TOP SECRET

File No.: 2800-177
(TD R531)

REVIEW OF SECURITY SCREENING

(SIRC STUDY 2013-01)

Security Intelligence Review Committee
December 13, 2013

TABLE OF CONTENTS

1 INTRODUCTION

Security screening is one of CSIS's primary responsibilities and also one of its most visible. As part of this function, the Service advises and assists the Government of Canada in preventing individuals who may pose a threat to Canada from obtaining either status or entry into Canada, as well as individuals who represent such threats from accessing sensitive sites, assets or information. This resource-intensive function includes the screening of immigrants and refugees who seek status in Canada, employees or contractors for the Government of Canada and members of the Canadian military who seek clearance. Ultimately, CSIS views security screening as a first line of defence against both terrorism and espionage.

SIRC has examined the process of security screening through its complaint function on a continuous basis, but it has been several years since SIRC has reviewed, overall, the Service's Security Screening Branch and related activities.[1] In this time, there have been several changes to the program, including initiatives to streamline the screening process, to improve the quality and consistency of screening products,

The review examines the key responsibilities of the Security Screening Branch (SSB) and the major changes that have been undertaken within the Security Screening program. Overall, SIRC found these initiatives to be very positive, particularly with respect to the efforts to standardize both screening procedures and products.

SIRC then turned its focus to how information collected for security screening is used and accessed for operational purposes. In particular, SIRC explored the implications and risk associated with CSIS's recent decision

1 SIRC Study 2006-07 Security Screening Outside of the Federal Government

2 METHODOLOGY

This review examined CSIS's activities related to the Security Screening program, which falls directly under the Deputy Director Operations and is one of the largest branches of the Service. SIRC looked at corporate, operational and policy documents,

In addition, SIRC held briefings with SSB to gain an understanding of the screening process, with the to understand its purpose, and with both Ottawa and Quebec Regions to better understand how the Service uses security screening information in their investigations of s.12 threats to the security of Canada.

The core review period for this study was January 1, 2010 to April 30, 2013, but SIRC examined documentation that fell outside this period in order to provide a complete assessment of relevant issues.

3 SECURITY SCREENING BRANCH

The mandate of the Security Screening program is to prevent individuals of security concern from gaining access to sensitive Canadian information, assets, sites or events, and to prevent the entry, or the acquisition of status in Canada, of non-Canadians who pose a security threat.[2] The Security Screening Branch (SSB) provides security assessments to other Government departments and security advice to Citizenship and Immigration Canada (CIC) and the Canadian Border Services Agency (CBSA) under the authorities of ss.13 and 14 of the *CSIS Act* respectively.

Under the Government Security Program (GSP), CSIS provides security assessments for all government departments and institutions, the Site Access program for airports, port and marine facilities, the Parliamentary Precinct and nuclear power facilities.[3] These assessments relate to a person's loyalty and reliability as it relates to loyalty as defined by the Treasury Board's Personnel Security Standard.[4] The Service only provides assessments or advice; the decision for granting, denying, suspending or revoking a clearance ultimately belongs to the requesting department or agency.

On the Immigration Screening side, CSIS provides advice to CIC and CBSA on individuals seeking residency status, both temporary and permanent, from inland and overseas, as well as those seeking visitor visas and Canadian Citizenship (*Citizenship Act s. 19*). Immigration and citizenship screening is focused on identifying individuals who pose a threat to the security of Canada or who could be inadmissible under the *Immigration and Refugee Protection Act* (IRPA).[5]

3.1 Modernization

In 2009, CSIS published its Business Modernization Plan (BMP) which formed the basis for many fundamental changes in CSIS's business practices and operations. SSB was not implicated in the BMP's process as its focus was on s. 12 operations. Recognizing a need to modernize independent of the BMP, in 2010, SSB instituted corporate changes to address several challenges including: an increasing volume of requests and growing

2 Security Screening Business Plan 2011-14 p. 3

3 CSIS Question Period Note 2012 03 07

4 Loyalty relates to whether an individual has engaged, or may be engaged in activities that constitute a threat to the security of Canada within the meaning of the CSIS Act. Reliability, as it relates to loyalty, is concerned with whether, because of a feature of character, association with persons or groups considered a security threat, or family or other close ties to persons living in oppressive or hostile countries, the individual may act or be induced to act in a way that constitutes a threat to the security of Canada, or that they may be induced or may be caused to disclose in an unauthorized way, classified information.

5 Section 34 of the *IRPA* includes such activities as: engaging in acts of espionage; subversion, terrorism; or being a member of an organization that there are reasonable grounds to believe engages or may engage in these acts.

demand for services; a lack of centralized accountability and corresponding performance standards; outdated or disjointed tools; and, "complex" business practices.[6] The new objective was described simply as "quality advice, on time" which has since become the motto and mission of SSB.

The Branch focused its efforts on Strategic Performance Initiatives (SPI) and National Program Development. The SPI focused on three categories: performance standards (timeliness, questionnaires, briefs, templates, etc.); accountability (semi-annual accountability regime, performance accountability framework); and business processes (wide range of efficiencies/improvements, better risk management).[7]

SIRC took note of two initiatives for improving performance standards. First, the Branch developed new templates for the reports that are sent to clients pursuant to security screening. In addition, SSB expanded the mandate of the

The National Program Development aimed at fostering a cohesive national strategy through regional visits, conferences, a Branch newsletter, improved case management tools and a Client Liaison function. Client Liaison is one of the top priorities of the Branch as "[n]o Service program is more client driven or more client sensitive than Screening, and liaison with GoC partners must be more strategic, systematic and standardized."[9] SSB currently has over 100 clients and focuses on educating and supporting external clients and other Branches within the Service, as well as measuring client satisfaction with Service assessments and advice.

