Privacy Commissioner of Canada
Commissaire à la protection de la vie privée du Canada

Privacy

AUDIT REPORT OF THE
PRIVACY COMMISSIONER OF CANADA

Examination of RCMP Exempt Data Banks

Section 36 of the *Privacy Act*

FEBRUARY 2008

Canada

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP54-5/2008
ISBN 978-0-662-05406-1

This publication is also available on our Web site at **www.privcom.gc.ca**.

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Téléc. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

February 2008

The Honourable Noël A. Kinsella, Senator
Speaker of the Senate
The Senate of Canada
Room 379 S, Centre Block
Ottawa ON K1A 0A4

Dear Mr. Speaker:

I have the honour to submit to Parliament a Special Report on the Examination of RCMP Exempt Data Banks pursuant to Section 36 of the *Privacy Act*.

Sincerely,

Jennifer Stoddart

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Téléc. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

February 2008

The Honourable Peter Milliken, M.P.
Speaker of the House of Commons
House of Commons
Room 222 N, Centre Block
Ottawa ON K1A 0A6

Dear Mr. Speaker:

I have the honour to submit to Parliament a Special Report on the Examination of RCMP Exempt Data Banks pursuant to Section 36 of the *Privacy Act*.

Sincerely,

Jennifer Stoddart

Jennifer Stoddart
Privacy Commissioner of Canada

Examination of Royal Canadian Mounted Police (RCMP) Exempt Data Banks

Table of Contents

Executive Summary

1.1 The *Privacy Act* attempts to strike a balance between individual access rights and the state's right to protect information relating to a particular public or private interest. Exempt banks serve to withhold the most sensitive national security and criminal intelligence information. Institutions with control over such records will consistently refuse to confirm or deny the existence of information in response to an individual's request for access.

1.2 The *Privacy Act* requires the head of a government institution to include in personal information banks all personal information under the control of the government institution that:

- has been used, is being used or is available for use for an administrative purpose; or
- is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.[1]

1.3 The personal information bank concept imposes an obligation on government institutions to organize personal information into logical groupings and identify that information by description, purpose, use, disclosure, retention and disposal criteria. This assists the public in identifying information that may be relevant to them.

1.4 Section 18 (Exempt Banks) is the one exempting provision of the *Privacy Act* that makes specific reference to "files". This logically establishes an obligation to identify and organize the information into identifiable files. This is necessary, not solely for ease of reference, but also to facilitate the determination of the predominance requirement

1 *Privacy Act*, s. 10.

established under section 18 of the Act (paragraph 2.3 of this report refers).

1.5 By virtue of design, exempt banks provide institutions with the privilege of keeping information totally exempt from public access. Individuals are neither accorded access to the information, nor are they aware of its existence. Therefore, it is incumbent upon institutions to ensure that the composition of such banks is restricted to files that legitimately warrant inclusion. As the Privacy Commissioner remarked in 1990,

> *No exempt bank once established can be allowed to become an uncontrolled hiding place for personal information*.[2]

1.6 The concept of exempt banks is defensible. We appreciate the special circumstances of security and intelligence work. We also recognize the importance of assuring law enforcement and security partners, both domestic and abroad, that information provided in confidence will be protected accordingly. Any perception that such protection has been lost may adversely affect the flow of information that is vital to the RCMP's investigative activities.

1.7 At the same time, individuals could potentially find themselves the subject of an exempt bank file by being in the wrong place, at the wrong time, talking to the wrong person. Inclusion in the bank may also be the result of information provided by a neighbor, friend or associate, some of whom may be motivated by something other than civic responsibility.

1.8 Accordingly, during the course of our audit we expected to find exempt bank files that:

- were identified by unique file numbers;
- were examined prior to placement in the exempt bank to ensure the information met the established criteria for inclusion; and
- were subject to an ongoing review mechanism to assess the merit of continued exempt bank status, with the appropriate injury tests or class test being applied based on clear principles.

1.9 We conclude that files were readily identifiable as exempt and were examined prior to placement in the exempt banks. However, we found that files have not been sufficiently managed to ensure that their exempt bank status was validated on an ongoing basis, as prescribed under RCMP policy. Of the exempt bank files opened prior to 2004, approximately 70% of the national security files and 90% of the criminal operational intelligence files within the audit sample had not been subject to ongoing review.

2 Privacy Commissioner's Annual Report 1989-90, p. 28.

1.10 Upon identifying exempt banks as a high risk area, the RCMP initiated an internal review in February 2006. Records were removed where it was found that they did not meet the criteria for inclusion in an exempt bank. As of September 19, 2007, over 1,400 national security files and approximately 45,000 criminal operational intelligence documents have been removed from the exempt banks. Notwithstanding these substantial reductions, more work is required.

1.11 Section 18 of the *Privacy Act* requires that each file within an exempt bank consist predominantly of personal information as described in section 21 (international affairs and defence) or section 22 (law enforcement) of the Act. Section 18 is explicit in this regard. While not pervasive among our testing sample, we found files in both exempt banks that did not satisfy the predominance requirement. By extension, their inclusion in the banks does not comply with the *Privacy Act*.

1.12 Furthermore, approximately 50% of the national security files and 60% of the criminal operational intelligence files we tested did not meet the established threshold for continued exempt bank status under RCMP policy.

1.13 The primary reasons for the non-compliant state of the two banks are: a lack of a well defined accountability infrastructure; a general lack of awareness of exempt bank policy; and the absence of ongoing monitoring and regular audit.

1.14 In the late eighties, the RCMP's criminal operational intelligence exempt bank order was rescinded for non-compliance. It was reinstated in 1990, with an understanding that there would be strict adherence to guidelines for managing exempt bank holdings. In our view, the RCMP has not met this commitment.

1.15 In moving forward, the RCMP must develop a strategy to verify that its current exempt bank holdings comply with the requirements of section 18 of the *Privacy Act* and associated internal policies. We would suggest that the RCMP's Access to Information and Privacy (ATIP) Directorate be fully engaged in this exercise.

1.16 Accountability for the ongoing maintenance of exempt banks must be clearly defined and enforced. Furthermore, as policy observance is key to maintaining the integrity of the files over time, exempt bank related compliance audits should be included in future plans and priorities of the RCMP.

1.17 There is no quick remedy. Indeed, considerable resources and a coordinated effort will be required to sustain the integrity of the banks. Left unattended, the RCMP runs the risk of placing itself in a position similar to that of the late eighties when the validity of its exempt bank order was challenged – and ultimately revoked by the Governor in Council.

The Royal Canadian Mounted Police have responded. The Force agrees with our recommendations. Its detailed responses follow each recommendation throughout the report.

Introduction

Background

2.1 The President of the Treasury Board is the Designated Minister under the *Privacy Act* responsible for issuing policies and guidelines governing the operation of the Act and Regulations.[3]

2.2 Within federal government departments and agencies, the responsibility for ensuring organizational compliance with the *Privacy Act* rests with Ministers and other heads of institutions as designated by Order in Council.

2.3 To qualify for designation as an exempt bank, the bank must contain files, *all of which* consist predominantly of personal information described in section 21 (international affairs and defence) or section 22 (law enforcement and investigations) of the Act. Treasury Board policy defines "predominantly" as meaning that a preponderance – or more than half – of the information in *each of the files* must qualify for exemption.

2.4 In December 1993 the Government of Canada introduced its policy on Privacy and Data Protection. The policy – which replaced previous directives – applies to all institutions listed in the Schedule to the *Privacy Act*.

2.5 Pursuant to the policy, institutions must consult with Treasury Board on any proposal for the establishment or revocation of an exempt bank. The policy further requires that all requests for exempt bank designations be submitted to the President of the Treasury Board, and prescribes the information to be included therein.

