TOP SECRET – CEO

SIRC REVIEW 2016-03

SIRC REVIEW OF SECURITY SCREENING

SUMMARY

- **CSIS's security screening program has evolved to become more efficient and effective at providing its clients with required information in a timely manner, in part due to recent technological advances.**

- **Overall, the operationalization of security screening provides additional tools and effective methods to gain information. However, CSIS must ensure that all investigative policies and procedures apply equally to the conduct of security screening investigations, including applications for warrants.**

- **SIRC found that CSIS had unnecessarily shared information about Canadians with a five-eye partner.**

- **Overall, SIRC found CSIS's use of conformed to policy however SIRC found that CSIS's procedure is silent on its use for security screening purposes.**

- **SIRC found that without a warrant for security screening investigations creates a situation through which CSIS can obtain information for s. 12 purposes without a warrant. Because of the concerns identified above, SIRC recommends that, when access to employer-held assets is deemed necessary for the purposes of a security screening assessment, all s. 15 investigations follow a procedure similar to the requirements applicable in the s. 12 and 16 investigative contexts, including seeking a warrant from the Federal Court in appropriate cases.**

- **SIRC recommends that the Department of Justice review all cases where information was obtained pursuant to the August 2013 DDO Directive, and if it is determined that *Charter* rights were infringed upon, the information be purged from all CSIS databases.**

- **SIRC recommends that CSIS update procedure to include its use in security screening investigations.**

Table of Contents

1 INTRODUCTION

CSIS has two major operational programs: the collection of threat-related intelligence and security screening for threats related to national security. As part of this latter function, CSIS 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.[1]

This review first sought to examine CSIS's response to SIRC's 2013 security screening review wherein it was recommended that CSIS consult the Office of the Privacy Commissioner (OPC) about a change it had enacted to allow for broader internal access to security screening information. Although consultation with the OPC is still ongoing, . Moving forward, SIRC expects CSIS to abide by any recommendations or decisions made by the OPC.

Next, SIRC focused on the impact of some technological changes that have allowed SSB to become more efficient and effective, as well as to enhance the quality of its products and analysis. SIRC found that technological advances have resulted in CSIS being better equipped to manage not only its regular screening responsibilities, but also any emerging issues or special events that may arise. In one instance, however, SIRC found that CSIS had unnecessarily shared information on Canadians with a five-eyes partner.

SIRC then looked at the "operationalization" of the Security Screening Branch (SSB) by reviewing some of the cases where tools that were usually associated with s. 12 investigations were used for security screening purposes. SIRC found CSIS's use of to conform to internal policies and procedures. SIRC found however, that the procedures for are silent for its use for security screening investigations and therefore recommended that this be updated to conform to the overarching policy.

Finally, SIRC looked at CSIS's practice of collecting information that has been in the possession of an employer. SIRC believes that obtaining employer-held information for security screening assessments creates a way for CSIS to obtain information for other investigations where a warrant may be required because constitutionally protected rights are engaged. In addition, SIRC is concerned that a violation of s. 8 of *Canadian Charter on Rights and Freedoms* (the *Charter*) may have occurred in some cases that it reviewed. SIRC recommends that CSIS follow the same procedures for obtaining and searching employer- held information that it would for obtaining similar information in its other investigations.

[1] http//www.scis.gc.ca; accessed July 15, 2016.

Overall, the operationalization of security screening provides additional tools and effective methods to gain information. However, CSIS must ensure that all relevant investigative policies and procedures apply equally to the conduct of security screening investigations, including applications for warrants.

2 METHODOLOGY

This review examined CSIS's activities related to the Security Screening Branch (SSB), which falls under the Deputy Director Operations, and is one of the largest branches of the Service. SIRC looked at corporate, operational and policy documents, as well as a sample of both immigration and citizenship security screening files that CSIS identified for field investigations. In addition, SIRC held several briefings with SSB both at Headquarters and in Toronto region.

The core review period for this study was January 1, 2014 to April 30, 2016, but SIRC examined documentation that fell outside this period in order to provide a complete assessment of relevant issues.

