign agency file number in your header.

All outgoing correspondence must have the approval of the OIC or his designate.

## **Briefing Notes**

All investigations that may be of interest to the media, affect the Provincial or Federal government, embarrass the government or the RCMP, impact border security operations or international relations or have a national security nexus, must be reported on, in a timely fashion, by way of a Briefing Note.

After initially reporting on an investigation through a Briefing Note, updates should be provided to clarify any new developments in the continuing investigation.

## **Security of Information Act**

The *Security of Information Act (SOIA)* was introduced in December 2001, as part of Bill C-36 of the *Anti-Terrorism Act* and replaced the *Official Secrets Act (OSA)*. The Act permanently binds all levels of RCMP employees who have access to special operational information to secrecy by respecting information they have become knowledgeable about during the course of their employment.

A newly-created unit within the RCMP's Departmental Security Branch is responsible for overseeing the implementation of the provisions of the SOIA in the RCMP. The unit's overall objective is to sensitize the RCMP membership to the SOIA and educate employees of their statutory responsibilities and possible penalties for non-compliance under the Act.

It is the Section Head/Supervisor/Team Leader's responsibility to identify if the people working within their area deal with "special operational information/techniques". If so, they should be identified as people bound to permanent secrecy. Individuals responsible for these areas are asked to assist in sensitizing anyone working with this information to the Act and educating employees about their statutory responsibilities as well as the possible penalties for non-compliance.

What this means for employees: Anyone who, during the course of their duties, has become knowledgeable of special operational information within a Department covered by the *SOIA* is legally bound to permanent secrecy. Anyone covered under the *SOIA* who communicates special operational information without authority to do so and does so knowingly or not, is guilty of an offence under the *Act* and subject to prosecution with a maximum imprisonment of 14 years. These provisions apply both during and after service with the Government of Canada. More information on the Security of Information Act and Security Requirements and Procedures can be found on the RCMP Info Web under *Security*.



## Chapter Eight — Ministerial Direction on National Security

Note: the Solicitor General of Canada is now known as the Minister of Public Safety

### **Ministerial Direction National Security Responsibility and Accountability**

- A. This direction outlines the responsibilities and accountabilities of the Solicitor General of Canada and the Commissioner of the Royal Canadian Mounted Police (RCMP) in matters related to RCMP investigations that fall under subsection 6(1) of the *Security Offences Act* and investigations related to a terrorist offence or terrorist activity, as defined in section 2 of the *Criminal Code of Canada*, as amended by the *Anti-terrorism Act*.

### **Responsibilities**

- B. In relation to the RCMP, the duties, powers and functions of the Solicitor General of Canada extend to and include all matters over which Parliament has jurisdiction. As per subsection 5(1) of the *RCMP Act* (<http://laws.justice.gc.ca/en/R-10/index.html>), the control and management of the RCMP, and all matters connected therewith, is the responsibility of the Commissioner of the RCMP, under the direction of the Solicitor General.
- C. The accompanying Ministerial direction sets out the principles and guidelines for RCMP investigations with respect to matters that fall under subsection 6(1) of the *Security Offences Act* and investigations related to a terrorist offence or terrorist activity, as defined in section 2 of the *Criminal Code of Canada*.
- D. It is the responsibility of the Commissioner of the RCMP to ensure that operational policies are in place to guide members. It is also the responsibility of the Commissioner to ensure that all investigations with respect to matters that fall under subsection 6(1) of the *Security Offences Act*, and investigations related to a terrorist offence or terrorist activity, as defined in section 2 of the *Criminal Code of Canada*, be centrally coordinated at RCMP National Headquarters. Such central coordination will enhance the Commissioner's operational accountability and in turn, will enhance ministerial accountability, by facilitating the Commissioner's reporting to the Minister.

National Security Criminal Investigations — Orientation Guide

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

35

**Accountabilities**

- E. The Minister is accountable to the Parliament of Canada for the RCMP. The Commissioner, in turn, reports to and is accountable to the Minister.
- F. As part of the accountability process, the Minister will be advised or informed regarding certain RCMP investigations with respect to matters that fall under subsection 6(1) of the *Security Offences Act*, and investigations related to a terrorist offence or terrorist activity, as defined in section 2 of the *Criminal Code of Canada*. The Commissioner of the RCMP shall exercise his judgment to inform the Minister of high profile RCMP investigations or those that give rise to controversy.