3 *Order in Council P.C. 1983-1584 2 June, 1983.*

1993 Treasury Board Policy – Privacy and Data Protection

Policy Requirements – Exempt banks

Government institutions must submit to the Designated Minister any requests to designate exempt personal information banks. Requests for exempt banks submitted to the Designated Minister must include:

(a) a description of the information to be included in the exempt bank;

(b) the specific exemption provision under which the information requires protection, including, for exemption provision 22(1)(a)(ii), the law concerned (e.g. the Income Tax Act), and for any injury test exemption, a statement of the expected detrimental effect ;

(c) an explanation, including cost implications, of why the information should be placed in an exempt bank rather than being subject to review on a case-by-case basis;

(d) certification that all files in the bank consist predominantly of personal information of the type described in Sections 21 or 22 of the *Privacy Act* and that procedures are in place to ensure that files are reviewed on an ongoing basis;

(e) a draft Order in Council; and

(f) a draft Regulatory Impact Analysis Statement.

[The complete Privacy and Data Protection Policy can be found on the Treasury Board Secretariat's Web site at: http.//www.tbs-sct.gc.ca]

2.6 The Governor in Council has sole responsibility for determining and designating as exempt certain personal information banks. This authority is derived from subsection 18(1) of the *Privacy Act*. An order made by the Governor in Council under subsection 18(3) specifies:

- the section on the basis of which the order is made; and
- where the bank contains files which consist predominantly of personal information described in subparagraph 22(1)(a)(ii), the law concerned.

The Commissioner's Authority

2.7 Section 36 of the *Privacy Act* empowers the Privacy Commissioner to review files contained in an exempt bank and make recommendations that the Commissioner considers appropriate. For example, the Commissioner could request the removal of any file which, in the Commissioner's opinion, does not meet the established criteria for inclusion in the bank. If the institution refuses to remove the file, the Commissioner may apply to the Federal Court for a review of the matter.[4]

4 *Privacy Act*, s. 43.

The History Is Important

2.8 An issue that arose during the first years of the *Privacy Act* was the status of – and the necessity for – exempt banks.[5] Little concern was expressed about exempt banks during the legislative passage of the Act [6], and the Office of the Privacy Commissioner (OPC) had adopted a working assumption that such banks were properly closed (constituted).

2.9 The status of exempt banks was challenged in 1984 following a request for personal information held in RCMP Bank P-130, Security Service Records.

2.10 In responding to the request, the RCMP would neither confirm nor deny whether any personal information about the requester was held in the bank. The individual complained to the Privacy Commissioner. The Commissioner found that he too could neither confirm nor deny the existence of any record, and informed the complainant that there was no basis to recommend that he had been denied a right under the *Privacy Act*.

2.11 The individual appealed to the Federal Court for a review. His legal representative sought confirmation that all files in the bank had been examined before it was closed to determine whether they met the test of exempt bank status. The Department of Justice was unable to defend the validity of the exempt bank and agreed that the bank should be treated as open (non-exempt).[7]

2.12 Prior to the conclusion of the case, the OPC had initiated an investigation of the exempt banks held by Employment and Immigration Canada (EIC). The Privacy Commissioner found, following the investigation, that the banks were not properly examined prior to the application for exempt bank status.

2.13 The Federal Court case referenced above and the investigation of EIC's exempt banks compelled the OPC to abandon an initial working assumption that such banks were properly closed.[8]

2.14 In October 1985 the Privacy Commissioner wrote to all federal institutions with exempt bank holdings and requested evidence that their respective banks had been examined in a manner that would satisfy the requirements of section 18 of the *Privacy Act*. The departmental replies indicated that many of the banks were being

5 Privacy Commissioner's Annual Report 1985-86, p. 21.
6 Privacy Commissioner's Annual Report 1985-86, p. 22.
7 Privacy Commissioner's Annual Report 1985-86, p. 22.
8 Privacy Commissioner's Annual Report 1985-86, p. 22.

treated as open and the process of rescinding the exempt bank orders had commenced.[9]

2.15 When the *Privacy Act* came into effect, nineteen (19) – of approximately 2,200 banks across the federal government – were designated as exempt (closed).[10] An additional bank was closed in 1985. The exempt status of 15 of the 20 banks was rescinded in February 1987.[11] By 1989, three banks remained, one of which was in the process of having its exempt status revoked.

Present Day Exempt Banks

2.16 There are currently four exempt banks. Two are held under the control of the Royal Canadian Mounted Police (RCMP), with one being retained by the Canadian Security Intelligence Service (CSIS) and one by the Communications Security Establishment (CSE). The two exempt banks held by the RCMP are: Criminal Operational Intelligence Records, and National Security Investigations Records.

Prior Audit of the Criminal Operational Intelligence Records Exempt Bank

2.17 The RCMP was one of eight institutions that the Privacy Commissioner contacted in October 1985 regarding their exempt banks. At that time, the RCMP held two exempt banks: P-PU-140 Protection of Personnel and Government Property, and P-PU-120 Criminal Operational Intelligence Records.[12]

2.18 In responding to the Commissioner, the RCMP advised that a process was underway to have bank P-PU-140 – Protection of Personnel and Government Property – deregistered. The exempt bank order was subsequently rescinded.

2.19 Turning to exempt bank P-PU-120 (renumbered P-PU-015), Criminal Operational Intelligence Records, the Commissioner of the RCMP reported that he was satisfied the bank met the criteria of section 18 of the *Privacy Act* as certified in the Order in Council. To validate this claim, the Privacy Commissioner initiated an audit of the bank in 1986.

---

9 Privacy Commissioner's Annual Report 1986-87, p. 24.

10 Privacy Commissioner's Annual Report 1985-86, p. 22.

11 Orders in Council P.C. 1987-282 to 295 inclusive, passed on 1987-02-19 rescinded the exempt status of banks held by the Department of Employment and Immigration, Canada Employment and Immigration Commission, Canada Post, Correctional Service Canada, Department of National Revenue, Canadian Security Intelligence Service and the Department of the Solicitor General. [Privacy Commissioner's Annual Report 1986-87 p. 24].

12 RCMP Exempt Bank P-130, Security Service Records, the exempt bank status of which was challenged in Federal Court (paragraph 2.11 refers) had not been held by the RCMP since the separation of the RCMP Security Service and the formation of the Canadian Security Intelligence Service on July 16, 1984.

2.20 The examination focused on whether all files in the bank had been individually reviewed to verify that the predominance test under section 18 of the Act had been met. In summary, the audit found that the bank did not comply with the requirements of the *Privacy Act*. In October 1987 the Commissioner recommended that the Solicitor General rescind the exempt bank order and seek a new order, if the Minister considered it necessary to maintain the bank's exempt status.[13]

2.21 During the same period – and in response to the OPC's audit findings – the RCMP completed an examination of the exempt bank.

2.22 The audit resulted in significant policy and procedural changes at the RCMP. In the end, the RCMP accepted the Commissioner's recommendation and the exempt bank order was revoked. Coincident with the application for revocation, a new Order in Council was sought to reconstitute the bank.

2.23 The application was accompanied by a *Regulatory Impact Analysis Statement*, a key element of which was the establishment of a compliance regime to ensure exempt bank files were subject to complete and regular review.

Regulatory Impact Analysis Statement

Compliance Mechanism

The RCMP is entitled by law to request and maintain an exempt personal information bank. All the files within the Criminal Operational Intelligence Records bank are certified and consist predominantly of exempt personal information and each of these files will be reviewed within two years and at other times to ensure the files continue to qualify for exempt bank status. Compliance will be monitored by both internal and external audit.

[The complete text of the Regulatory Impact Analysis Statement can be found in the *Canada Gazette Part II, Vol. 124, No. 6*]

2.24 On February 22, 1990 the existing Order was revoked and a new Order for the Criminal Operational Intelligence Records Exempt Bank was issued.[14] A description of the bank is provided below.

13 Privacy Commissioner's Annual Report 1987-88, p. 21.

14 *Exempt Personal Information Bank Order No. 13 (RCMP),* S.O.R./90-149.

