~~TOP SECRET // CEO~~

NSIRA Review 2018-15
File No. 08-4-16

August 14, 2019

The Honourable Ralph Goodale, P.C., M.P.
Minister of Public Safety and Emergency Preparedness
269 Laurier Avenue West
Ottawa, ON, K1A 0P8

Subject: Review of CSIS's Internal Security Branch

Dear Minister:

The purpose of this letter is to provide you with the results of the Review of the Canadian Security Intelligence Service's (CSIS) Internal Security (IS) Branch, which conducts personnel security screening, inquiries, and investigations into employees or incidents. This review was conducted under the authority described in subsections 8(1)(a) and 8(3) of the *NSIRA Act* to review any activity carried out by CSIS and to make any finding and recommendation that NSIRA considers appropriate.

The focus of this review was to follow up on a previous review of IS's activities conducted in 2013, particularly related to the adequacy, adherence to, and effectiveness of IS processes and policies. The review was facilitated by meetings with IS management, as well as analysis of case files, briefing materials, and CSIS responses to questions.

NSIRA has concluded that while significant improvements have been made with respect to internal security at CSIS since the 2013 review, further improvements to internal security policies could strengthen the consistency of decision-making on personnel security files and investigations, and improve the procedural fairness of these processes writ large.

Based on the information reviewed and interviews conducted, NSIRA finds that:

1. Internal inquiries/investigations at CSIS are professionally managed and seek to minimize bias and subjectivity to the extent possible;

2. CSIS conducted the activities reviewed in accordance with its legal obligations set out in the *CSIS Act*. However, CSIS has not developed sufficiently detailed

governance on when and how to report suspected criminal activity uncovered during an internal inquiry/investigation or security assessment;

3. CSIS's has a number of interrelated governance issues, including:

   - Informal policies and procedures;
   - No privacy impact assessment on polygraph process; and
   - No employee feedback mechanism specific to the polygraph;

4. The polygraph is central to CSIS' inquiry and five-year update processes;

5. Internal Security complies with the Treasury Board Secretariat Standard on Security Screening (SSS) and its own policies in its management of complex cases arising from the security assessment process, but the associated decision-making could be strengthened with improved governance and policy clarity; and,

6. Several pertinent legal opinions and legal documents were received only once the review was substantially written and complete, preventing their timely incorporation and consideration in the final report.

With respect to addressing the findings made in this review, NSIRA recommends that:

1. CSIS develop an internal policy, in consultation with TBS, outlining parameters on reporting information obtained during the course of Internal Security screening, inquiries, and investigations to law enforcement in a timely manner;

2. CSIS strengthen internal governance over activities, including modifying the methodology for conducting polygraph assessments, as appropriate;

3. CSIS update applicable policy and procedures on the use of the polygraph to address security and procedural fairness implications stemming from failed polygraph results; and,

4. CSIS further align its overarching policy suite with the assessment criteria for adverse information outlined in the SSS, Appendix D, as well as update the

Questionnaire Guidebook with clear definitions to align to risk indicators within the

Before this review was finalized, CSIS officials had an opportunity to review it for factual accuracy.

If you have any questions or comments, I would be pleased to discuss them with you at your convenience.

Yours sincerely,

Pierre Blais

Pierre Blais, P.C.
Chair

cc: David Vigneault, Director, CSIS

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: *1-833* 890-0293 Fax: *613* 907-4445

National Security and Intelligence Review Agency

Office de surveillance des activités en matière de sécurité nationale et de renseignement

~~TOP SECRET // CEO~~

REVIEW OF CSIS'S INTERNAL SECURITY BRANCH (NSIRA STUDY 2018-15)

Contents

I AUTHORITIES

This review began under the authority of the Security Intelligence Review Committee (SIRC) as articulated in subsection 38(1) of the *Canadian Security Intelligence Service's (CSIS Act)*, which declares that SIRC is mandated to review CSIS's operations in the performance of its duties and functions.

During the course of the review, Bill C-59 – *An Act Respecting National Security Matters* – received Royal Assent on June 21, 2019. Part 1 of Bill C-59 enacts the *National Security and Intelligence Review Agency Act* (NSIRA Act), and came into force by order of the Governor in Council on July 12, 2019. The *NSIRA Act* repeals the provisions of the *CSIS Act* that establish and govern SIRC and establishes in its place the National Security and Intelligence Review Agency (NSIRA). The *NSIRA Act* sets out the composition, mandate and powers of NSIRA and amends the *CSIS Act*, and other Acts, in order to transfer certain powers, duties and functions to NSIRA.

This review continued under the authority described in subsections 8(1)(a) and 8(3) of the *NSIRA Act* to review any activity carried out by CSIS and to make any finding and recommendation that NSIRA considers appropriate.

II INTRODUCTION

The focus of this review was to examine Internal Security (IS) Branch inquiries and investigations, as well as the adequacy, adherence to and effectiveness of policies, processes, tools, and decision-making.

SIRC last conducted a review of CSIS's IS activities in 2013. The review examined CSIS activities related to: allied-driven security standards; IS Branch's role in screening potential employees, physical security, searches and access-lists; and, internal investigations. The review made a number of significant findings and recommendations pertaining to the management of internal investigations and the overall internal security posture. In particular, SIRC recommended in 2013 that CSIS:

1. Develop robust procedures governing access lists;
2. Re-examine an internal investigation in its entirety and address specific concerns pertaining to the subject;
3. Create a training and mentoring program suited to the unique work of IS employees;
4. Create a detailed policy on the conduct of IS investigations;
5. Take immediate action to ensure all decision-making pertaining to investigations is documented in the appropriate case files; and
6. Upon completing a formal investigation, IS should forward the report to another group in the Service for review.