Changes are still ongoing, but overall, they have been largely successful in creating more consistency and enhancing responsiveness. The Committee has also noted that the

6 From: Memorandum. "Security Screening Program – Update of Strategic Performance Initiatives and National Program Development." (File # 19000-45) 13 May 2011.

7 From: Canadian Security Intelligence Service, Security Screening Program Briefing to SIRC. 10 April 2013.

9 From: Memorandum. "Security Screening Program – Update of Strategic Performance Initiatives and National Program Development." (File # 19000-45) 13 May 2011.

inventory in screening has declined and that there has been a significant decrease in the number of complaints that SIRC has received on delays in security screening.
SIRC found the initiatives undertaken by SSB to be very positive, particularly the establishment of a quality control mechanism and increased standardization across the Branch and the Regions with respect to procedures and products.

3.2 Investigative Authorities

The Service is authorized to collect information and conduct investigations under three separate legislative authorities of the *CSIS Act*: ss. 12 (threats),15 (screening) and 16 (foreign states and persons). Section 12 authorizes the collection of information strictly necessary for investigating activities that may reasonably be suspected of constituting a threat to Canada. Screening investigations are for the purpose of providing security assessments pursuant to Government screening and advice pursuant to immigration screening.

However, there are two major differences between s. 12 and screening, namely the provision of consent by the subject of the interview and the rationale for collecting information.

In order to begin a screening investigation, a person must provide written consent for their personal information to be collected for the purposes of attaining a security clearance, site access or status in Canada. This is not the case with s. 12 investigations, where the information is collected without consent, for the purposes of determining if a person or group is a threat to Canada.[10]

The focus of s. 12 and screening interviews is also different. Screening interviews must focus solely on the individual applying for status or clearance, while s. 12 interviews

During SIRC's briefings, it was made clear that operationally the Service emphasizes the differences between s. 12 and screening to ensure that screening interviews are not used inappropriately to pursue s. 12 collection.[11]

The security assessments

10 Briefing Note: EDG SSB to DDO 29 11 2011

11 SIRC Briefing with Ottawa Region, July 12, 2013

or advice therefore contain only information relevant to screening.[12]

12 In other words, volunteered threat-related information that is not deemed relevant to the individual being interviewed, will not be included in the security screening report.

4 OPERATIONAL USE OF SECURITY SCREENING INFORMATION

The notion that CSIS has to protect personal information has been ingrained since its creation. In fact, the McDonald Commission stressed this point in its report. This discussion was timely, given that the *Privacy Act* was being written into legislation as the McDonald Commission was completing its work.

The Commission emphasized that while the Privacy Commissioner could review complainants' allegations of improper disclosure, "it is of the essence of security intelligence investigations that the subjects of such investigations be unaware of the investigation". For this reason "we believe *a system of prior approval, involving judicious application of a strict test of necessity*, is needed as a means of ensuring that government information about the personal details of one's private life, beyond those items that are generally public knowledge, is used for national security purposes *only when a clear case for the necessity of such use has been made*" [emphasis added]. The secretive nature of CSIS's information collection is precisely the reason why CSIS must be diligent in its use of personal information, specifically information collected under the umbrella of screening.

4.1 The *Privacy Act*

CSIS collects a great deal of information through its separate legislative authorities. Disclosure of personal information, even within an organization, is subject to protection under the *Privacy Act*. Whereas information collected under s.12 is done so without the knowledge or consent of individuals, under screening (including information collected in support of both Government and immigration), individuals provide *written, informed consent* for the Service to collect information for a specific purpose.

Personal information can be disclosed to an investigative body such as CSIS by following the requirements of paragraph 8(2)(e) of the *Privacy Act* or by relying on section 7 of the same act. In order to share information, paragraph 8(2)(e) requires a written request including the name of the investigative body and the person requesting the information, a description of the information being sought, and finally, the federal statute under which the investigative activity is being undertaken. A government body or agency would have to follow this procedure unless it determined, as per s. 7, that the information is "consistent" with the purposes for which it was originally collected. This will be discussed in more detail below.

4.2

These provisions exist because, as SIRC previously noted, s. 12 and screening information are collected under separate legislative authorities in the *CSIS Act*.

4.3 Potential for Abuse

In addition to the privacy issues raised above, SIRC is also concerned about the potential for CSIS to stray beyond the "strictly necessary" boundaries.

SIRC has concerns that extending security screening information access, even with *post facto* audits, will increase the potential for abuse. This is the main reason why the protection of personal information often involves front-end controls (i.e. written requests), as required by the *Privacy Act*. For larger systemic changes to how an organization shares and uses personal information, a Privacy Impact Assessment is required.

Although the Service is in the midst of preparing a Privacy Impact Assessment with regard to broader changes with their information management system, it is not clear if SIRC's specific concerns, discussed here, will be adequately addressed in a full and timely manner.

SIRC strongly recommends that CSIS consult with the Office of the Privacy Commissioner (OPC) before the end of the calendar year for an assessment of its decision to extend access of its security screening information

5 CONCLUSION

Overall, SIRC found SSB to be proactively attempting to adopt sound practices, incorporating a great deal of internal and external stakeholder input in order to create a better, more valuable product. These changes are so far positive, but are ongoing. The serious concerns raised in this review pertain to CSIS's operational use of information collected for security screening purposes.