Criminal Operational Intelligence Records – CMP PPU 015

The following is a summary extracted from the description published in Info Source, Sources of Federal Government Information, 2006-2007 Volume 2, p. 587-588.

The bank contains personal information on individuals who have been implicated, following criminal investigations, in organized crime activities such as drug trafficking, securities fraud, pornography, extortion and prostitution. The bank also retains personal information about confidential human sources and witnesses requiring protection relating to criminal operations. Information is maintained in both electronic and hard copy formats, with a minimum retention period of two calendar years.

[The complete bank description can be found at: http.//www.infosource.gc.ca]

Creation of the National Security Investigations Exempt Bank

2.25 In 1992 the OPC was informed of the RCMP's intention of establishing an additional exempt bank to retain records relating to its national security investigations. A submission seeking the exempt bank designation was prepared and submitted to the OPC for review.

2.26 The RCMP's submission was delayed pending the reconstitution of the Criminal Operational Intelligence Records exempt bank and the implementation of policy and procedural changes for the maintenance of exempt bank files.

2.27 Upon completing his review, the Privacy Commissioner was satisfied that the content of the files met section 18 requirements. Consequently, no objection was raised.[15]

National Security Investigations Records – CMP PPU 025

The following is a summary extracted from the description published in Info Source, Sources of Federal Government Information, 2006-2007, Volume 2, p. 588-589.

This bank contains personal information about individuals who have come to the attention of the RCMP in the course of national security enforcement, including information collected in the fulfillment of the primary responsibility conferred by subsection 6(1) of the *Security Offences Act* – specifically, information obtained or prepared for investigation purposes in respect of an offence under any law of Canada where:

- the alleged offence arises out of conduct constituting a threat to the security of Canada within the meaning of the *CSIS Act*, or
- the victim of the alleged offence is an internationally protected person within the meaning of section 2 of the *Criminal Code*.

15 In responding to the RCMP, the Commissioner drew attention to the fact that he had not commented on the validity of the exemptions applied as he would not wish to, nor be seen to, prejudice the matter should he receive a complaint from an individual whose personal information was contained in the files.

The bank also retains security assessments relating to internationally protected persons, data concerning the management of confidential sources and witnesses used in national security investigations, and personal information on individuals who have been involved in investigations relating to threats, potential threats, or incidents against persons of national or international importance or involving government property. Information is maintained in hard copy format as well as electronically in the Secure Criminal Information System (SCIS). Records are maintained for a minimum of five calendar years.

[The complete bank description can be found at: http.//www.infosource.gc.ca]

2.28 The above bank was designated by the Governor in Council as a Personal Information Exempt Bank on May 25, 1993.[16]

About the RCMP

2.29 Formed in 1873, the RCMP is Canada's national law enforcement police service. Pursuant to the *RCMP Act*, the Commissioner, under the direction of the Minister of Public Safety, is responsible for overall management of the Force.

2.30 The RCMP's responsibilities include the investigation of offences under section 2 of the *Security Offences Act*, the *Criminal Code* and the *Security of Information Act* – formerly the *Official Secrets Act*. The Force is also responsible for protective security measures to safeguard designated persons (VIPs), federal properties and other vital points from security offences and threats.

2.31 RCMP Headquarters (HQ) is located in Ottawa. The Force is organized into four regions, 14 divisions and the RCMP's training facility in Regina,[17] with a presence in all provinces and the three territories. A listing of Divisions is found at Annex B. The RCMP's staff complement includes regular and civilian members, as well as public service employees.[18]

About the Audit

Rationale

2.32 The decision to proceed with an examination of the RCMP's exempt banks was taken following a risk-based assessment. The following factors were considered during the assessment process:

- the banks had not been reviewed for 20 years;

16 *Exempt Personal Information Bank Order No. 25 (RCMP),* S.O.R./93-272.

17 RCMP Report on Plans and Priorities 2007-2008, p. 19.

18 According to its Web site, the RCMP had an on-strength staff complement of 24,641 as of January 1, 2007.

- the inherent sensitive nature of the information stored in the banks; and
- the increased sharing of information, including exempt bank data, between law enforcement and security partners following the events of September 11, 2001.

2.33 Given the composition of exempt banks, individuals are not provided access to personal information contained therein, nor are they aware of its existence. With this in mind, the examination was viewed as important in terms of providing the Canadian public with a level of comfort that the banks are properly managed – and by extension, the privilege of keeping them totally exempt from public access was defensible.

Objective

2.34 To ensure that the National Security Investigations Records and Criminal Operational Intelligence Records exempt banks have been constituted in accordance with the criteria established under section 18(1) of the *Privacy Act*.

Sub-objectives:

a. To establish whether an effective management control framework exists for exempt banks, and measure the level of compliance with the framework.

b. To determine whether exempt bank files have been kept beyond established retention and disposal schedules.

Scope and approach

2.35 Our audit was conducted under the authority of section 36 of the *Privacy Act*. It was not initiated pursuant to section 37 of the Act. Accordingly, we did not assess the extent to which the personal information management practices of the RCMP are in compliance with sections 4 through 8 of the *Privacy Act* in significant detail.

2.36 It was not part of our audit to conclude whether the banks should or should not have exempt status. This is for the Governor in Council to decide. Nor did we attempt to discern how information in an exempt bank file was actually used – or influenced decisions – as part of the day-to-day operations of the RCMP. This would require an in-depth analysis of each investigative file, including all actions and decisions taken.

2.37 We did consider the risk of including inaccurate personal information in an exempt bank. To that end, our lines of inquiry were directed at establishing whether the reliability of data was assessed and recorded on file. In addition, inquiries were made – through interviews and file

examinations – to determine the extent to which information obtained by data brokerage entities is used to develop exempt bank files.

2.38 Given the audit objective, the majority of resources were dedicated to the examination of exempt bank files. This was complemented by interviews with selected personnel engaged in the administration of such files, and our review of relevant policies and procedures.

2.39 Responsibility for the management of personal information holdings, including exempt bank files, rests at the divisional level of the RCMP. In addition to RCMP HQ, our audit activity was carried out at:

RCMP A Division (National Capital Region)

RCMP O Division (Ontario)

Niagara Regional Detachment

Integrated National Security Enforcement Team

Milton Detachment

2.40 Our intent to carry out an examination of exempt banks was first signaled in November 2005 (see paragraph 3.1 below). The RCMP was given written notification of our audit on August 9, 2006. The examination was substantially completed by August 7, 2007. Therefore, the observations and recommendations in this report are based on information as of that date – and it is the effective date of reporting the results of the audit.

Audit team

Director General: Trevor R. Shaw

Michael Fagan
Robert Bedley

Observations and Recommendations

RCMP Internal Review: Moving Towards Compliance

3.1 In her submission to the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* in November 2005, the Privacy Commissioner commented on the importance of internal oversight and accountability, and the need for federal government departments and agencies to develop and implement strong privacy management frameworks that include an internal privacy audit capacity. The Commissioner also indicated that an audit of exempt banks would be undertaken in 2006.

3.2 Approximately four months later the RCMP initiated an internal review of its exempt bank holdings. Coordinated by RCMP HQ, the review was initiated in February 2006 and was substantially completed by August 2007 – as we were completing our audit.

3.3 To facilitate the internal examination, divisions were provided listings identifying the exempt bank records held within their respective jurisdictions, as captured in the RCMP's national security and criminal intelligence databases.