This study presents an opportunity for NSIRA to follow up on CSIS's implementation of the recommendations made in 2013.

Additionally, given recent changes in how CSIS conducts inquiries and investigations, as well as

updated policies and procedures, this was an appropriate time to re-assess CSIS's IS activities.

III OBJECTIVES

The four objectives of this review were to assess:

1. The progress made by CSIS in implementing SIRC's 2013 recommendations;
2. The adequacy of IS processes used to examine actual or potential security incidents, violations and breaches;
3. The adherence to IS processes used to examine actual or potential security incidents, violations and breaches; and,
4. The effectiveness of IS processes used to examine actual or potential security incidents, violations and breaches.

IV SCOPE AND METHODOLOGY

CSIS's IS Branch is the Policy Centre for all policy and procedural documents related to security inquiries and investigations. Its activities involve examining actual or potential security incidents, violations and breaches. The review focuses on IS inquiries and investigations, as well as the adequacy, adherence to and effectiveness of policies, processes, tools, and decision-making. In order to complete this review, NSIRA examined all applicable written and electronic records, files, correspondence and other documentation related to the inquiries/investigative case files chosen for review, as well as documentation of IS Branch's various activities, including policies, procedures, and legal advice to verify conformity with legal, ministerial and policy requirements.

In order to gain context, NSIRA held briefings with IS managers and other personnel involved in the activities under review (Refer to Annex A). In particular, NSIRA assessed IS's recent efforts at applying actuarial science to inquiries, investigations, and other applicable initiatives aimed at reducing bias and subjectivity.

To test for adherence to, and the effectiveness of, policies and procedures, NSIRA selected a random and selected sample of IS inquires/investigations (Refer to Annex B). Additionally, NSIRA examined training manuals and managerial direction to understand how policy and procedures are interpreted by management and subsequently conveyed to employees.

Additionally, the review provides a general update on the status of the Safeguarding Initiative (covered within SIRC's 2013 review), as well as briefly outlines any associated security challenges in order to provide a more contemporary update on CSIS's IS posture.

V CRITERIA

Legal and Ministerial Requirements

NSIRA expects CSIS to conduct its activities in accordance with the *CSIS Act*, the *Canadian*

Charter of Rights and Freedoms, the *Privacy Act*, the *Criminal Code of Canada*, and any other relevant legislation. Additionally, NSIRA expects CSIS to conduct its activities in accordance with Ministerial Direction.

NSIRA expects CSIS to follow pertinent Justice Canada legal advice/opinions, and to explain the rationale/justification for any departures from the recommended course of action.

Policies and Procedures

NSIRA expects CSIS to:

1. Follow guidelines and direction provided by Treasury Board Secretariat (TBS) in its policy suite pertaining to departmental security practices, such as the Directive on Departmental Security Management and the Standard on Security Screening,;
2. Establish appropriate internal policies and procedures to guide its activities and to provide sufficient direction on legal and ministerial requirements. To determine the adequacy of policies and procedures, NSIRA used the draft policy provided by CSIS, namely, CSIS Policy and Procedures: Internal Security Inquiries and Investigations, February 18, 2019;
3. Ensure its employees are knowledgeable about, and comply with, policies and procedures; and,
4. Maintain the integrity of activities by applying an effective framework, including appropriately accounting for important decisions and efforts to eliminate bias and subjectivity.

VI BACKGROUND

This review sought to assess the management of internal security risks at CSIS through the lens of inquiries and investigations. The IS branch is the policy centre for security guidance and direction to the organization and the branch responsible for investigating complex employee and applicant security cases.

Safeguarding Initiative

The management of enterprise and IT security risks was assessed as part of SIRC's 2013 review. At that time, the Service reported compliance with the milestones of the 'Safeguarding Initiative' in December 2013, as reported to SIRC in 2014.

Since then, CSIS has enhanced its security posture in ways that align with the various objectives of the Safeguarding Initiative. Specifically:

The Service continues to look for ways to improve our audit-related processes and technologies in order to be more efficient and mitigate threats To enhance access controls, the Service is working on implementing processes and tools

The program has identified additional recommendations to improve security and reduce overall risk to the organization.

Through yearly Integrated Business Planning, the Service reviews and approves various proposed projects to enhance our security posture

Relevant IS units and security processes

The unit is responsible for the full spectrum of security assessment activities pertaining to external candidates and contractors. The on the other hand, handles case files of existing employees as part of the five-year update process and any associated inquiries. Additionally, there is an investigations unit for the conduct of internal security assessments.

During the course of the review, because of information provided to NSIRA, several processes surfaced as critical components of the work of IS.

The five-year update process, by which employees' Enhanced Top Secret (ETS) security clearance is updated, emerged as a key process that identifies security issues associated with specific CSIS employees. The ETS update process includes subject interviews, verifications and review of employees' security forms and internal security files, open-source checks, and other verifications – in addition to the polygraph examination, which became a central pillar of the review due to CSIS's reliance on this assessment tool as part of the five-year update process.