[Original Signed by the Solicitor General of Canada on 2003-11-04]

**Ministerial Direction National Security Related Arrangements and Cooperation**

- A. This direction establishes the process for the Royal Canadian Mounted Police (RCMP) to follow when entering into an arrangement with foreign security or intelligence organizations for the purpose of performing its duties and functions with respect to matters that fall under subsection 6(1) of the *Security Offences Act*, and those related to a terrorist offence or terrorist activity, as defined in section 2 of the *Criminal Code of Canada*. The RCMP may, with the Minister's prior approval, enter into a written or oral arrangement, or otherwise cooperate, with foreign security or intelligence organizations. This direction is in addition to the *Ministerial Directive on RCMP Agreements*, dated April 5, 2002.
- B. The Commissioner will manage such arrangements or cooperation subject to any conditions imposed by the Minister.
- C. This direction does not pertain to arrangements and cooperation with foreign law enforcement agencies or organizations.

D. The following guidelines will be adhered to when entering into an arrangement:

- Arrangements may be established and maintained as long as they remain compatible with Canada's foreign policy towards the country or international organization in question, including consideration of that country or organization's respect for democratic or human rights, as determined in ongoing consultations with the Department of Foreign Affairs and International Trade (DFAIT);
- Arrangements may be established and maintained when such contacts are in the interests of the security of Canada, further to the RCMP investigations related to subsection 6(1) of the *Security Offences Act*, and section 2 of the *Criminal Code of Canada*; and,
- Arrangements will respect the applicable laws and practices relating to the disclosure of personal information.

E. On matters related to threats to the security of Canada, as defined by the *Canadian Security Intelligence Service (CSIS) Act*, CSIS is the lead agency for liaison and cooperation with foreign security or intelligence organizations.

F. A written arrangement will clearly establish its purpose and obligations, including the applications of privacy and access to information legislation.

G. The RCMP will maintain records relating to foreign arrangements, including a written record of the terms and understandings of oral arrangements. The RCMP will indicate its means of periodic evaluation or audit of the arrangement, and the provisions for its cancellation. The Commissioner will report annually to the Minister on the status of the RCMP's written and oral arrangements with foreign security or intelligence organizations.

H. Should any potentially controversial issue arise from such arrangements, the Commissioner shall advise the Minister in a timely fashion.

[Original signed by the Solicitor General of Canada on 2003-11-04]



**Ministerial Direction National Security  
Investigations in Sensitive Sectors**

- A. This direction will guide the investigations of the Royal Canadian Mounted Police (RCMP), with respect to matters that fall under subsection 6(1) of the *Security Offences Act*, and investigations related to a terrorist offence or terrorist activity, as defined in section 2 of the *Criminal Code of Canada*, as they relate to sensitive sectors of Canadian society.
- B. Recognizing that there are no sanctuaries from law enforcement, special care is required with respect to RCMP investigations conducted with respect to matters that fall under subsection 6(1) of the *Security Offences Act*, and investigations related to a terrorist offence or terrorist activity, as defined in section 2 of the *Criminal Code of Canada*, which have an impact on, or which appear to have an impact on, fundamental institutions of Canadian society. Primary among these institutions are those in the sectors of academia, politics, religion, the media and trade unions.
- C. With regards to university or post secondary campuses, in particular, it is paramount that the investigations undertaken by the RCMP do not impact upon the free flow and exchange of ideas normally associated with an academic milieu. Furthermore, the activities of the RCMP shall not adversely affect the rights or freedoms of persons associated with academic institutions.
- D. It is the responsibility of the Assistant Commissioner, National Security Criminal Investigations at the RCMP National Headquarters, or in his/her absence, his/her appointed designate, to approve all RCMP investigations involving these sensitive sectors of Canadian society.