3.4 In terms of the national security exempt bank, internal reviews at RCMP HQ and all 14 divisions have been completed. Divisions located in the three territories do not hold national security exempt

bank files. The results of the internal reviews conducted at RCMP HQ and A Division were not available.[19]

Exhibit A: RCMP Internal Review of National Security (SCIS) Exempt Bank Files

Division	Review Initiated	National Security Exempt Bank Files as of 2006-03-13	Review Completion Date (RCD)	National Security Exempt Bank Files as of RCD
A	2006-03-13	626	2006-09-26	Not Available
B	2006-03-13	139	2006-04-13	28
C	2006-03-13	427	2007-05-25	201
D	2006-03-13	336	2006-09-14	276
E	2006-03-13	108	2006-09-11	87
F	2006-03-13	117	2006-09-20	100
G	2006-03-13	0	2006-03-13	0
H	2006-03-13	168	2006-05-09	116
J	2006-03-13	814	2006-07-27	222
K	2006-03-13	342	2006-05-02	190
L	2006-03-13	23	2006-03-28	16
M	2006-03-13	0	2006-03-13	0
O	2006-09-21	941	2007-09-19	732
V	2006-03-13	0	2006-03-13	0
HQ	2006-03-13	666	2006-04-24	Not Available

3.5 As reported in the above Table, 10 divisions reported reductions following their reviews, ranging from approximately 15 to 79 percent. When examined collectively, over 1,400 files were removed from the national security exempt bank.

3.6 Turning to the criminal operational intelligence exempt bank, each division was provided a report highlighting their exempt bank holdings within the National Criminal Data Bank (NCDB). The reports captured:

- the number of NCDB documents that were flagged as being retained in the exempt bank;
- the location of the documents (general or restricted folder); and
- a breakdown of the above by year.

3.7 We were informed that each exempt document in NCDB is linked (cross-referenced) to a specific exempt bank file. A file may contain one or many flagged documents, and a flagged document may be retained on more than one exempt bank file.

19 The internal review at RCMP HQ was completed on April 24, 2006. RCMP A Division finalized its examination on September 26, 2006. The number of files that remained in the exempt bank following the reviews is unknown (was not recorded at the time the examinations were completed). In terms of available data, RCMP HQ held 238 national security exempt bank files on November 15/07, representing an overall reduction of 428 files during the period covering March 2006 to November 2007. The number of national security exempt bank files at A Division decreased by approximately 12 percent during the same period – from 626 files in March 2006 to 552 files as of November 15/07.

3.8 The internal reviews at RCMP HQ and 10 divisions were completed prior to December 2006. Two additional reviews were finalized by May 2007. Examinations at A and H divisions were ongoing when we completed our audit field work.

3.9 Of the thirteen completed examinations, RCMP HQ and four divisions (B, C, L and V) recorded the number of NCDB documents that were removed from the exempt bank following their respective reviews.

Exhibit B: RCMP Internal Review of Criminal Intelligence (NCDB) Exempt Bank Documents

Division	Review Initiated	Exempt Bank Documents	Review Completed	Documents Following Review
B	2006-02-08	55,118	2006-08-10	18,391
C	2006-02-08	6,471	2007-05-09	5,622
L	2006-02-08	2,218	2006-06-15	1,966
V	2006-02-08	10	2006-02-10	0
HQ	2006-03-13	2,797	2006-06-30	35

3.10 All five reported reductions in the number of NCDB documents, and by extension, the number of criminal operational intelligence exempt bank files. Of particular significance are the reductions reported by B Division and RCMP HQ, where collectively over 39,000 documents were removed from the bank.

3.11 Statistical data for the remaining eight divisions was not captured at the time the reviews were finalized, and the NCDB database lacks the capacity to produce such information. As an alternative, the RCMP provided:

- the number of NCDB documents that were held in the exempt bank on 2006-02-08 (date the internal review was initiated); and
- the number of exempt bank documents that were uploaded in NCDB prior to the completion of the divisional reviews.[20]

20 The data does not include the exempt bank documents that were added to NCDB prior to the completion of the divisional review, but were subsequently removed from the bank.

Exhibit C: RCMP Internal Review of Criminal Intelligence (NCDB) Exempt Bank Documents

Division	NCDB Exempt Bank Documents as of 2006-02-08	Review Completion Date (RCD)	Exempt Bank Documents uploaded to NCDB prior to RCD
D	17,477	2006-09-01	17,382
E	25,213	2007-04-05	24,373
F	890	2006-04-12	427
G	2,751	2006-02-12	2,765
J	24,200	2006-10-31	24,294
K	1,471	2006-05-05	1,778
M	294	2006-03-29	328
O	20,986	2006-11-08	16,606

3.12 It is important to remain mindful that the fourth column of the above Table includes NCDB documents that were added to the exempt bank while reviews were ongoing. As the number of documents involved cannot be extrapolated, the extent of the reductions – and the reported divisional increases – cannot be verified. Notwithstanding, the data does confirm that the internal review yielded reductions in a minimum of four of the eight divisions.

3.13 As a number of divisional reviews have yet to be completed and certain data elements are unavailable, the results of the RCMP's internal examination are not fully known.

3.14 Despite the absence of complete data, we can conclude that the internal review has led to significant reductions in exempt bank files. From a compliance perspective, the data illustrates a condition where files were retained in an exempt bank for periods when their inclusion was unwarranted.

3.15 **Files have yet to be assessed**. As a result of administrative oversight, certain files were not subject to assessment as part of the RCMP's internal review. Warranting specific mention are files that are designated as exempt in the Police Information Retrieval System (PIRS).

3.16 PIRS is a recording and retrieval system that contains information on events (occurrences) reported to the RCMP. It includes data on individuals who have been involved in investigations under the *Criminal Code*, federal and provincial statutes, municipal by-laws and territorial ordinances. As PIRS only captures 299 characters of free text, it is generally considered a records management indexing system. The actual files are paper based.

3.17 PIRS data is retained in regional databases. Statistics capturing regional inventories of exempt files in PIRS were unavailable at the time of preparing this report. While the data would be useful in terms of assessing the significance of the administrative oversight, it is not required for reporting purposes. Our audit sample included a selection

of criminal operational intelligence files flagged as exempt in PIRS. The selection covered an eleven year period (1993-2004). With one exception, none of the files had been examined during the RCMP's internal review. Furthermore, we observed files that had not been reviewed subsequent to their placement in the exempt bank.

3.18 Our inquiries would also suggest a number of national security exempt bank (SCIS) files were overlooked during the internal review. As noted in paragraph 3.3, file listings were issued to facilitate divisional examinations. These listings identified files by collator code (location).

3.19 Of the eight divisions that reported the results of their reviews, five noted that the listings included SCIS files that were held in other jurisdictions (another collator code had been assigned). These observations were reported to RCMP HQ. The information received suggests that no subsequent action was taken. On that basis, it would appear that these files have yet to undergo review to validate their exempt bank status.

3.20 While we acknowledge and appreciate the importance of the RCMP's internal review, additional work is required.

Non-Compliance with Critical Element of Control Framework

3.21 Compliance with section 18 of the *Privacy Act* presupposes the existence of an administrative infrastructure to ensure the integrity of exempt banks is maintained on a routine basis.

3.22 Recognizing the flaws that undermined the validity of the exempt bank order that existed prior to 1990, the RCMP implemented a number of policy and procedural changes to manage its exempt bank holdings.

3.23 One of the key control features was the establishment of a process to ensure exempt bank files were subject to ongoing review on a two year basis. In addition to being prescribed under RCMP exempt bank policy, this commitment was embedded as a compliance mechanism in the *Regulatory Impact Analysis Statements* that accompanied the applications for exempt bank designations.

3.24 These systematic reviews are to be undertaken for the purpose of assessing whether a file meets the test for exempt banks status. Where a determination is made that the threshold has not been met, RCMP policy stipulates that the information must be extracted from the bank.

3.25 The RCMP has a designated form (reference 2893) to capture the results of the two-year reviews. This form records whether the file qualifies for continued inclusion in the exempt bank – or alternatively that it no longer meets the criteria – the name of the reviewing officer,

and the date upon which the examination was completed. It also records the date of the next scheduled review.

3.26 While there were exceptions (paragraphs 3.15 and 3.17 refer), the files selected for examination generally contained the above-referenced form, capturing the results of the RCMP's internal review. However, compliance with the policy was largely ignored prior to 2006. Of the exempt bank files opened prior to 2004, approximately 70% of the national security files and 90% of the criminal operational intelligence files that we examined had not been subject to ongoing review.