Often, information obtained through the five-year ETS update process warrants a follow up by way of an inquiry by Internal Security. An inquiry is a fact-finding process to determine whether a security incident, violation or breach has occurred and to determine if additional follow-up is required. Depending on the findings of an inquiry, the Director may approve that an investigation take place.

These terms have been recently codified in a revised IS policy suite.[2] Pursuant to this policy suite, if an IS Inquiry or Investigation reveals that a security incident, violation or breach may result in a breach of conduct,[3] or may also constitute operational non-compliance, IS must refer the issue to the relevant DG or RDG or to Health Workplace Management in accordance with CSIS internal policy.

Once security issues have been identified with an employee, and when there is no quick resolution of these issues, the employee will be placed on the IS's Complex Case list. The purpose of this list is to devote IS resources towards risk-mitigation,

[2] Refer to CSIS Policies and Procedures on Inquiries and Investigations; and on Individual Security Screening.
[3] e.g. CSIS's Code of Conduct and/or other employee conduct provisions within other policy documents.

When dealing with Complex Cases, CSIS has additionally developed

Over the course of the review, it became apparent that the work conducted by IS Branch is unique when compared to any other activity within CSIS; every decision made on inquiries/investigations can have a profound impact not only on the individuals being assessed, but also for the organisation as a whole. To perform internal security properly, this requires specialized training, mentorship, clear policies and procedures and the right tools and resources used consistently, cohesively, and objectively.

VII FINDINGS AND RECOMMENDATIONS

a) Internal security processes and practices at CSIS

Finding no. 1: Improvements to IS processes and practices since 2013 review

Based on the information reviewed and interviews conducted, NSIRA finds that internal inquiries/investigations at CSIS are professionally managed and seek to minimize bias and subjectivity to the extent possible.

SIRC's previous review of IS in 2013 was controversial, not because of the nature of the review, but due to the totality of the implications derived from the findings:
The evidence assessed from the current review has led NSIRA to arrive at an updated conclusion. In particular, CSIS's training and mentoring programs have been augmented; policy has generally been improved; decision-making pertaining to inquiries was documented in the appropriate files; and finally, CSIS has taken constructive steps towards reducing bias and subjectivity through the creation of innovative tools and by consulting with pertinent stakeholders outside of IS to help develop practical risk-mitigation strategies.

Within SIRC's 2013 study, a recommendation stated that upon completing a formal

---

[3] ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security, 17 June 2019.

investigation, "IS should forward the report to another group in the Service for review." The purpose of this recommendation was to help reduce bias and subjectivity within IS, given the serious issues identified within a case file. CSIS did not agree with this recommendation, arguing that:

> Third party review of formal investigations jeopardizes the confidentiality and sensitivity of certain investigations, injects a layer of bureaucratic oversight which will affect timelines and objectivity of the investigation, and impede the Director's authority in the personnel management of employees.[6]

Moving to NSIRA's current examination of this issue, IS has met with a number of related stakeholders to discuss a complex case:

NSIRA believes that the creation of the Meetings is a positive step in meeting the intent of the initial recommendation. CSIS effectively reduces the probability that favoritism, bias, or subjectivity play a role in outcomes by applying a wider purview of stakeholders into the decision matrix. Although it is in its early stages of development, this framework for consultation could be used to further guide other complex cases moving forward; and in many respects exceeds the recommendation SIRC had proposed to CSIS back in 2013.

That said, this review also identified areas for which practice, policy, and procedures can be improved. Although the review makes a number of findings and recommendations, NSIRA recognizes that decision-making in applicant and employee security files is often complex. In particular, internal security issues sometimes bleeds into the realm of human resources, which further complicates these issues. It is hoped that the observations made within this analysis will further assist CSIS's notable efforts at managing the development and implementation of the national security program to protect CSIS, its assets, operations and employees from all security threats.

b) Legal Requirements Pertaining to Informing Law Enforcement

Finding no. 2: Compliance with the Law

Based on the information reviewed and interviews conducted, NSIRA finds that CSIS conducted the activities reviewed in accordance with its legal obligations set out in the *CSIS Act*. NSIRA notes, however, that CSIS has not developed sufficiently detailed governance on when and how to report suspected criminal activity uncovered during an internal inquiry/investigation or security assessment.

NSIRA expected to see that CSIS has sought legal advice and developed informed policies/procedures related to pertinent legal issues encountered by IS Branch; and furthermore,

[6] Letter from DG ER&L to SIRC Executive Director dated 27 February 2015.

that CSIS has met its legal obligations as they arise when conducting inquires/investigations.

NSIRA observed that requirements pertaining to the timelines and logistics of reporting information to the authorities are spread across multiple internal governance documents, CSIS has obtained several legal opinions on this issue.

On the specific issue of whether CSIS has an obligation to report a crime, IS indicated that they rely on a 2011 legal opinion which notes that

The Treasury Board Standard on Security Screening (SSS), applicable to CSIS pursuant to s. 2 of the *Financial Administration Act*, states that when information is uncovered that provides reasonable grounds to suspect that the individual may pose a serious threat to others, or may be involved in fraud or other criminal conduct, the information may be disclosed to law enforcement authorities.[10]

NSIRA notes that internal CSIS policy diverges from the standard outlined in the SSS on the issue of when it may be appropriate to report information to the authorities. An example of the divergence between the SSS and internal policy is found in the Procedure on Individual Security Screening, which states that information may be disclosed to entities with lawful authority if the information amounts to "admissions of activities of a serious criminal nature or those which are deemed to pose a serious risk to the safety of others."[12] The internal CSIS policy does not adopt the language of the SSS with regard to either the threshold (reasonable grounds to suspect) or the activities in question (may be involved in fraud or other criminal conduct).