3 BACKGROUND

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. To this end, the Security Screening Branch (SSB) provides security assessments to other Government departments and security advice to Immigration, Refugees and Citizenship Canada (IRCC) and the Canadian Border Services Agency (CBSA) under the authorities of ss.13 and 14 of the *CSIS Act* respectively.

Guided by the Government of Canada Policy on Government Security, CSIS investigates and provides security assessments on persons whose employment with the Government of Canada requires them to have access to classified information or sensitive sites, such as airports, major ports, and the Parliamentary Precinct and nuclear power facilities.[2] These assessments relate to a person's loyalty and reliability as it relates to loyalty as defined by the Treasury Board's *Standard on Security Screening*, which took effect in October 2014. CSIS only provides assessments; the decision for granting, denying, suspending or revoking a clearance ultimately belongs to the Deputy Head of the requesting department or agency.

On the Immigration Screening side, CSIS provides advice to IRCC 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 may on reasonable grounds be suspected of posing a threat to the security of Canada or who could be inadmissible under the *Immigration and Refugee Protection Act* (*IRPA*).

3.1 Privacy Impact Assessment

In 2013, SIRC examined the key responsibilities of SSB and some recent changes that had 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 was used . In particular, SIRC explored the implications and risk associated with CSIS's then-recent decision to

[2]http//www.csis.gc.ca; accessed September 7, 2016. Additionally, CSIS may assist RCMP with accreditation for Canadians and foreign nationals participating in events in Canada; provide assessments to the CBSA and, provide assessments to foreign government agencies and international organizations with regard to Canadians seeking to work abroad. CSIS may also enter into arrangements with provincial governments and police forces to provide security assessments.

SIRC was concerned that there was a risk that CSIS could be in violation of the *Privacy Act* by relying on the consistent use clause to allow [3] SIRC recommended that CSIS consult with the Office of the Privacy Commissioner (OPC) before the end of the calendar year for an assessment of this decision. In response, in December 2013, CSIS informed the OPC that it was working on a Privacy Impact Assessment (PIA) that would address SIRC's concerns within the context of a larger information management project related to the implementation of

In the spring of 2015, CSIS engaged with the OPC on this matter by giving it an overview of , discussing its decision to allow and sharing a draft PIA. According to CSIS, "the PIA was well-received overall"; however, after an informal discussion with OPC the front line staff, CSIS decided to bolster its rationale related to in order for the OPC to consider this practice consistent use. , in consultation with SSB and CSIS's Access to Information and Privacy section, strengthened the rationale to argue that did not contravene the *Privacy Act.*

SIRC examined the updated draft of the PIA and identified one section that was misleading. CSIS stated that if an individual did not consent to then the ability for CSIS to conduct that person's security assessment would be impacted. In response to an inquiry from SIRC, CSIS responded that this was an error and that the PIA has since been amended to indicate that there would be no effect on the primary activity (screening) if it were unable to [4]

Although consultation with the OPC is still ongoing,

---

[3] CSIS argued that was justified as its use was originally collected. It is important to note that CSIS was always able to Additionally, there is a mechanism

[4] SIRC Briefing June 22, 2016

Going forward, SIRC expects CSIS to abide by any recommendations or decisions made by the OPC.[5]

[5] The PIA is in the final stage of approval at CSIS.

4 THE IMPACT OF TECHNOLOGY

Numerous SIRC reviews have noted the impact of technology on CSIS's investigative capability. Since SIRC's last screening review, SSB has benefited from significant advances in technology: not only has technology changed how SSB performs its duties on a daily basis, but also how SSB is able to collaborate with its international partners. To illustrate this evolution, SIRC looked at the role of and within SSB, as well as two case studies.

CSIS developed following a study that found that the dated tools and technology it was using were constraining its ability to carry out its mandate.

CSIS believed that this procedure had the potential to adversely affect the accuracy and comprehensiveness of CSIS assessments and, by extension, the integrity of investigations and advice provided.[6]

CSIS assesses that the impact on SSB has been twofold. The first impact is related to how an investigator retrieves and uses the data.