3.27 In the absence of information to suggest otherwise, it would appear that accountability for compliance with the exempt bank policy, insofar as ensuring that complete and regular reviews are undertaken, has not been clearly established and communicated. The importance of addressing this gap cannot be over-emphasized.

3.28 The responsibility for compliance should be well understood and properly enforced. Without clear accountability and enforcement, divisions – or detachments within divisions – may circumvent exempt bank policy requirements, deliberately or otherwise, without consequence.

3.29 **Recommendation**: The RCMP should establish a sound organizational accountability structure for the management of exempt banks.

RCMP Response:

Agree.

- RCMP is committed to developing a sound governance structure.
- The model will be an integrated accountability structure with our National Security Criminal Investigations / Criminal Intelligence and the Access to Information and Privacy Branch; specific accountabilities within the model will be identified.

Overpopulated Repositories

3.30 Criteria for the placement and retention of a file in either the criminal operational intelligence or the national security investigation exempt bank is established under section 18 of the *Privacy Act* and is supplemented by RCMP exempt bank policy.

3.31 As noted in paragraph 3.14 of this report, the RCMP has removed a significant number of files from both exempt banks over the past year and a half. Notwithstanding the Force's efforts in this regard, we believe the banks remain overpopulated.

3.32 For each file within the audit sample we measured compliance with the requirements of the *Privacy Act* and the standard established under the RCMP's exempt bank policy.

3.33 **Section 18 Requirements**. To qualify for inclusion in an exempt bank, a file must consist predominantly (or more than half) of personal information that could be exempted under sections 21 or 22 of the *Privacy Act*.

3.34 Treasury Board (TBS) policy describes section 21 and paragraph 22(1)(b) as discretionary exemptions based on an injury test, whereas paragraph 22(1)(a) is described as a discretionary class test exemption.

3.35 Exemptions based on an injury test permit government institutions to deny access to information if the disclosure "could reasonably be expected to be injurious" to the interest specified in the exemption. Treasury Board policy describes "injury" as having a detrimental effect.

3.36 For discretionary class test exemptions, such as paragraph 22(1)(a) of the Act, there is no requirement to prove injury. The institution need only demonstrate that the information falls within the category (class of information) described in the section.[21]

3.37 **Internal Policy Standard.** The RCMP's internal policy establishes the injury test under paragraph 22(1)(b) of the *Privacy Act* as the standard for inclusion in either of the two exempt banks. The policy is silent on the use of the discretionary class test in paragraph 22(1)(a). And with respect to national security exempt bank files, the policy is also silent on the injury test available in section 21 of the Act.[22]

3.38 Paragraph 22(1)(b) provides that a government institution may refuse to disclose personal information if the disclosure could reasonably be expected to be injurious to the enforcement of any law of Canada or a province, or the conduct of a lawful investigation. Examples of the types of information to which the exemption may apply are included in the Act. They are:

- information relating to the existence or nature of a particular investigation;
- information that would reveal the identity of a confidential source of information;

21 Treasury Board policy states: "Despite being applicable to a class of information, paragraph 22(1)(a) is a discretionary exemption. Government institutions should, therefore, consider the disclosure of personal information covered by this exemption if they are satisfied that no injury will result from disclosure."

22 The National Security Investigations Records Exempt Bank was designated as exempt, by Order in Council (PC 1993-1034), on the basis of sections 21 and 22 of the *Privacy Act*.

– information that was obtained or prepared in the course of an investigation.

3.39 The injury test under paragraph 22(1)(b) is applied – at the RCMP divisional level – when a file is initially placed in the criminal operational intelligence or national security exempt bank. It is also applied when the file becomes subject to periodic examination (ongoing two-year reviews). The RCMP's exempt bank policy sets out a number of tests and considerations to assist staff in applying the injury test.

3.40 **Predominance test is not met in all cases.** In measuring compliance under the *Privacy Act*, we applied all of the authorities available to the RCMP under sections 21 and 22, including the discretionary class test exemption under paragraph 22(1)(a) of the Act.

3.41 While not pervasive among the audit sample, we found some files in both exempt banks that did not meet the predominance requirement established under section 18 of the *Privacy Act* (examples provided below in Exhibit D).

Exhibit D: Predominance Test

The following are illustrations of exempt bank files that do not meet the predominance requirement established under section 18 of the *Privacy Act*.

- File retaining policy related records on tips received under the Crime Stoppers program. No specific tips are referenced on the file.
- File opened to store documents related to the RCMP's attendance at a Canada-US Security Fraud Enforcement Conference in 1998.
- File containing documents relating to a fraud investigation involving a corporate entity. No personal information contained therein.
- File containing information regarding several protests and demonstrations being planned to mark the anniversary of a specific event.

3.42 As noted in paragraph 2.3 of this report, *each file* within an exempt bank must consist predominantly of personal information described in section 21 or section 22 of the *Privacy Act*. Section 18 is explicit in this regard. The inclusion of any file in an exempt bank that does not satisfy this requirement is in non-compliance with the Act.

3.43 **Non-compliance with exempt bank policy threshold**. Of the 116 files that we examined, approximately 50% of the national security files and 60% of the criminal operational intelligence files did not, in our view, meet the established threshold for continued exempt bank status under RCMP policy. Examples of national security exempt bank files are found in Exhibit E. We also observed files the inclusion of which in an exempt bank was assessed as questionable.

3.44 The files at issue related to investigations that had been concluded (closed) for an extended period of time and the rationale for continued exempt bank status – from either a criminal intelligence or national security intelligence perspective – was not self evident.

3.45 We also noted instances where the status of the information had changed (e.g. had become public, led to prosecution, etc.), as well as files that were designated as exempt solely on the basis that the information had been provided by a third party.

Exhibit E: National Security Investigations Exempt Bank Files

A frustrated vacationer

The subject and his wife travelled to New York for a 15-day bus tour through the United States and Canada. On the first day of the tour, the couple was late returning to the bus following a sight seeing excursion. The tour bus departed without them. Upon returning to the hotel, the subject confronted the tour guide about being left behind.

Seven days later the tour was on a stopover in Canada. As travellers were returning to the bus, the subject approached the bus driver and commented that the tour guide was running late and the driver should depart without her. When the driver refused, the subject threatened to hijack the bus. He then returned to his seat. No further incident occurred and the bus tour continued. The driver reported the incident to his employer the following day.

Approximately four days later the tour was en route back to the United States. While at the Canadian border, the bus driver contacted US Customs and reported the incident that occurred four days earlier. US Customs authorities notified the RCMP, but the bus had departed prior to the RCMP's arrival. When the tour bus arrived at US Customs, the individual was searched, handcuffed and placed in a holding cell prior to questioning.

As the alleged incident occurred in Canada and there was an apparent lack of criminal intent, prosecution was not pursued. The file was concluded approximately five years ago.

Concerned citizens

A resident alleged that an individual entered a rooming house in the neighborhood. Believing that drugs may have been involved, the resident contacted the police. The investigation revealed that the individual had dropped off his daughter at school (down the street from the rooming house), and he had stepped out of his car to have a cigarette. The file was concluded approximately seven years ago.

In another case, a neighbor observed two males carrying something that resembled a large drum, wrapped in canvas, into their house. The local police force with jurisdiction investigated. Officers examined the individuals' automobile and house. Items for export were found in the car. No item matching the description provided by the neighbor was located during the search. The file was concluded approximately five years ago.

An unreliable source

An individual contacted the police to report that three individuals identified as suspects on "America's Most Wanted" were working in Canada. The source also alleged that the individuals were sympathizers of a militant group.

The RCMP's attempt to interview the source met with negative results. The home address and telephone number provided by the source were not his, and the investigation revealed that they never were.