[10] Treasury Board Secretariat, Standard on Security Screening, effective October 20, 2014, para 6.2.9

[12] Treasury Board Secretariat, Standard on Security Screening, effective October 20, 2014, para 6.2.9

Further, none of the above-noted policy instruments or legal advice provide any direction with regard to the timeliness of reporting. The concept of "imminent risk," which was canvassed by the Supreme Court of Canada in the context of a physician's right to disclose confidential patient information, necessarily implies prompt action.[14] For example, in the context of child abuse, generally speaking, provincial legislative instruments require anyone who believes a child is in need of attention must report this promptly to a designated person or agency. The *Alberta Child, Youth and Family Enhancement Act*, for example, requires that when an individual believes that a child is in need of intervention s/he must "forthwith" make a report to the director.[15] Use of the word 'forthwith' is generally seen as the strongest expression of the time commitment for the performance of an undertaking or an obligation. It means 'immediately' or 'without delay,' often indicating that action is to be taken within 24 hours.

NSIRA selected for review one case where CSIS came across legally incriminating information about the conduct of an employee CSIS took two months to report this information to law enforcement.[16] When asked about this delay, CSIS explained that a number of factors contributed to the delay, including seeking legal advice, ensuring that all relevant facts had been assembled, and arriving at consensus on a novel disclosure.[17] Following this case, IS decided to aim to contact local enforcement within 48 hours when there are concerns about

NSIRA recognizes that while prompt reporting is required in certain circumstances, there may also be a risk in reporting to law enforcement in haste. There are several important issues to consider when deciding whether or not (and how) to report information to the authorities. Once law enforcement is involved, the relationship between the employee and the Service is irrevocably impacted. Furthermore, the issues may include: privacy protections; labour relations obligations; the authority under which the disclosure is taking place; the method of disclosure; the appropriate authority to receive the disclosure; whether or not to notify the individual about the disclosure; as well as any potential harm to the employee, to the Service, to other employees, to the government, and to the public interest.[19]

In NSIRA's view, it would be prudent for CSIS to cohesively consider these difficult issues and to develop an internal policy, in consultation with relevant policy centres, outlining the parameters on reporting information obtained during the course of IS screening, inquiries, and

[14] *Smith v. Jones* [1999] 1 SCR 455

[16] In response to the draft report, IS provided the following comment on July 30, 2019:

[19] An example of where it may be unclear on whether to report to authorities is where

While IS indicated that it is not up to them to investigate a crime, it is, however, incumbent on them to properly assess all of the available information before reporting an issue to the authorities. This includes, at times, conducting an internal inquiry and seeking internal advice as required.

investigations to the authorities. For such disclosures to function effectively under tight deadlines, this may require having a panel of senior managers and legal advisors, identified in advance, to form a committee, in exceptional circumstances, in order to render a swift, yet prudent, course of action with regard to reporting information to the authorities. To this end:

NSIRA recommends that CSIS develop an internal policy, in consultation with TBS, outlining parameters on reporting information obtained during the course of IS screening, inquiries, and investigations to law enforcement in a timely manner.

c) Policies and Procedures

Finding no. 3: Adequacy and Adherence of Policies and Procedures Pertaining to the Polygraph

Based on the information reviewed and interviews conducted, NSIRA finds that CSIS's has a number of interrelated governance issues, including:

- **Informal policies and procedures;**
- **No privacy impact assessment on polygraph process; and**
- **No employee feedback mechanism specific to the polygraph.**

NSIRA expected to see that CSIS's has detailed written policies and procedures governing polygraph examinations. NSIRA also expected to see that CSIS managers have a robust understanding of, and control over, the polygraph program, that the process is as transparent as reasonably possible for employees, and that there is a redress mechanism.

Policy guidance regarding use of the polygraph

Polygraph examinations have been part of CSIS's screening program since its inception in 1984. Until 2014, CSIS only screened for loyalty to Canada. The SSS, which came into effect on October 20, 2014, identifies the polygraph examination as a tool used in ETS clearance applications to assess an individual's criminality and/or loyalty to Canada as well as reliability as it relates to loyalty.

According to to be compliant with this policy, CSIS is required to conduct polygraph examinations for ETS clearances.[20] Over the course of the review, it became evident that activities are so integral to internal inquiries and investigations that separating one from the other would pose review accuracy risks; indeed, and the conduct of internal inquiries are symbiotic insofar as they collectively contribute to the security assessment of applicants/employees.

[20] NSIRA meeting with May 14, 2019.