[Original signed by the Solicitor General of Canada on 2003-11-04]



**National Security Criminal Investigations — Orientation Guide**

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

37



## Chapter Nine — Software, Data Systems and Access

### **Records Management System**

The Records Management System (RMS) used by the RCMP for national security criminal investigations is called SPROS (Secure Police Reporting and Occurrence System).

Within 24 hours of receiving information, an occurrence (file) should be opened on SPROS that contains the details of the investigation. A file is opened whenever NSCI conducts an investigation. Another system, Secure Criminal Information System (SCIS), is also used for older investigations.

SPROS files typically have a 5 day diary date, meaning every 5 days, information must be updated to the file as to the progress of the investigation.

### **General:**

- Use of RCMP IT facilities, e.g. laptops, desktops, mainframe, networks, e-mail, for personal profit, personal recreation or illegal purposes is prohibited.
- Activities on RCMP IT facilities including e-mail are subject to being monitored.
- All software used on RCMP IT facilities must be authorized by the RCMP. Software may only be downloaded from the Internet when it is work related and authorized by the Regional Informatics Officer.
- Before any executable programs, diskettes and other storage media are used on RCMP IT facilities; they must be scanned by a current virus scanner approved by the departmental security officer to ensure they are virus free.
- Laptop computer users are responsible for the security of the laptops and any data contained in them.

**Internet:**

- > Only unclassified or non-sensitive information may be transmitted on the Internet. Designated or classified information must use encryption systems approved by the Departmental Security Officer.
- > Users will not subscribe to automated mailing lists without the approval of the Regional Informatics Officer.

**ROSS:**

- > Only desktop and laptop workstations approved by the Regional Informatics Officer will be connected to ROSS.
- > Once a desktop workstation is connected to the network, it must not be moved to a different location. All requests for relocations will be made through the LAN Administrator.
- > The user will not alter the workstation's configuration, e.g. autoexec.bat, config, sys, nwclient directory. All requests for different configurations will be made through the LAN Administrator.
- > Installation of software on the network will be performed by the LAN Administrator. Software programs may be installed on the local hard disk drive of a networked workstation with the prior approval of the LAN Administrator.
- > ROSS provides for the storage and transmission of data up to and including the security designation of Protected "A". An alternate security method must be used for information with a higher security classification. All exceptions must be approved by the Departmental Security Officer.
- > The data saved on removable media, e.g. floppy diskette, removable hard disk, optical drive, must be protected in accordance with the highest level of classification or designation on the information.
- > Software on the ROSS network is covered by RCMP license agreement. Unauthorized copying of software programs may lead to prosecution under the Copyright Act.
- > Storage of data on local hard drives is not recommended and will not be the responsibility of RCMP Informatics. The making of backup copies of the data stored on the user's local workstation is the sole responsibility of the user.

- > The ROSS Mail system is a delivery system only. Mail messages which meet the criteria of a record as defined in the Informatics Manual, Part IV (<http://infoweb.rcmp-grc.gc.ca/rcmpmanuals/eng/im/imtofc/imtofc.htm>) must be stored in an official RCMP file. Mail messages will be retained on the system on a temporary basis. If a user wants to retain a message older than three months, the user may archive it to his/her local hard disk.
- > When using mail on the ROSS network:
  - > If you are absent for up to three months, appoint a proxy to read and respond to your mail or forward it to another user for action.
  - > Use caution when using automated reply messages (rules) because an improperly created rule can cripple a local post office.
  - > Large file attachments, (greater than 100 KB) should only be sent during quiet hours, after 3:00 p.m. local time. These messages, including attachments, must not exceed 5 MB.
  - > If you will not be using your account for over three months, have your LAN Administrator disable it.
  - > Logout from the ROSS network if you are going to be away from your workstation for more than two hours.
  - > To protect the system when you are away from your workstation for less than two hours, activate a network screen saver including the password option to set a maximum of fifteen minutes of inactivity before activation. The screen saver is not to be used as a substitute for logging out when you are away from your workstation for more than two hours. This feature is not foolproof but it will protect the system against casual intruders or pranksters.



## Chapter Ten — Training

There is a requirement under the Canada Labour Code that certain mandatory training be completed by all employees.