The source's motivation for contacting the police is unknown. He may have genuinely believed that he saw the individuals identified on the television broadcast. Alternatively, he may have orchestrated the incident to cause trouble for the three individuals. What is known is that he deliberately misled the police, suggesting that his intentions were less than honourable. The file was concluded over six years ago.

The consequence of exercising poor judgment

The subject was selected to participate in a youth project. Participants were provided with access to an e-mail site to facilitate communication with each other. In an e-mail to other participants, the subject made a threat against senior government officials. He was subsequently dismissed from the project.

When interviewed by police, the individual indicated that he didn't realize his comments would be taken so seriously. He was cautioned about the potential consequences of his actions. In the end, the RCMP concluded that the subject did not pose a threat. The file was closed approximately seven years ago.

3.46 In our view, advancing a compelling argument to support the exempt bank status of the above files – and many others that we observed – would be challenging. Our assessment in this regard – as it relates to criminal operational intelligence exempt bank files – was affirmed through an examination of files that had been removed from the bank during the RCMP's internal review. Included among the grouping

were investigative files relating to individuals who had been implicated in drug trafficking, human smuggling and money laundering activities.

3.47 As for the factors that contributed to the high percentage of non-compliant files among the audit sample, many appeared to be the product of members' unfamiliarity with the exempt bank policy – and more importantly, limited experience in terms of its application.

3.48 With regards to national security exempt bank files, it should be noted that in the immediate aftermath of September 11, 2001, there was a significant redeployment of resources to the RCMP's national security mandate. This redeployment and the operational pressures led to challenges in training and oversight regarding the classification (scoring) of some national security files. This may have resulted in the inappropriate scoring of files and their inclusion in the exempt bank.

3.49 While not verified through interviews, our analysis would suggest that in assessing whether a file warranted exempt bank status, the reviewing officer may have been influenced by an assumption that extraction from the exempt bank renders a file accessible. It does not.

3.50 The removal of a file from an exempt bank – or the revocation of the entire bank's exempt status – does not translate into the inability to protect sensitive information. While the treatment of an open bank involves a change in terms of the manner in which personal information requests are processed, there is no change insofar as the authority to withhold information is concerned.

3.51 Losing exempt bank status means that a file can be exempt only after a specific, new examination and not merely because it is retained in a bank designated as exempt. In other words, the institution is required to examine the file and justify denying access through the application of the exempting provisions contained in the *Privacy Act*; it cannot reject the request automatically because of the privileged position of an exempt bank.

3.52 It is also worth emphasizing that removing a file from an exempt bank does not preclude its subsequent reinsertion should circumstances arise to warrant it. As this is not reflected in the RCMP's exempt bank policy, there may have been a lack of awareness among those involved in the internal review. Consequently, examinations may have been undertaken without the benefit of information that could have been pivotal in assessing the relative merits of retaining or extracting a file from the bank.

3.53 **Privacy expertise under-utilized**. Within federal departments and agencies, personnel of the access to information and privacy units (ATIP) act as privacy advocates, educators, and arguably the leading authority in terms of the entity's compliance with the *Privacy Act* and associated internal and external (TBS) policies.

3.54 We were struck by the seemingly passive role of the ATIP unit in the RCMP's internal review. As the resident privacy and exempt bank policy experts, we expected the unit to be fully engaged. It was not. Rather, its role appeared limited to that of consultant, offering advice and guidance only when requested to do so.

3.55 In our view, an active ATIP presence would have had much more success in bringing about an awareness of exempt bank policy requirements. By extension, it is likely to have had a direct and measurable impact on the effectiveness of the internal review.

3.56 **Good practices identified.** A number of positive observations warrant reporting. The audit included an examination of source/witness protection files. These files contain debriefing reports and information relating to the management of confidential sources. Without exception, the files were found to be in compliance with section 18 requirements and associated RCMP policies. We therefore conclude that the control framework for managing these files is working well.

3.57 The efforts of the Niagara Regional Detachment should also be acknowledged. In September 2006 the detachment examined its exempt bank holdings as part of the RCMP's internal review. Fifty (50) files were identified for continued inclusion in the bank. These files were re-evaluated in March 2007.

3.58 At that time, 47 of the 50 files were removed from the exempt bank. The detachment recognized the merit of a conducting a further (second) review and the appropriate action was taken. The results confirm that it was time well spent.

3.59 **Recommendation:** The RCMP should develop a strategy for ensuring that all files within its exempt banks comply with the requirements of section 18 of the *Privacy Act* and associated internal exempt bank policy. This strategy should include:

- Further examination of the files retained in Exempt Personal Information Banks CMP PPU 015 and CMP PPU 025; and
- The provision of training to the managers and staff selected to participate in the examination.

For quality assurance, we suggest that the ATIP Directorate assume a lead role in this exercise.

Further, we request that the compliance strategy be provided to the OPC within 90 days after our final audit report is issued.

RCMP Response:

Agree.

A strategy will be provided to the Privacy Commissioner within 90 days to ensure that the Exempt Banks comply with the requirements of section 18 of the Privacy Act and associated internal exempt bank policy. Major components of the strategy include:

- Exempt bank training that has already been incorporated in the National Security Criminal Investigator Course and will be incorporated in future courses for Criminal Intelligence personnel;
- Developing an accredited "Train-the-Trainer" work shop;
- Giving priority training to those selected to participate in the further examination of the files retained in the Exempt Banks; and
- Conducting a further examination of the current content of the Exempt Banks.

For other elements of the strategy, see also RCMP Responses to Recommendations #3.66, 3.72, 3.82.

File Status Is Not Consistently Reconciled

3.60 To facilitate our on-site examination activities, we were provided with electronically generated listings of exempt bank documents and files. These were subsequently used to randomly select records for review.

3.61 Of the 153 files initially selected for examination, approximately 14% (21 criminal intelligence files and one national security file) had been removed from the exempt bank during the RCMP's internal review.

3.62 When a determination is made to extract a file from an exempt bank, the file coding (OSR code) is amended to reflect the file's non-exempt status as well as its revised retention period. In the cases referenced above, the files were removed from the bank and no subsequent action was taken to ensure the OSR code was modified in the applicable database.

3.63 Our observations mirrored those of the RCMP's internal review. Some divisions found files that were recorded (electronically scored) as exempt, but were associated with files that had been extracted from the exempt banks. There were also reports of files that were incorrectly scored as exempt at the time of their creation.

3.64 Where the OSR coding of an electronic file differs from its corresponding hard copy (paper) file, there is a risk that personal information may be retained longer than it should be. Subject to legal requirements, personal information should only be retained as long

as necessary to fulfill the purpose(s) for which the information was obtained.

3.65 Upon reaching the expiration of its established retention period, the information, regardless of the medium in which it is stored, should be destroyed.[23] Any further retention may result in prejudice against the individual to whom the information relates. In our view, this underscores the importance of ensuring the status of files is accurately reconciled electronically.

3.66 **Recommendation**: To facilitate ongoing monitoring of exempt bank files, and to ensure that files are disposed of in accordance with established schedules, the RCMP should implement means to ensure the status of files is accurately reflected in the applicable databases.

RCMP Response:

Agree.

Status of files will be accurately reflected in the applicable data bases by:

- Centralizing the review mechanism for files being considered for Exempt Bank status, including their disposal as per established schedules;
- Ensuring that the status of files is accurately reflected in both automated and hard copy files;
- Continuing to use the current "secure" and "non-secure" Police Reporting Occurrence System (PROS); this automated system has a built in accountability and review mechanism for files designated as "exempt".

Lack of Internal Monitoring and Audit

3.67 The RCMP's exempt bank policy states that compliance will be monitored by internal audit and by ATIP during the review process for an access request. Although the exempt banks were considered as a component of the National Security Operations Management Control Framework Audit in 2007, no comprehensive compliance review has been conducted by the RCMP since the creation of the exempt banks.