The SSS provides a definition of 'reliability as it relates to loyalty:'

> Because of personal beliefs, features of character, association with persons or groups considered a security threat, or family or other close ties to persons living in countries that pose a security risk to Canada, the individual has acted, is acting, may act or may be induced to act in a way that constitutes a threat to the security of Canada; or the individual has disclosed, may disclose may be induced to disclose, or may cause to be disclosed in an unauthorized way, sensitive information.[21]

However, part of the ethical responsibility of a polygraph examiner is to ensure that an examinee is treated fairly and understands the questions they are being asked with respect to reliability as it relates to loyalty

Although the SSS does provide some guidance with regard to the assessment,[23] it offers no qualitative measures. Furthermore, the SSS does not mention admissions of involvement in criminal activity unknown to law enforcement in the context of adverse information.[24]

Nevertheless, the SSS provides the foundation for CSIS's polygraph policies and procedures. There is a new IS policy released relating to internal inquiries/investigations in May 2019. However, NSIRA notes that CSIS last updated its 'Policy on the Use of the Polygraph in Internal Security Administrative Investigations' five years ago, meaning it uses terminology and has clauses which are not aligned with the newly updated policy suite.[25] There is no specific policy on the use of the polygraph for five-year updates; rather, there are aspects of polygraph policy and procedures spread across multiple internal governance documents.[26]

The review observed that the current policy suite is insufficiently detailed to answer questions related to standardization of polygraph assessments, examiner training, quality-control measures and definitional thresholds, etc. Although has created pamphlets for, and provided presentations to employees on, "demystifying the polygraph," this information is cursory.[27] NSIRA's review concluded that this is no accident: employees are discouraged from researching the polygraph given the possibility that countermeasures could be used to circumvent the instrument.

---

[21] SSS, Appendix D, Section 7

[23] I.e. type of criminal activity, the duties to be performed, the nature and frequency of the offence, and the passage of time.

[24] ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security," June 17, 2019.

[25] Refer to CSIS Procedures: Use of the Polygraph Examination In an Internal Security Administrative Investigation," File No. June 23, 2014.

[26] As observed by CSIS in response to NSIRA's draft report, policy on the polygraph can be found on Internal Security Inquiries and Investigations, the Policy and Procedures on Individual Security Screening, as well as within

[27] notes that any information beyond cursory could compromise the use of the technique, and given the sophisticated counter intelligence efforts against Canada, CSIS considers the protection of this tool to be paramount. Refer to IS response to draft review, July 30, 2019.

With respect to internal controls. however, senior IS managers do not have either detailed knowledge of, methodology.[33] Of note, when SIRC conducted a review of IS in 2013, who was the fulcrum of alleged concern.[34] Although there is no evidence to doubt the professionalism of within the context of this review, there is inherent risk in placing confidence in a select number of people for whom there is limited external or internal oversight – apart from quality control administered by other

[33] NSIRA was told by IS management that they refrain from knowing detailed information about nethodology, given that this could complicate their own screening assessment once they transition out of IS or during their own clearance update processes. Refer to NSIRA meeting with June 17, 2019.
[34] Refer to SIRC Study 2013-06.

polygraph examiners within or the Chief which cannot be considered independent.[35]

Standardization and administration of the polygraph

To the extent possible, NSIRA attempted to assess the degree to which the polygraph has been administered in a standardized and reasonable manner. Arriving at a conclusion was difficult, given that few governance documents outside of the methodology – which is geared towards technical, rather than managerial standards – were available for review. To illustrate. stated that

When NSIRA asked for the policy or document where this is specified, responded that "no formal documentation exists as a policy. This was an internal reorientation of practice within "[36] Later, elaborated on this by noting that:

> This 'best practice' reorientation came upon the realization by
>
> hereby undermining the integrity of the Service's polygraph program. Every security application is unique; more recently (circa 2017), we have attempted to implement a standard procedur

Despite this change in practice, NSIRA reviewed 10 cases where it appeared that employees

[38] Given the inconsistent use of polygraph terminology, NSIRA was unable to render a definitive determination if was meeting its own standard.

Other variations were also observed over the course of the review.[41] In one case,

[35] NSIRA asked about how polygraph employees are tested for loyalty and reliability as it relates to loyalty. CSIS responded that "An independent examiner (quality control officer) or Chief conducts polygraph examinations of polygraph personnel. It is the same standardized test." NSIRA notes, however, that cautioned researchers of the importance of keeping the methodology secret, given that if the methodology is known to the subject taking the test, its reliability would be jeopardized. Refer to ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security," June 17, 2019; and, NSIRA Meeting with on June 18, 2019.

[36] ERC Email to NSIRA, "Briefing to SIRC on 2019-05-14," May 21, 2019.

[38] Refer to case files

[39] Refer to file

[40] NSIRA Meeting with June 21, 2019.

[41] Refer to previous footnote with file numbers.

had been polygraphed

NSIRA was told that this practice, although said to be procedurally sound has been discarded given an update to the methodology.[42]

NSIRA believes that when changes are made to polygraph processes they must be documented. This is necessary to ensure precision on what standard is being applied when making a determination CSIS raised the concern that if the standard was written down, which could result in exploitation.[43] NSIRA notes that this concern could be alleviated if the standard is embedded within the methodology, which is not made available to the general employee population. acknowledged that they may update the methodology to include this standard once more time has elapsed to determine its utility.[44]

Another issue of standardization raised over the course of the review involved assessment of medical issues disclosed by examinees. The CSIS polygraph consent form states the following:

> I understand that I will be asked personal, medical and psychological as well as security questions during the pre-polygraph interview. The answers to these questions allow the Examiner to determine my fitness to undergo a polygraph test.[45]