The second impact, and specific to SSB, is that is a platform for the

In January 2015, was released, launching the new and security screening results viewer. Both of these enhancements were implemented with the goal of providing a faster turnaround time

This faster turnaround response allowed CSIS to consistently meet the national standard to its screening clients.[8]

CSIS estimated that was able to resulting in fewer cases being sent [9] Since the introduction of ACE, screening analysts spend more time on analysis, and less on typing information into various databases. This has allowed SSB to reprofile some positions to focus on

[6] Speaking notes: Presentation to the Office of the Privacy Commissioner – April 27, 2015,

[8] Security Screening Branch – Performance Accountability Framework – Third and Fourth quarters of 2014-2015, p. 3-4.

[9] Ibid, p. 4 and Presentation given to SIRC in PowerPoint – *Security Screening Renewal* – 2016 05 19 and SSB – Performance Accountability Framework – First and second quarters of 2015-2016, p. 6. Prior to this less than were

analytic competencies.[10] The outcome of this transformation has meant fewer cases being referred to the regions, which are then able to concentrate on priority cases.

During the review period, in addition to CSIS's regular screening requests, SSB processed site access requests for the Pan-Am Games and played a large part in the screening of Syrian refugees. SSB HQ told SIRC that without meeting the screening timeline requirements for the Syrian refugees would have been difficult, if not impossible.[11]

4.1 Operation Syrian Refugee (OSR)

In November 2015, the Government of Canada announced it would resettle 10,000 Syrian refuges by the end of the year, with an additional 15,000 to be resettled by end of February 2016. A coordinated whole of government approach was taken to support the relocation of the refugees from their current locations to Canada. CSIS was represented within the Government Operations Centre, working closely with partner agencies on OSR. CSIS's role was to provide security advice, in accordance with s.14 of the *CSIS Act,* to IRCC and the CBSA. CSIS also provided s.12 threat assessments and intelligence reporting to support GoC efforts.[12]

SSB NHQ committed to conduct security screening for all refugees cases referred to CSIS by IRCC. The refugees who were considered for OSR had been pre-selected by the United Nations High Commission for Refugees. All Syrian cases were treated as soon as received by CSIS and processed . Information received from IRCC was

. This strategy allowed CSIS to process the files quickly and complete the screening process at HQ without assistance from the regions.[13]

4.2 Technology and Information Sharing

Technological advances have facilitated SSB information sharing with CSIS's foreign partners.

[10] SIRC Briefing with SSB HQ May 10, 2016.
[11] Ibid.
[12] Executive Directive – Operation Syrian Refugee, dated 2015 12 04. File number 17300-3
[13] Deck provided to SIRC: Immigration Screening and Operation Syrian Refugee; CSIS Briefing to SIRC May 10, 2016

SIRC has no concerns with CSIS exchanging information about applicants and understands the value of these exchanges . This process involves checks allowable under the authority of a screening investigation. Although adds confidence to SSB's findings. SIRC does, however, question the necessity of sharing the [17]

SIRC found that CSIS had unnecessarily shared information about Canadians with a five-eye partner.

SIRC has no recommendation on this matter because, as a result of SIRC's inquiry, CSIS has begun to expunge information from the data it sends as part of the initiative.

---

[17] Email from dated July 27, 2016. In a written answer to SIRC regarding the discrepancy between what had been communicated in the briefing and the documentation, CSIS told SIRC that this information was sent because

5 THE OPERATIONALIZATION OF SECURITY SCREENING

CSIS's policy on the conduct of operations governs all of its investigations, including security screening, therefore reflecting requirement that all investigations be authorized, necessary and proportionate. Additionally, all investigations must be conducted in accordance with the law. Moreover, this policy also reflects the need to use the least intrusive techniques first, except in emergency situations or where less intrusive investigative techniques would not be proportionate to the gravity and imminence of the threat, or if it appears they are unlikely to succeed.[18] This policy overarches the procedures that govern the individual tools and techniques used in different investigations.

For the purposes of this review, SIRC requested information

SIRC reviewed these cases in order to understand the contribution that these additional tools/methods made to screening investigation; whether the operationalization of SSB was adequately reflected in operational policies; and finally, if SSB actions were in compliance with internal policies and the law.

