TOP SECRET

File No.: 2800-133
(TD R468)

REVIEW OF A COUNTER INTELLIGENCE INVESTIGATION -

(SIRC STUDY 2007-02)

Security Intelligence Review Committee
August 22, 2008

TABLE OF CONTENTS

In Canada, CSIS believes the to run aggressive operations targeting economic, political, scientific and technical information.

1.1 Objectives and Methodology

The objective of this study was to examine the Service assess CSIS's performance in countering attempts to cultivate sources of information within the Government of Canada and to surreptitiously obtain economic intelligence and controlled technologies from Canadian businesses.

SIRC staff examined documentation pertaining to investigation within a review period of September 1, 2005 to September 30, 2006,

In addition, SIRC researchers met with the DG of Headquarters' and the Chief in March 2008. This meeting provided additional insight into the overall context

2 ASSESSMENT OF THE INVESTIGATION

All regions and CSIS headquarters report that they have sufficient resources to achieve their operational objectives.

Based on its analysis of the sample targets selected for this review, SIRC concludes that is professionally run with very few concerns. We believe the quality of this investigation is partly the result of strong operational planning and extensive experience in investigating the espionage threat posed by

targets and has had the opportunity to test and perfect investigative methodologies. As a result, it is often well positioned both to identify and counter new initiatives

Although there are many successes in this investigation, SIRC noted several challenges facing CSIS, such as: closing identified intelligence gaps;

2.1 Intelligence Gaps

CSIS regularly identifies intelligence priorities in its annual program plans.

2.5 Concerns

In addition to these challenges, SIRC's review found several issues associated with this investigation that require further consideration by CSIS. In Section 3, SIRC raises issues pertaining to CSIS's investigation of security concerns following the construction of a highly sensitive Department of National Defence (DND) facility. Based on our evaluation of CSIS's role, we also assess the effectiveness of CSIS's client-driven approach to site access security screening.

3 ISSUE 1: THE NORAD ABOVE GROUND COMPLEX

DND informed CSIS of a possible security breach during the construction of the North American Aerospace Defence Command (NORAD), Above Ground Complex (AGC) facility in North Bay, Ontario.

Under the Government Security Policy (GSP), responsibility for the security of this facility ultimately rests with DND. The policy also requires DND to report any identified security incidents to CSIS for investigation.[26]

SIRC examined CSIS's response to DND's reported security incidents. This examination is informed, in part, by the conclusions of two Office of the Auditor General of Canada (OAG) independent audits. The OAG confirmed in May 2007 that there were serious security lapses during the construction of the AGC and, in October 2007, identified significant flaws in the contracting and site-access security screening processes.

This section first explores CSIS's decision-making between September 2005 and September 2006, to determine why the Service responded

Second, and with consideration of the OAG's conclusions from October 2007, we assess whether CSIS's client-driven approach to site-access security screening is sufficient to meet the requirements of Canadian national security.

3.1 Background

The NORAD air defence system, established in 1958 as a bilateral international agreement between Canada and the United States, is an integrated network of air defence radar systems that seeks to prevent air attacks against North America, tracks

[26] Canada, *Government Security Policy*, Section 10.15.

air targets and responds to unauthorized air activity.[27] DND is responsible for Canadian operations and runs NORAD institutions in Winnipeg and North Bay, Ontario. All NORAD facilities, including the US headquarters in Colorado Springs, Colorado, have interconnected computerized systems that process information, identify targets and guide the interception of threats.[28] A serious security breach can have considerable and wide-ranging implications for the North American air defence system.

3.2 History of the Case

The construction of a new Above-Ground Complex (AGC) was first proposed in 1998 as part of a broader NORAD modernization project. In 2003, DND expanded its original plans for the facility and intended the AGC to replace the existing North Bay NORAD facility.[29] The new complex was designed to be highly secure

The contract for construction was awarded to an Etobicoke-based company, Bird Construction, in October 2003, and construction was completed in October 2006.[31]

CSIS information indicates that DND personnel first raised concerns regarding the security of the AGC before 2003.

---

27 North American Aerospace Defence Command (NORAD), "About Norad," <http://www.norad.mil/about/vision.html>.

28 Office of the Auditor General of Canada (OAG), *Report of the Auditor General of Canada to the House of Commons*, "Chapter 6: Modernizing the NORAD System in Canada – National Defence," May 2007: Para 6.4.