The RCMP standard will need to be completed as follows:

### **Regular Members (RM's)**

1. Use of Force Training (ASP, OC and Carotid)
2. Annual Firearms Qualification
3. First Aid (EMRT)
4. Periodic Health Assessment (PHA — includes PARE or physical)

### **All Team Members (CM's, PSE's, TCE's)**

1. Canada Labour Code (Employee and Supervisor)
2. Harassment Training

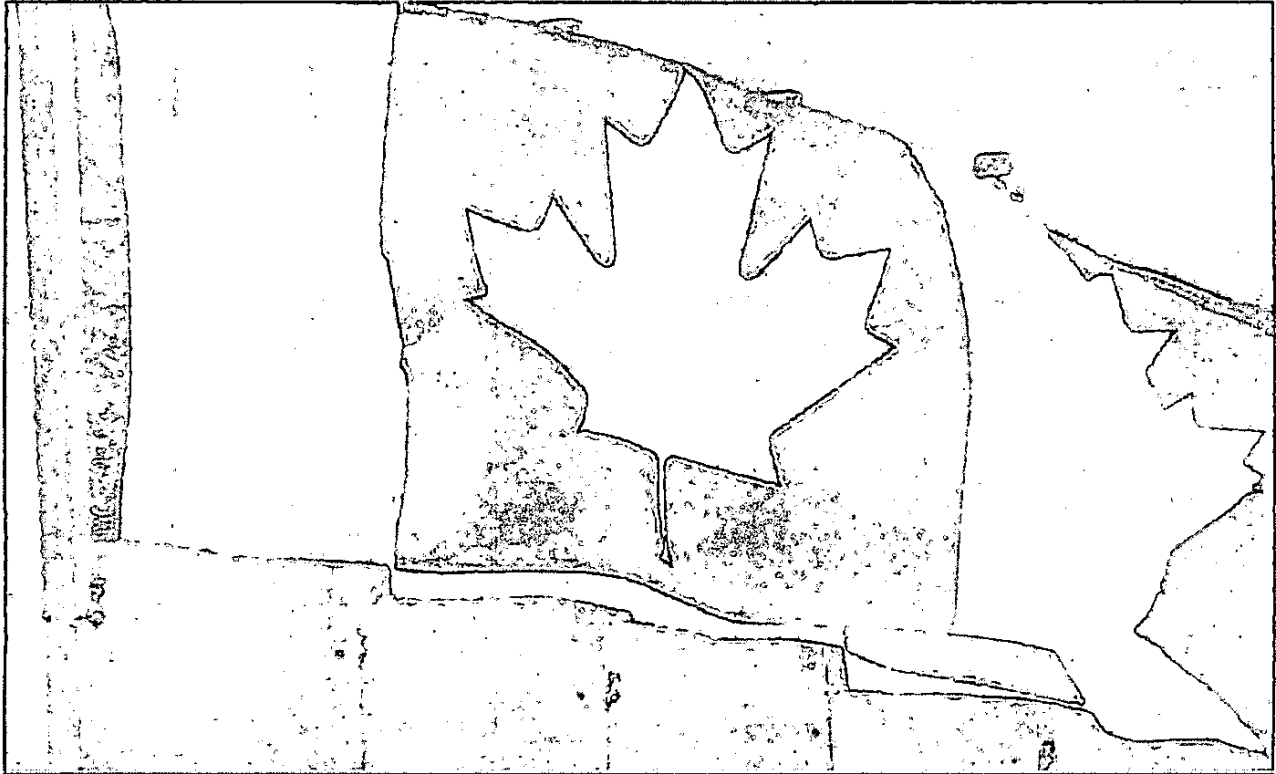
### **In Service Training Programs, Workshops, Seminars and A250 Program**

Each team member is encouraged to be involved with continuous learning. There is a variety of on-line courses through the RCMP INFOWEB. Team members will be registered for courses, workshops and seminar opportunities by the unit throughout the calendar year.

Employees must complete Form 3999 — Individual Development/Learning Plan - to identify their developmental goals. The employee should meet with their supervisor to discuss their learning plan. Training opportunities are based on the needs of the unit, career aspirations of the team members and operational demands. All requests for training are to be made through your supervisor and the unit training NCO.