When asked to provide the training given to polygraph examiners to help them make assessments on medical disclosures, CSIS responded that "training on physiology and anatomy is provided"

During a subsequent meeting with they stated that examiners are not medically trained, and emphasised that they are only required to collect minimal medical details on examinees.[47] In the course of the review, however, NSIRA observed that, in the context of a polygraph examination

Further, although emphasised that medical conditions can impact test results, was unable to demonstrate how the specific medical information collected pertains to the proper functioning of the polygraph test.[48]

NSIRA observed evidence which raises concerns about how medical information provided by examinees is used by One examiner made comments regarding

[42] Refer to NSIRA meeting with June 21, 2019; and, Refer to file
[43] NSIRA Meeting with June 17, 2019.
[44] NSIRA Meeting with June 17, 2019.
[45] CSIS Polygraph Consent Form, provided to NSIRA via ERC email on April 23, 2019.
[46]

Refer to ERC Memo to NSIRA, "Additional Questions on Polygraph," June 7, 2019.
[47] NSIRA Meeting with June 18, 2019.
[48] The methodology was reviewed by the Senior Research Advisor on July 19th, 2019.

In another example, a polygraph examiner commented

No evidence contained within methodology, or within responses to questions, defines boundaries between polygraph and medical analysis. In the absence of written clarification, medical questions asked of examinees may be assessed by polygraph examiners, despite the absence of medical training. This practice requires attention by CSIS management; and consideration should be given to the privacy impacts[51] of collecting personal medical information in the context of a polygraph examination.

Privacy implications of the polygraph examination

Given that the polygraph is an invasive tool, employees are required to consent to having it administered if they want to have their ETS clearance granted or renewed.[52] NSIRA therefore enquired about Privacy Impact Assessments (PIAs) conducted on the polygraph process at CSIS. According to TBS, a PIA is to be initiated for a program or activity whenever personal information is used for, or is intended to be used as, part of a decision-making process that directly affects the individual.[53] Despite this policy requirement, no PIA has been conducted on CSIS's polygraph process.

NSIRA believes that a PIA is necessary for a program as invasive as the polygraph not only to help ensure the proper collection, handling and storage of personal information; yet equally important, as a signal to employees that the process is as transparent and respectful as possible. Over the course of the review, IS told NSIRA that a decision has been made to conduct a PIA in the coming months.[54]

---

[49] Refer to file E-mail dated December 14, 2018.

[50] In this case, Refer to

[51] notes that the CSIS polygraph booklet is currently being subjected to a Privacy Impact Assessment (PIA). See IS comments on draft report 2018-15, received July 29, 2019.

[52] In 2016, examined its polygraph consent form authority, purpose, caution (i.e. a condition of employment) and consent to polygraph. This was undertaken in consultation with DLS It was approved by the DG IS on April 5, 2018. Refer to ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security," June 17, 2019.

[53] The other circumstances that require a PIA include: upon substantial modifications to existing programs or activities where personal information is used or intended to be used for an administrative purpose; and when contracting out or transferring a program or activities to another level of government or the private sector results in substantial modifications to the program or activities. Refer to TBS Directive on Privacy Impact Assessment, s.6.3.1, April , 2010.

[54] CSIS's complete response reads: "Over the course of the last month, Internal Security has re: the completion of a

" Refer to ERC Memo to NSIRA, "Additional Questions on Polygraph," June 7, 2019.

In the absence of a PIA, NSIRA enquired about other mechanisms or processes by which to gauge employee experiences with the polygraph. CSIS employees both understand the need to take the polygraph and expect that their examination will be conducted professionally. Despite this reasonable expectation, there is no employee survey question exclusive to polygraph-related activities, although test subjects can raise issues with the Chief or D/ Chief in writing or in person.[55] For its part, stated that they only received "approximately 1 or 2 complaints" last year about the polygraph.[56]

CSIS must have reliable data upon which to rate the activities of polygraph examiners. Just over a year ago, the CSIS Director publically acknowledged that harassment, bullying, and reprisals are issues which need to be addressed across the Service. Although NSIRA has no evidence of systematic harassment, bullying or reprisals from

All CSIS employees must fall under the Director-led CSIS People and Respect Strategies launched over the past year,[59] and is no exception.

NSIRA recommends that CSIS strengthen internal governance over activities, including modifying the methodology for conducting polygraph assessments, as appropriate.

Finding no. 4: Effectiveness of Policies and Procedures Pertaining to the Polygraph

Based on the information reviewed and interviews conducted, NSIRA finds that:

- **The polygraph is central to CSIS' inquiry and five-year update processes;**

CSIS does not have policy clarity regarding how this issue is to be addressed.

NSIRA expected to see, pursuant to the SSS, that the polygraph is one tool, among many, used to help CSIS make effective assessments on loyalty and reliability as it relates to loyalty.

---

[55] ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security," June 17, 2019.

[56] felt confident that employees are generally supportive of the polygraph process, citing examples where employees "thanked the polygraph examiner". Refer to ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security," June 17, 2019.

[57] Given the fear of reprisals, few of the employees met by NSIRA wanted their names officially recorded. That said, ERC is aware of the employees who reached out to NSIRA in order to raise concerns about their polygraph experiences. NSIRA does not believe that the employees are a representative sample, and therefore, concludes that the information supplied must be properly assessed as anecdotal.

[58] NSIRA Meeting with June 17, 2019.

