TOP SECRET

File No.: 2800-169
(TD R521)

CSIS' WARRANTS

(SIRC STUDY 2012-01)

Security Intelligence Review Committee
April 19, 2013

TABLE OF CONTENTS

1 INTRODUCTION

In recent years, CSIS's ability to monitor the communications of individuals believed to represent a threat to national security has been enhanced through warrant power. This power allows the Service, with the assistance of the Communications Security Establishment Canada (CSEC), to intercept the telecommunications of Canadian targets travelling, or residing, abroad.

the acquisition of warrant power was described as a major achievement,

CSIS views the collection of information on targets travelling overseas, as filling a "blind spot" in its investigations.

This is SIRC's first examination of warrant power. The review examined the processes, policies and controls that CSIS has put in place to manage this new power, as well as CSIS's cooperation and exchanges with CSEC. The review also sought to evaluate how important the information obtained from warrants has been to the Service's investigations thus far.

35 warrants that included powers were issued during the review period.[2] The Committee found that CSIS encountered several challenges these included some technical issues,
the efficacy of collection;
control of the information collected; and, future expectations of CSIS concerning warrants.

There has been substantial progress since the first warrant was issued. However, CSIS is still in a learning phase and it will need to manage expectations against the realities, meaning limitations, of reporting from collection.

2 Plus 7 supplemental applications on existing warrants.

2 METHODOLOGY

This review examined all documents concerning internal processes and policies to manage powers, as well as all corporate documents relating to CSIS's cooperation with CSEC on the execution of the warrants. In addition, SIRC selected a sample of warrants for in-depth review.

SIRC also attended several briefings the Department of Legal Services, and the Assistant Director of Technology (ADT), to acquire knowledge on the evolving relationship between CSIS and CSEC.

The core review period for this study was from January 1, 2008 to December 31, 2011.

3 BACKGROUND AND EXECUTION OF WARRANTS

CSIS first applied for powers in a Section 21 warrant application in 2005. The warrant application was withdrawn for operational reasons and the Service tried again in 2007. The Federal Court dismissed the 2007 application stating that the Court did not have jurisdiction under the *CSIS Act* to issue warrants authorizing the Service to conduct investigative activities outside Canada. Following the 2007 decision, CSIS reconsidered the manner in which the case was articulated to the Court. After consultation with the Deputy Attorney General of Canada, the Service filed a second application in 2009 which was approved by the Court. Since that time, have requested powers, to ensure coverage of targets if they leave Canada.

powers involve the collection of signals intelligence, or SIGINT, which is information carried over global telecommunications systems Communications Security Establishment Canada (CSEC) is responsible for the collection of SIGINT. CSIS, has the mandate to investigate individuals, including Canadians, suspected of posing a threat to national security, Although CSEC cannot, in law, direct its activities against Canadians or at any person within Canada, it may provide assistance to security and law enforcement agencies acting under lawful authority.[3]

CSEC is part of a wider allied SIGINT community comprised of the United States' National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD), and New Zealand's Government Communications Security Bureau (GCSB) – the so-called Five Eyes. Given the global telecommunications network, and the sharing within the Five Eyes SIGINT community, CSIS must routinely leverage allies (or second party) assets in order to maximize collection under a warrant.

3 This activity falls under Mandate C of CSEC – Support to Lawful Access (SLA).

3.1 COLLECTION

4 CHALLENGES AND EXPECTATIONS

4.1 TECHNICAL CHALLENGES

4.1.1.1 CLASSIFICATION

4.1.1.2 EFFICACY

Relying on a partner agency for collection means that CSIS investigations will sacrifice some efficiency.

4.2 COVERAGE

SIRC found that there are clear advantages to leveraging second party assets in the execution of warrants, and indeed this is essential for the process to be effective. However, there are also clear hazards – including the lack of control over the intelligence and

In practice, if an allied agency were to pick up intelligence on a Canadian citizen, would ideally take the lead based on an informal agreement governing interactions amongst the Five Eyes SIGINT agencies. Nonetheless, it is understood that each allied nation reserves the right to act in its own national interest.

The risk to CSIS, then, is the ability of a Five Eyes partner to act independently on CSIS-originated information. This, in turn, carries the possible risk of detention or harm of a target based on information which originated with a CSIS

SIRC has seen indications that the Service has started using caveats that require allied agencies to contact CSIS in the event that information based on Service is to be acted upon.

These caveats, as they currently stand, are still considered a "work in progress" by the Service, but they do not yet address the wider reality of collection. **SIRC therefore recommends that CSIS extend the use of caveats and assurances in regards to collection, to include agencies in order to ensure that no dissemination occurs without the Service's knowledge.**

5 CONCLUSION

powers were introduced in order for the Service to maintain coverage of targets who represented a threat to Canada as they travelled or, in some cases, resided overseas.

In sum, CSIS faces several challenges in managing expectations

SIRC therefore advises that CSIS devise appropriate protections for the sharing of Service information, and keep itself as informed as possible concerning the potential uses of CSIS information.