(The RCMP A250 program is an expense recovery program for members that take fee based training courses outside of the RCMP. Pre-approval and successful completion of the course is required.)

(In-Service Training are the courses taken during work hours)



## Chapter Eleven — Official Languages

*Extract from a memorandum on the Official Languages in the NCR, sent on September 26th, 2003, by C/Supt. Yves Bouchard, DG, Human Resources Programs*

As employees of the RCMP, working in the National Capital Region (NCR), we need to be aware of the *Official Languages Act (OLA)* and its obligations.

RCMP employees in regions designated as bilingual for the purpose of language of work have the right to use English or French for internal communications. You will find the list of bilingual regions in the RCMP Admin. Manual, Appendix II.6.1.

Obligations related to the language of communication between regions will be found in Appendix II.6.2 of the Manual.

As per the RCMP Admin. Manual, II.6.1.4, "Final use of written communications will determine whether they should be produced in both official languages, e.g. a memo or e-mail to all employees in a bilingual region must be **simultaneously** issued in French and English." This applies to correspondence originating from all units located in the NCR.

Managers in bilingual regions are urged to inform employees of their obligations regarding internal communications and to lead by example by communicating in both official languages with their employees. They are also required to create a work environment conducive to the use of both official languages in their unit.

### **What it means to you:**

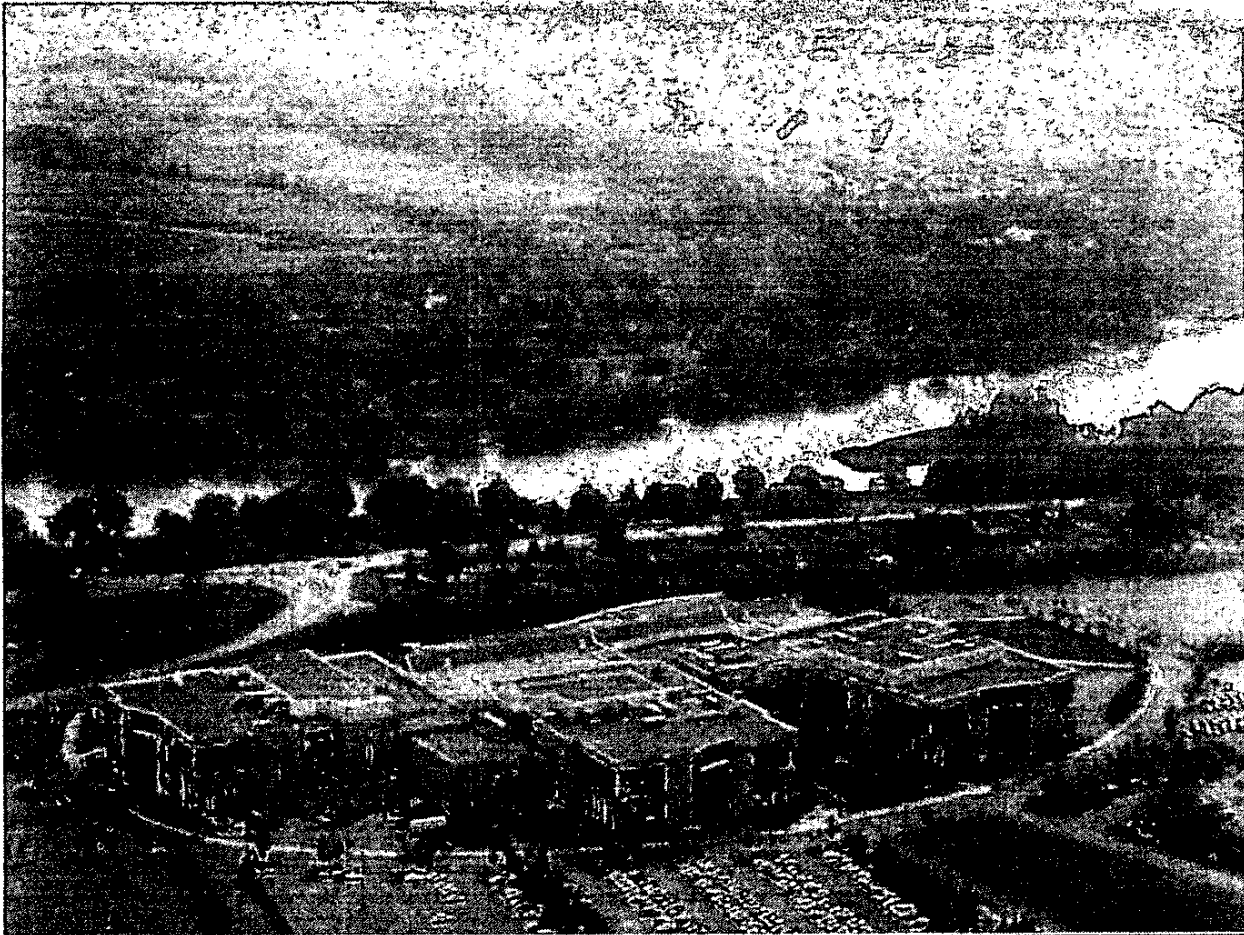
All employees are entitled to work and receive essential services in their first official language. Supervision will be provided in your first official language. Your employee appraisals will be done in the language of your choice. Meetings will be conducted in both official languages.