5.1

CSIS provided SIRC with a list of over 30 files

[18] CSIS Policy: Conduct of Operations: Effective 2014-01-10 File No.:

Overall, SIRC found CSIS's use of conformed to policy.[24] However, in addition to policy, which articulates general principles and core concepts, procedures provide detailed instructions on how to implement policy and articulate what can be done

SIRC found that CSIS's procedure is silent on its use for security screening purposes. In order to prevent non-compliance with procedure, **SIRC recommends that CSIS update its procedure to include its use in security screening investigations.**

5.2 Employer-held Information

In addition to using , SSB receives assistance from in carrying out investigations.

During the review period, CSIS informed SIRC that instances when CSIS approached employers with requests to, without a warrant, for the purposes of providing a security assessment. In cases, the employers complied with CSIS's requests to obtain information without a

---

[24] One case of was more intrusive; however SIRC believes it to be not disproportionate to the threat. File

warrant. In the case, refused to comply with the Service's request.

In August 2013, a memo regarding and CSIS's ability to examine and report on information obtained from third parties normally obtained by a warrant, was sent from the to HQ and the regions. The memo concluded that for the purpose of s.15 investigations in support of s.13 of the *CSIS Act*, CSIS had the authority to : employer assets without a warrant, and that there was no need to notify the Assistant Director nor consult with Department of Justice, National Security Litigation and Advisory Group (NSLAG) in the case of a s. 15 investigation when doing so.[31]

[31] SIRC does note that there are cases where CSIS sought legal advice with regards to

A subsequent DDO Directive, issued in October 2013, addressed in relation to s. 12 and s. 16 investigations. The Directive provided that the waiver of privacy in the ss. 12 and 16 contexts cannot come from the third party provider of the information but only from the individual who holds the privacy interests, and in all cases, NSLAG must be consulted and provided with necessary information to make a determination concerning privacy interests.[32]

SIRC has two concerns with the August 2013 DDO Directive. First, the rigor that is applied to ss. 12 and 16 investigations is not present. Unlike the October 2013 DDO Directive, there is no consideration of rights engaged or the application of *the Charter.* Second, CSIS's ability to share information from security screening with s. 12 investigations is problematic in the context of obtaining information without a warrant when *Charter* rights are engaged.

SIRC found that without a warrant for security screening investigations creates a situation through which CSIS can obtain information for s. 12 purposes without a warrant.[33] Because of the concerns identified above, SIRC recommends that, when access to employer-held assets is deemed necessary for the purposes of a security screening assessment, all s. 15 investigations follow a procedure similar to the requirements applicable in the s. 12 and 16 investigative contexts, including seeking a warrant from the Federal Court in appropriate cases.

Additionally, **SIRC recommends that the Department of Justice review all cases where information was obtained pursuant to the August 2013 DDO Directive, and if it is determined that *Charter* rights were infringed upon, the information be purged from all CSIS databases.**

SIRC understands the benefit of operationalization when it comes to security screening investigations and recognizes that there are instances where employer-held information may be key to being able making an accurate assessment. However, SIRC expects all security screening investigations to be conducted according to the principles articulated in CSIS's policy on the Conduct of Operations, including necessity and proportionality to the threat. This includes only infringing on the privacy of individuals when there are valid reasons to do so and only to the extent that is necessary.[34]

---

[32] Consultation does not apply in situations where

[33] CSIS is able to use threat-related information obtained from s. 15 investigation for s. 12 purposes.

[34] SSB Briefing to SIRC August 4, 2016;

6 CONCLUSION

Overall, the security screening program has evolved to become more efficient and effective at providing its clients with required information in a timely manner. This is due both to technological advances and the Branch's reprofiling of the jobs in order to do more front-end analysis. SSB's response to the Government of Canada's initiative to resettle the Syrian refugees in 2015-2016 represents a key success for the Branch.

SIRC sees the benefit of SSB's operationalization. However, the nature of security screening investigations can entail the collection of a great deal of personal information related to the subject and others. SIRC will continue to monitor that CSIS ensures that, through training, policy and practice, screening investigations observe the same principles of respect for the law, proportionality and necessity that are applicable to all its other investigations.