3.68 When an exempt bank file becomes the subject of a *Privacy Act* request, the file is reviewed to verify that its exempt status has been assessed every two years as prescribed under RCMP policy, and the information contained therein continues to satisfy exempt bank criteria. If one of

23 This does not apply to personal information that has been designated by the National Archivist as having archival or historical value. Upon surpassing its scheduled retention period, such information is transferred to the control of Library and Archives Canada.

these conditions is not met, the file is removed from the exempt bank and processed accordingly. The frequency with which this occurs is not recorded by the ATIP unit. In our view, capturing such data would be valuable for trends analysis and compliance monitoring purposes.

3.69 While we acknowledge the ATIP process as a control feature within the compliance framework, it must be noted that such reviews are limited to the files that have become the subject of a *Privacy Act* request. This represents a small percentage of the exempt bank population. Using fiscal year 2005-2006 as a baseline, the RCMP responded to 1,631 privacy requests. The exempt bank provision, subsection 18(2) of the Act, was invoked in four instances.[24]

3.70 The failure to properly maintain an exempt bank can result in the revocation of its exempt status. The absence of ongoing monitoring and regular audit is, therefore, surprising. In our view, auditing for compliance should have been as much a part of internal audit as routine financial or management audits.

3.71 As monitoring compliance with personal information management policies generally calls for both auditing and privacy competencies, it would appear logical that responsibility for the exempt bank policy remain shared. That said, we believe there is a compelling argument to support designating ATIP as the responsibility centre – with the requisite auditing powers and resources. We would encourage the RCMP to assess the feasibility of such an approach. Absent a formal audit mandate, we suggest that ATIP be actively involved in exempt bank reviews undertaken by internal audit.

3.72 **Recommendation:** The RCMP should seek to include exempt bank related compliance audits in future plans and priorities. It is further recommended that consideration be given to having the ATIP Directorate engaged in such reviews.

RCMP Response:

Agree.

Based on assessment of risk, the Exempt Banks will be considered in future audit planning. The RCMP is committed to:

- Developing a Quality Assurance National Review Guide for Exempt Banks to assist units in their mandatory annual Unit Level Quality Assurance (ULQA) process; and
- Conducting an internal review of its Exempt Banks every two years.

24 Public Safety and Emergency Preparedness Canada, Annual Report 2005-2006, *Access to Information Act and Privacy Act*, Statistical Reports – Departments and Agencies, p. 68.

Project Shock

3.73 The RCMP's immediate response to the events of 9/11 was an effort to coordinate all tips that had been received concerning the terrorist attacks in New York, Washington and Pennsylvania.

3.74 Referred to as Project Shock, the effort was coordinated by the National Security Intelligence Branch at RCMP HQ. Each tip was investigated and concluded in the same manner as a normal investigation.[25]

3.75 Separate files were opened when a Project Shock tip spawned a criminal investigation relating to national security. This was done in order to address the issue of disclosure at the completion of the investigation. If this approach had not been adopted, it could have resulted in having to disclose the entire Project Shock file as part of mandated court disclosure.

3.76 The Project Shock file was opened as an investigation into the "Threat or Use of Violence by an Organization or Organizations". All records relating to such investigations are retained for a minimum of ten years. The Project Shock file forms part of the National Security Investigations Records exempt bank.

3.77 Given the extensive information holdings, Project Shock was not examined as part of this audit. However, a sampling of records was examined by our office in 2002. We found that tips generally related to suspected terrorist affiliations, suspicious persons or suspicious activity. Each file contained information concerning both the source and the subject(s) of the tip.

3.78 We noted that a number of tips appeared innocuous in nature, and in some cases seemed to amount to little more than public hysteria during a time of crisis. Nevertheless, as such tips constituted part of the Project Shock investigation file, they remained in the exempt bank and became subject to a minimum ten year retention period.

3.79 While files were not examined as part of this audit, we did advance lines of inquiry in May 2007 to verify that Project Shock had been examined during the RCMP's internal review, and each tip file had undergone an assessment to determine whether it warranted continued exempt bank status. These inquiries became moot with subsequent events (reported below).

3.80 In June 2007 the audit team met with senior managers of the National Security Investigations Directorate to discuss Project Shock. At that time, the RCMP acknowledged that the file contained information that may no longer be relevant from a national security intelligence

25 We were informed that the RCMP received in excess of 10,000 tips.

perspective. A full examination is therefore being undertaken by the RCMP, the purpose of which is to identify and extract information that does not satisfy the criteria for continued inclusion in the national security exempt bank. The review was expected to be completed by November 2007.

3.81 Mindful that the Project Shock file touches thousands of Canadians, the RCMP's decision to undertake the review is important and welcomed.

3.82 **Recommendation**: We request that the RCMP report the results of the Project Shock review to the Privacy Commissioner of Canada.

RCMP Response:

Agree and completed on September 13, 2007.

- All documents were reviewed for compliance and none were found to meet the criteria for continued inclusion in the Exempt Bank; therefore, the Project Shock file has been removed from the Exempt Bank.
- While many documents were found to have originally been properly placed within the bank, subsequent investigative actions, media exposure, and the passage of time have served to render the information either innocuous, exposed through other means, or adequately protected under other available processes.
- Upon expiry of the institutional retention period, in this case 10 years, and in accordance with the *Library and Archives of Canada Act* and agreements for the transfer of records with the Librarian and Archivist, the file will be either purged or transferred to the control of the Library and Archives of Canada.

Reliability of Data and Use of Data Brokers

3.83 While conducting our examination of exempt bank files, attention was given to noting whether the information contained therein had been subject to a reliability assessment prior to placement on file. We also noted instances where the services of data brokerage entities had been utilized.

3.84 Data reliability. RCMP sources of information are generally assessed and rated for reliability in one of four categories: reliable, believed reliable, unknown reliability or doubtful reliability.

3.85 Within the audit sample, information received from human sources was consistently assessed and assigned a reliability rating.

3.86 In terms of information obtained from domestic and foreign law enforcement and security agencies, we found that the information

was generally deemed to be reliable unless otherwise indicated. For the most part, the originating agency provided the source from which the information or intelligence was collected (e.g. database traces, surveillance activities, search warrant, etc.). Information obtained from confidential sources was consistently assessed for reliability.

3.87 Data Broker Use. Data brokers can be defined as private sector entities or individuals who collect, and sometimes analyze, personal information for the purpose of developing and selling data products. This may involve the use of financial, credit, health or other personal information that can be linked to specific individuals.

3.88 The RCMP has contractual agreements with a number of consumer information services. The information available through these data brokerage entities includes: commercial reports for public and private companies, and contact information (address and telephone numbers) for consumers and businesses.

3.89 Our inquiries revealed that the extent of data broker usage within the RCMP varies depending on the mandate of the operational unit. For example, RCMP Commercial Crime Units may prepare economic profiles on individuals and public or private companies in the course of a bankruptcy investigation.

3.90 We identified three files within the audit sample that involved the services of a data broker. All three were for the purpose of obtaining either address or telephone information.

3.91 The RCMP reported that the utilization of open source data is a complement to the intelligence/investigative process and is only considered as a secondary source of information of unknown relevance, accuracy and reliability. Accordingly, we understand that no action is undertaken solely on the basis of such information.

3.92 At this time we have no further observations to make. Our office is currently engaged in an information-gathering exercise to enhance our understanding of the extent to which data brokerage services are used throughout federal departments and agencies.

Conclusion

4.1 In 1986-87 the Office of the Privacy Commissioner conducted an audit of the RCMP's Criminal Operational Intelligence Records Exempt Bank. That audit found that the bank was not in compliance with section 18 of the *Privacy Act*.

4.2 Recognizing the flaws that undermined the validity of the exempt bank order that existed in the late eighties, the RCMP implemented a number of policy and procedural changes for the maintenance of its exempt banks.

4.3 While a comprehensive framework for managing the banks exists, key control features – such as prescribed ongoing reviews and compliance monitoring – were largely ignored prior to 2006. As a result, files remained in the exempt bank without cause from either a national security or criminal intelligence perspective.