You are required to ensure that bilingual services are available to clients at all times. If you cannot supply bilingual service personally, you will make arrangements for the client to receive bilingual service. Communications with bilingual regions are in the official language of the recipient or in both official languages. Communications to a unilingual region are in the language of work of the recipient. Wide area broadcasts are in both official languages.

~~(National Security Criminal Investigations — Orientation Guide)~~

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

40



## Chapter Twelve — Relocation of RCMP National Headquarters

On August 11, 2006, the Honourable Stockwell Day, Minister of Public Safety, announced that RCMP Headquarters had received authorization to relocate to a new facility located at 3000 Merivale Road in south Ottawa. The move to 3000 Merivale Road provides the RCMP with an opportunity to consolidate many of its National Headquarters functions into a modern and efficient work space and provide its employees with a bright, airy and functional working environment. For up-to-date information on the NHQ Relocation Project, visit the project Infoweb site at: [http://infoweb.rcmp-grc.gc.ca/cm/HQrehabilitation/NHQnew/index\\_e.htm](http://infoweb.rcmp-grc.gc.ca/cm/HQrehabilitation/NHQnew/index_e.htm)

## Chapter Thirteen — Commonly Used Acronyms

### Agencies

**BATF** — Bureau of Alcohol Tobacco and Firearms (ATF, United States)

**BATF** — Bureau of Alcohol Tobacco and Firearms (ATF, United States)

**BSS** — British Security Service

**CBSA** — Canada Border Services Agency

**CCG** — Canadian Coast Guard

**CIA** — Central Intelligence Agency

**CSE** — Communications Security Establishment (a branch of the Armed Forces)

**CSIS** — Canadian Security Intelligence Service (known as the Service or Sisters)

**DFAIT** — Department of Foreign Affairs and International Trade

**DFO** — Department of Fisheries and Oceans

**DHS** — Department of Homeland Security (United States)

**DND** — Department of National Defence (also known as the Canadian Armed Forces or CF)

**DOD** — Department of Defence (United States)

**DOJ** — Department of Justice (prosecute Federal charges)

**FBI** — Federal Bureau of Investigations (United States)

**FINTRAC** — Financial Transactions and Reports Analysis Centre

**FSB** — Russian Federal Security Branch (the former KGB)

**IBET** — Integrated Border Enforcement Team

**ITAC** — Integrated Threat Assessment Centre (Canadian intelligence sharing centre)

**JTF II** — Joint Task Force 2 (Canadian Armed Forces)

**NCIS** — Naval Criminal Investigative Service (United States)

**NCIU** — National Counter Intelligence Unit (Canadian Armed Forces)

**NOC** — National Operations Centre (at RCMP in Ottawa, active 24/7)

**NTC** — National Threat Center (United States)

**PSC** — Public Safety Canada

**SIRC** — Security Intelligence Review Committee

**USSS** — United States Secret Service

### Computer Systems

**ACIIS III** — Automated Criminal Intelligence Information System

**CABS** — Computer Arrest and Booking System (used by detachments)

**CIIDS** — Computerized Integrated Information and Dispatch System (used by detachments)

**CPIC** — Canadian Police Information Centre (National Law Enforcement inquiry system. Search for wanted persons, criminal records, criminal history, drivers license, vehicle license information)