29 Chapter 6 of the May 2007 Auditor General report discusses the period between 1999 and 2003 in paragraphs 6.51-6.52.

30 and OAG, *Report of the Auditor General of Canada to the House of Commons*, "Chapter 1: Safeguarding Government Information and Assets in Contracting," October 2007: Para. 1.74.

31 Department of National Defence, "Contract Awarded for Final Phase of Modernization of NORAD Operations Centre," News Release NR-03.018, October 14, 2003; Defence Construction Canada, "Moving On Up at 22 Wing North Bay," *DCC at Work* Vol. 5(5): 2. Defence Construction Canada is a crown corporation with a mandate to provide contracting, construction contract management and other services to DND.

3.3 Findings of the OAG

The OAG published reports in May and October 2007 that, in part, discussed the security incidents related to the NORAD AGC facility.[40] The May report listed the following items as security concerns: (a) the release of the blueprints into the public domain; (b) the physical control and access to the building site during construction; and, (c) the security clearance of workers. The OAG found that DND,

> had not completed a review of the building security requirements prior to construction. National Defence requires that a security checklist be completed for new buildings to ensure that security concerns are identified and addressed. Department officials told [the OAG] that due to time and budget constraints, this step was not taken. Several security concerns did arise during construction that have led to questions about the building and the subsequent feasibility of operating in it.[41]

The October report focused on the adherence to the Government Security Policy (GSP) in contracting processes by Public Works and Government Services of Canada (PWGSC), the RCMP and DND.[42] This report also discussed the NORAD AGC case.[43] The OAG revealed a disturbing trend in DND's contracting practices: 99 per cent of over 8,500 contracts awarded between April 2002 and March 2007 were not subject to security assessments as required by the GSP.[44] As a result, the OAG concluded that

---

40 The focus of this report was DND's NORAD modernization program between 1997 and 2006.

41 OAG, May 2007; Para. 6.55. This corroborates information SIRC found in CSIS documentation.

42 OAG, October 2007, Para. 1.13. The PWGSC is the lead agency for government contracting purposes and operates a program called the Industrial Security Program (ISP). See OAG, October 2007, page 1.

43 OAG, October 2007, Para. 1.13-1.14.

44 OAG, October 2007, Para 1.73. The DND's partner DCC is not formally bound to the GSP because it is not listed any of Schedules I, I.1 or II of the *Financial Administration Act* and is not subject to a Memorandum of Understanding with DND that establishes responsibilities. As a result, no obligation or responsibility for security has been formally conferred to DCC. See OAG, October 2007, Para 1.72.

there are no assurances that "contractors who received these contracts had been cleared" and that it is "unknown whether or not information and assets have been compromised."[45]

The OAG's findings are significant from a security perspective and situate the NORAD AGC case within broader pattern that reveal gaps in the Canadian security screening system. Despite having a primary role in the security screening system, CSIS is not a subject of the OAG audit and was not directly implicated in its findings or recommendations. Nevertheless, this revelation should be a concern for CSIS.

3.4 CSIS's Actions

The Government Security Policy (GSP) applies to all departments listed in Schedules I, I.1 and II of the *Financial Administration Act* (FAA).[46] Section 10.15 requires departments to report any security incident involving a threat to national interests to CSIS.[47]

In the case of the NORAD AGC, DND reported its security concerns to CSIS

a DND report on the matter that detailed the facts of the case.

---

45 OAG, October 2007, Para 1.73.

46 Canada, *Government Security Policy*, Sections 1 and 5. The Department of Public Works and Government Services and the Department of National Defence are both listed in Schedule 1 of the FAA.

47 GSP, Section 10.15.

3.4.1 Reluctance to Interfere in a DND Investigation

Despite its willingness to provide assistance in this matter, CSIS did not receive the necessary cooperation or disclosure from DND.

the GSP spells out jurisdiction in these matters: CSIS is the designated agency to investigate reports of security incidents involving threats to the national interest.[64] Drawing upon the *CSIS Act*, the GSP indicates that CSIS is responsible to "investigate and analyse physical and cyber threats to national security ... and provide related advice."[65] The GSP does not require CSIS to conduct an investigation: presumably, CSIS would assess the reported security incident against its investigative mandate under Section 12 of the *CSIS Act* SIRC suggests that the possibility of a breach at the NORAD AGC would meet the Section 12 threshold.

SIRC notes that CSIS is not prevented by the *CSIS Act* from launching an investigation before there is confirmation of a suspected threat. Section 12 establishes a threshold where CSIS "shall" collect information on "activities that may on reasonable grounds be suspected of constituting threats."