4.4 The primary reasons for the non-compliant state of exempt banks are: a lack of a well defined accountability infrastructure, a general lack of awareness of exempt bank policy, and the absence of ongoing monitoring and regular audit.

4.5 The RCMP must develop a strategy to verify that its current exempt bank holdings comply with the requirements of section 18 of the *Privacy Act* and associated internal policies. The Access to Information and Privacy Directorate should be fully engaged in this exercise.

4.6 Accountability for the management of exempt banks must be clearly defined and enforced. Furthermore, as policy observance is key to maintaining the integrity of the files over time, exempt bank compliance audits should be included in future plans and priorities of the RCMP.

Annex A

Audit Criteria

Collection Section 4 of *Privacy Act*	• No personal information shall be collected unless it relates to an operating program or activity of the institution. • The information in an exempt bank will be reviewed to determine that it is an authorized collection and consistent with a mandated activity of the institution.
Retention & Disposal Subsection 6(1) of *Privacy Act*	• Personal information must be retained and disposed of in accordance with approved records and retention and disposal schedules. • Except as otherwise provided in law, or when the individual consents to earlier disposal, personal information that has been used in a decision-making process that directly affects the individual must be retained for a minimum of two years after the last time it was so used. • Records should be properly disposed of in a manner consistent with their security classification and in accordance with the *Privacy Act Regulations* and related directives (i.e. Treasury Board Privacy Policies and the Government Security Policy).
Use Section 7 of *Privacy Act*	• Without the consent of the individual to whom it relates, personal information shall be used by a government institution for the purpose for which it was collected, or for a use consistent with the original purpose, or for a purpose for which the information may be disclosed under subsection 8(2) of the *Privacy Act.*
Disclosure Section 8 of *Privacy Act*	• Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed to a third party except in the limited number of circumstances established under subsection 8(2) of the *Privacy Act.*
Index of Personal Information Sections 10 and 11 of *Privacy Act*	• The head of an institution must include all personal information in personal information banks, which must include a description of: the purpose(s) for which the information was obtained or compiled and the uses consistent with said purpose(s), the retention and disposal standards applicable to the personal information, and an indication that the bank was designated as exempt by an order under section 18 of the Act (and the provision of section 21 or 22 on the basis of which the order was made).
Access Section 16 of *Privacy Act*	• Where the head of a government institution refuses to give access to any personal information, the head of the institution must notify the individual and advise them that the information does not exist or the grounds on which it has been refused or could be refused. • The organization must actually review the information in question to ensure that the appropriate exemption is applied. In the case of exempt banks, the information must also be reviewed to ensure that it is properly included in the exempt bank.

Annex B

Organization Structure of the RCMP – Divisions

A Division	**National Capital Region**
B Division	**Newfoundland and Labrador**
C Division	**Quebec**
D Division	**Manitoba**
E Division	**British Columbia**
F Division	**Saskatchewan**
G Division	**Northwest Territories**
H Division	**Nova Scotia**
J Division	**New Brunswick**
K Division	**Alberta**
L Division	**Prince Edward Island**
M Division	**Yukon Territory**
O Division	**Ontario**
V Division	**Nunavut Territory**
X Division	**Headquarters**

Annex C

Legislation – *Privacy Act*

EXEMPT BANKS

Governor in Council may designate exempt banks	**18.** (1) The Governor in Council may, by order, designate as exempt banks certain personal information banks that contain files all of which consist predominantly of personal information described in section 21 or 22.
Disclosure may be refused	(2) The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that is contained in a personal information bank designated as an exempt bank under subsection (1).
Contents of Order	(3) An order made under subsection (1) shall specify (a) the section on the basis of which the order is made; and (b) where a personal information bank is designated that contains files that consist predominantly of personal information described in subparagraph 22(1)(a)(ii), the law concerned. 1980-81-82-83, c. 111, Sch. II "18".

RESPONSIBILITIES OF GOVERNMENT

International affairs and defence	**21.** The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada, as defined in subsection 15(2) of the *Access to Information Act*, or the efforts of Canada toward detecting, preventing or suppressing subversive or hostile activities, as defined in subsection 15(2) of the *Access to Information Act*, including, without restricting the generality of the foregoing, any such information listed in paragraphs 15(1)(*a*) to (*i*) of the *Access to Information Act*. 1980-81-82-83, c. 111, Sch. II "21".
Law enforcement and investigation	**22.** (1) The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) (a) that was obtained or prepared by any government institution, or part of any government institution, that is an investigative body specified in the regulations in the course of lawful investigations pertaining to (i) the detection, prevention or suppression of crime, (ii) the enforcement of any law of Canada or a province, or (iii) activities suspected of constituting threats to the security of Canada within the meaning of the Canadian Security Intelligence Service Act, if the information came into existence less than twenty years prior to the request; (b) the disclosure of which could reasonably be expected to be injurious to the enforcement of any law of Canada or a province or the conduct of lawful investigations, including, without restricting the generality of the foregoing, any such information (i) relating to the existence or nature of a particular investigation, (ii) that would reveal the identity of a confidential source of information, or (iii) that was obtained or prepared in the course of an investigation; or (c) the disclosure of which could reasonably be expected to be injurious to the security of penal institutions.
Policing Services for provinces or municipalities	(2) The head of a government institution shall refuse to disclose any personal information requested under subsection 12(1) that was obtained or prepared by the Royal Canadian Mounted Police while performing policing services for a province or municipality pursuant to an arrangement made under section 20 of the Royal Canadian Mounted Police Act, where the Government of Canada has, on the request of the province or municipality, agreed not to disclose such information.
Definition of "investigations"	(3) For the purposes of paragraph (1)(b), "investigation" means an investigation that (a) pertains to the administration or enforcement of an Act of Parliament; (b) is authorized by or pursuant to an Act of Parliament; or (c) is within a class of investigations specified in the regulations. 1980-81-82-83, c. 111, Sch. II "22"; 1984, c. 21, s. 90, c. 40, s. 79.

REVIEW OF EXEMPT BANKS

Investigation of exempt banks	**36.** (1) The Privacy Commissioner may, from time to time at the discretion of the Commissioner, carry out investigations of the files contained in personal information banks designated as exempt banks under section 18.
Sections 31 to 34 apply	(2) Sections 31 to 34 apply, where appropriate and with such modifications as the circumstances require, in respect of investigations carried out under subsection (1).
Report of findings and recommendations	(3) If, following an investigation under subsection (1), the Privacy Commissioner considers that any file contained in a personal information bank should not be contained therein within the terms of the order designating the bank as an exempt bank, the Commissioner shall provide the head of the government institution that has control of the bank with a report containing (a) the findings of the Commissioner and any recommendations that the Commissioner considers appropriate; and (b) where appropriate, a request that, within a time specified therein, notice be given to the Commissioner of any action taken or proposed to be taken to implement the recommendations or reasons why no such action has been or is proposed to be taken.
Reports to be included in annual or special reports to Parliament	(4) Any report made by the Privacy Commissioner under subsection (3), together with any notice given to the Commissioner in response thereto, may be included in a report made pursuant to section 38 or 39.
Review of exempt banks by Court	(5) Where the Privacy Commissioner requests a notice under paragraph (3)(b) in respect of any file contained in a personal information bank designated under section 18 as an exempt bank and no notice is received within the time specified therefor or the action described in the notice is, in the opinion of the Commissioner, inadequate or inappropriate or will not be taken in a reasonable time, the Privacy Commissioner may make an application to the Court under section 43. 1980-81-82-83, c. 111, Sch. II "36".

REVIEW BY THE FEDERAL COURT

Applications respecting files in exempt banks	**43.** In the circumstances described in subsection 36(5), the Privacy Commissioner may apply to the Court for a review of any file contained in a personal information bank designated as an exempt bank under section 18. 1980-81-82-83, c. 111, Sch. II "43".