**E&R III** — Evidence and Reports (Major Case Management tool used to manage projects)

**ICES** — Integrated Customs Enforcement System (used by CBSA Customs)

**FOSS** — Field Operations Support System (CBSA Immigration system)

**PIRS** — Police Information Retrieval System

**PRIME** — Police Records Information Management Environment (system used by all BC Police agencies)

**PROS** — Police Reporting and Occurrence System

**SCIS** — Secure Computer Information System

**RMS** — Record Management System

**ROSS** — Non-secure computer system, access PIRS; Email, Word Perfect

**SPROS** — Secure Police Reporting and Occurrence System

**Supertext** — Records management for large quantity of documents (scanning)

National Security Criminal Investigations — Orientation Guide

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.

13

Protected "A"

### RCMP Units

**ATFIU** — Anti-Terrorist Financial Investigation Unit  
**BIT** — Border Integrity Team  
**CBRN Team** — Chemical, Biological, Radiological and Nuclear Response Team (an explosives disposal unit function)  
**CI** — Criminal Intelligence – Ottawa (formerly Criminal Intelligence Directorate or CID)  
**EDU** — Explosives Disposal Unit  
**FIO** — Federal and International Operations  
**FIU** — Financial Intelligence Unit  
**GEU** — General Enforcement Unit  
**IBET** — Integrated Border Enforcement Team  
**IMET** — Integrated Market Enforcement Team  
**INSET** — Integrated National Security Enforcement Team  
**IPOC** — Integrated Proceeds of Crime  
**JIG** — Joint Intelligence Group  
**NSCOB** — National Security Criminal Operations Branch  
**NSCOSB** — National Security Criminal Operations Support Branch  
**NSLAB** — National Security Legislative Affairs Branch  
**NPS** — National Police Services  
**OISP** — Office of Investigative Standards and Practices  
**ORRCC** — Operational Readiness and Response Coordination Centre  
**PDS** — Police Dog Section  
**QRT** — Quick Response Team  
**SDU** — Source Development Unit  
**SIPS** — Strategic Integration and Program Support  
**TA** — Threat Assessment

### Miscellaneous Terms

**AOD** — Absent on Duty (on a training course, at court, etc.)  
**AOL** — Absent on Leave (vacation)  
**CM** — Civilian Member  
**CROPS** — Criminal Operations  
**GD** — General Duty (in reference to uniform police officers at a detachment)  
**GIS** — General Investigation Section (in reference to the plainclothes element at a detachment)  
**HRMIS** — Human Resources Management Information System: Every employee is assigned a HRMIS number which is required for pay & compensation, computer access, etc.  
**MLAT** — Mutual Legal Assistance Treaty (agreement between governments on sharing of information)  
**MOU** — Memorandum of Understanding (agreement between agencies)  
**ODS** — Off Duty Sick  
**PSE** — Public Service Employee  
**RIO** — Regional Intelligence Officer (CBSA)  
**RM** — Regular Member  
**SEC** — Senior Executive Committee  
**SMT** — Senior Management Team  
**TCE** — Temporary Civilian Employee



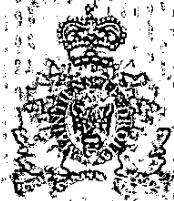
## NATIONAL SECURITY CRIMINAL INVESTIGATIONS

### National Security Criminal Investigations — Orientation Guide

44

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is to be used for the intended purposes only, and should not be disseminated, in whole or in part, without the prior consent of the originator. For any enquiries concerning the information, please contact the originator of the document.





NATIONAL SECURITY  
CRIMINAL INVESTIGATIONS

# ORIENTATION GUIDE 2008