---

64 Section 10.15 requires incidents suspected of constituting criminal offenses be reported to law enforcement; possible compromises of Cabinet confidence to the Privy Council Office; incidents involving threats to national interest to CSIS; incidents affecting critical assets and services to the Office of Critical Infrastructure Protection and Emergency Preparedness; etc.

65 GSP, Appendix A, Section 4.1.

3.5 Security Screening by CSIS

The GSP requires all private sector organizations and individuals to have site access clearance to secure facilities, "prior to the commencement of duties."[68] The Auditor General's report has confirmed that none of workers on the AGC site received security clearances.[69] This is supported by CSIS records.[70]

---

68 GSP, Section 10.4 and 10.9.

69 OAG, May 2007, Para. 6.55.

70 CSIS Memo to SIRC, December 12, 2007, Response to Question 7.

Under Section 13 and 15 of the *CSIS Act*, as well as the GSP, the Service is responsible for providing security assessments on behalf of all Government of Canada institutions (except the RCMP) on persons whose work requires access to Government of Canada assets. The current procedure requires CSIS to carry out security these assessments "on receipt of a duly authorized request."[72]

CSIS does not advise clients of their obligations under the GSP. According to CSIS, "pursuant to 10.4 of the GSP, there are no provisions or requirements for the Service to advise [government], in advance, that any contractors hired to complete a project would require site access security clearances.[73]

In a case like the NORAD AGC, the failure of the client to request CSIS's services creates an exploitable security gap and therefore a potential Section 12 intelligence threat.[75]

In the past CSIS has stated that "new initiatives in Security Screening are client-driven and the product of interdepartmental discussions. ... In the course of these discussions, CSIS may provide advice on appropriate security procedures and related threat and risk assessments."[76]

---

72 CSIS, Ministerial Direction 2001 Compendium, Annex B, "Security Assessments and Advice to Ministers." This is also reflected in Appendix A, Section 4.1 of the GSP and CSIS OPS-108.1.2-1.3.

73 CSIS Memo to SIRC, December 12, 2007, Response to Question 6.

75 CSIS agreed with this assertion. See CSIS Memo to SIRC, December 12, 2007, Response to Question 6b.

there should be a standardized procedure for CSIS to advise departments on the necessity of security assessments and site access or security clearances.

SIRC recommends that CSIS consult with Treasury Board Secretariat to clarify its responsibility to investigate incidents reported under the GSP, and to explore the value of developing an enhanced interdepartmental liaison to advise departments of their responsibilities under the GSP for security screening.

SIRC recognizes that a proactive approach to security screening would not guarantee the prevention of security incidents; however, it would help CSIS to be better positioned and more informed should they occur.

The approach recommended above would not only clarify some of the jurisdictional confusion that was evident in this case, but would also address the security gap revealed by the OAG. SIRC therefore encourages CSIS to consider this recommendation as part of its future planning, including any discussions with Treasury Board about the Service's role in the GSP.[78]

[77] GSP, Appendix A, Section 4.1.

4 ISSUE 2: SOURCE SECURITY

Annex E of Ministerial Direction requires CSIS to manage its human sources so as to protect their personal safety and the security of CSIS operations.

6 CONCLUSION

SIRC believes that CSIS is uniquely positioned and qualified to advise and support the Government of Canada to ensure an effective security screening system. In this regard, CSIS should use their expertise as a basis to take a leadership role in developing policy that will correct the security gaps identified by OAG in its October 2007 report. We strongly recommend that CSIS assess whether its client-driven approach to site access security screening best responds to the needs of Canadian national security.

SUMMARY OF FINDINGS

- SIRC found no issues of compliance arising from its review of sampled targets, human sources or warrant powers executed between September 1, 2005 and September 30, 2006.

RECOMMENDATIONS

- SIRC recommends that CSIS consult with Treasury Board Secretariat to clarify its responsibility to investigate incidents reported under the GSP, and to explore the value of developing an enhanced interdepartmental liaison to advise departments of their responsibilities under the GSP for security screening.

LIST OF ACRONYMS

AGC	Above Ground Complex
DCC	Defence Construction Canada
DFAIT	Department of Foreign Affairs and International Trade
DND	Department of National Defence
FAA	*Financial Administration Act*
GSP	Government Security Policy
ISP	Industrial Security Program
NSA	National Security Agency
NORAD	North American Aerospace Defence Command
NATO	North Atlantic Treaty Organization
OAG	Office of the Auditor General of Canada
PWGSC	Public Works and Government Services of Canada
RCMP	Royal Canadian Mounted Police
STS	Science and Technical Services