[59] Stemming from harassment complaints within CSIS which the CSIS Director acknowledged were founded, the goal of the Respect Campaign is to promote awareness, increase employee engagement, and ultimately, transform the workplace. The CSIS People Strategy, meanwhile, integrates and guides a host of interrelated initiatives that are modernizing how CSIS selects and develops employees; how employees are guided in their work; and how CSIS ensures that employees are safe and respected in the workplace. Refer to CSIS's The Source: Respect Campaign and People Strategy.

Additionally, NSIRA expected to see that the polygraph has been used by CSIS in a reasonable and necessary manner when making assessments on loyalty and reliability as it relates to loyalty.

Use of Polygraph for Security Assessments

Historically, CSIS has underscored that security clearances or employment are not denied solely based on a polygraph examination; supporting evidence from other sources has always been required. For example, testifying before the Standing Committee of the House of Commons on Justice and Solicitor General on December 11, 1986, the Director of CSIS noted in particular that the polygraph examination is only one of numerous steps in the recruitment process and that any concerns raised by this test are pursued by investigation afterwards. He went on to state that:

> I think were it so that the polygraph was used as the single tool for determining whether someone is being reticent or untruthful in terms of the answers provided, it would be quite wrong, and if that were the case we would not be using it.[60]

SIRC has been critical of the use of the polygraph by CSIS; and has questioned the polygraph's accuracy and the extent to which it was voluntary. For example, in 1992 the Committee stated:

> Starting with our 1985-86 Annual Reports, we have criticized the way CSIS uses the polygraph in seven consecutive reports. We continue to doubt the accuracy of polygraph examinations and their validity in security screening programs. The error rate of the test (ten per cent or more), combined with the test's perceived scientific legitimacy, creates too high a risk of serious injustice to a person who appears to have the intent to deceive or whose test results appear inconclusive. We believe the polygraph is given more weight than its reliability warrants.[61]

This historical perspective has contemporary relevancy. The SSS cites the polygraph as one assessment measure among many available to Canadian departments and agencies. Significantly, the SSS is silent on what is to transpire if an applicant or employee fails the examination; the expectation appears to be that a thorough assessment is derived from the cumulative use of all available tools.[62]

At the start of the review, affirmed that the polygraph is not determinative.[63] However, at a subsequent briefing, IS indicated that, in order to be granted an ETS clearance, an individual must pass the polygraph exam.[64]

---

[60] SIRC Public Annual Report, 1986-1987, p.47.
[61] SIRC Public Annual Report, 1991-92, p.53.
[62] SSS, Appendix B Section 7. Other tools cited by the SSS include identity and background verification, educational and professional credential verification, personal and professional reference checks, law enforcement inquiry, financial inquiry, CSIS security assessment, security questionnaire, security interview, and open-source inquiry.
[63] NSIRA meeting with May 14, 2019.
[64] NSIRA meeting with IS, June 18, 2019

Over the course of the review, it became clear that for external applicants

This evidence contradicts original claim that the polygraph is not determinative and supports the indication by IS that, in order to be granted an ETS clearance, the individual must pass the polygraph examination.

For employees, there is added complexity

Procedural fairness requirements outlined in the SSS and internal CSIS policies require that employees be provided with an opportunity to respond to any adverse information before a decision relating to the security assessment is made.[68]

A failed polygraph would appear to constitute adverse information, as this is certainly the standard being applied to outside applicants

In general, there appears to be a dual standard in CSIS's use of the polygraph for screening external applicants and employees

[65] ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security," June 17, 2019.
[66] Both external and internal applicants are entitled to procedural fairness protections offered in the "resolution of doubt" process as prescribed by the SSS and CSIS internal policies before having a clearance rejected.
[67] Refer to files and

[68] It should be noted, that external candidates are also afforded the opportunity to respond to adverse information throughout the screening process. Refer to SSS, Appendix D Section 2.
[69] CSIS claims that
Refer to NSIRA meeting with June 17, 2019.

Risk mitigation stemming from unresolved polygraph results

believes that if the proper methodology is followed, the polygraph is scientifically accurate [70]

Assuming that the polygraph is highly reliable, the remaining question is how CSIS risk manages employees who have an unsuccessful result.

The statistical information provided by presents a challenge in assessing risk management. Over the course of the review, NSIRA repeatedly requested statistical information on the program, and sat down with polygraph examiners in order to discuss the supplied data. To illustrate, in 2018-2019 conducted tests, with the following results:

Type of Test	Type of Result	Percentage[72]
Loyalty	Significant Reactions & Admission	
	Significant Reactions & No Admissions	
Reliability	Significant Reactions & Admission	
	Significant Reactions & No Admissions	

acknowledged that producing macro data is difficult given the technical limitations of their current database.[73] This also means that there is no clear picture of organisational risk regarding unresolved polygraph results (i.e. significant reactions, inconclusive reactions, etc.).

NSIRA conducted additional research outside of CSIS in order to appropriately situate the observations made over the course of the review

For example, a recent review was conducted by the United States Office of the Inspector General (Department of Justice) on how the Federal Bureau of Investigation (FBI) has responded to unresolved results in polygraph examinations. Although the polygraph methodologies are presumed to be dissimilar, the issue of

[70] NSIRA Meeting with June 21, 2019.

ERC Memo to NSIRA, "Additional Questions on Polygraph," June 7, 2019.

[72] ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security," June 17, 2019.

[73] NSIRA meeting with June 21, 2019.

unresolved results should be of equivalent risk management concern to both CSIS and the FBI. The U.S. review found that:

> The FBI's policy generally prohibits access to Sensitive Compartmented Information for FBI employees who have not passed a polygraph examination within a specified period. We identified instances in which employees unable to pass multiple polygraph examinations were allowed to retain access to sensitive information, systems, and spaces for extended periods of time without required risk assessments…[74]

If there are serious admissions provided by the employee in the context of a security assessment, the employee will fall onto CSIS's Complex Case list, and appropriate scrutiny follows.[75]

As discussed above, CSIS has procedurally sought to

This is to help maintain accurate test results and avoid

NSIRA enquired about the circumstances that would permit an employee to avoid taking the polygraph entirely. CSIS responded that an employee can refuse to undergo a polygraph examination on a specific day due to health issues, work-related issues or decide at any time to recuse themselves from the process. However, a valid polygraph is a requirement for an ETS clearance at CSIS; therefore, in the case of a refusal, according to the SSS, the ETS clearance could be administratively cancelled due to a lack of cooperation or disciplinary actions against the employee could be pursued.

notes that under s. 6 of the *CSIS Act*, the Director has the authority to exempt individuals from undergoing a polygraph examination.[76] However, and regardless of the Director's prerogative, NSIRA has reviewed internal correspondence which makes clear that polygraph exemptions are not a policy option.[78] Further, IS confirmed that only temporary exemptions are issued and that any exemption is reassessed periodically. IS also confirmed that any deferrals are granted as a result of

---

[74] Office of the Inspector General, United States Department of Justice, "Public Summary: Review of the Federal Bureau of Investigation's Response to Unresolved Results in Polygraph Examinations," p.1, March 2018.
[75] A good example of this is
[76] Policy on Individual Security Screening, SEC-1200, s.3.16.
[77] ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security," June 17, 2019. However, on July 30, 2019, NSIRA received a contradictory comment on the draft report which stated: "Exemptions would be recorded on the subject's file, usually in the database
[78] Refer to File E-mail dated February 25, 2019.

cooperation with Occupational Health and Safety partners at CSIS.[79]

Employees who spoke to NSIRA on condition of anonymity described the negative impact that their unfavorable polygraph results had on their lives

This was also evident during documentation review of post-exam correspondence between employees and

Nevertheless, NSIRA believes that CSIS needs to address the security and procedural fairness implications stemming from the above-noted observations. "CSIS Procedure: Use of the Polygraph Exam in an Internal Security Administrative Investigation" was not updated along with the rest of the IS policy suite, resulting in contradicting terminology (i.e. the distinction between inquiries and investigations) and directions. Additionally, no policy or procedure exists specific to the conduct of polygraph examinations writ large.

In the absence of policy clarity, employees may continue to face negative impacts when they fail the polygraph. At the same time, there may exist a security risk that leaves CSIS vulnerable to insider threats, as there is a lack of policy clarity summarizing what risk mitigation strategies are to be applied in such scenarios.

NSIRA recommends that CSIS update applicable policy and procedures on the use of the polygraph to address security and procedural fairness implications stemming from failed polygraph results.

[79] ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security," June 17, 2019.
[80] For example, refer to
[81] NSIRA meeting with CSIS, June 17, 2019.

Finding no. 5: Adequacy, Adherence, and Effectiveness of Policies and Procedures Pertaining to Complex Cases

Based on the information reviewed and interviews conducted, NSIRA finds that IS complies with the SSS and its own policies in its management of complex cases arising from the security assessment process, but notes that the associated decision-making could be strengthened with improved governance and policy clarity.

In its review of Internal Security case files, NSIRA expected to find that inquiries or investigations are conducted in a reasonable and necessary manner, and in compliance with the SSS and the CSIS's own policies and procedures.[82] Additionally, based on the findings of NSIRA's previous review, the Committee also expected to see that investigative activities are conducted with integrity and that critical case decisions are made objectively based on facts. Objective and consistent decision-making is an important component of managing security risks as per the TBS's SSS and CSIS's own policies.[83]

NSIRA welcomes the notable improvements observed within IS with respect to case file documentation[84] and efforts to remove bias and subjectivity from the investigative process.[85] A prominent example of these efforts is the creation of a tool, which intends to correct for subjectivity while analyzing risks posed by individuals' activities.

Adequacy of policy guidance regarding investigative techniques

The newly updated Procedure on Internal Security Inquiries and Investigations (the Procedure) states that "based on the findings of an Inquiry, or as required, the DG IS may recommend to the DDA that an Investigation be conducted." The Procedure then delineates the investigative techniques that would become available as a result of this escalation.

[82] Treasury Board Standard on Security Screening (SSS); CSIS Policy and CSIS Procedure on Individual Security Screening; CSIS Policy and Procedure on Inquiries and Investigations.
[83] SSS, s.5.1, s.5.2.1.
[84] Case files consulted as part of this review for the most part included the full spectrum of inquiry and investigative activities, including the first instances of problems being uncovered through to the conclusion of a case and associated decision-making.
[85] Refer to case

[86] Meeting with IS, April 24, 2019. Refer to deck entitled '
[87] CSIS Procedure: Internal Security Inquiries and Investigations, 3.2-3.3.
[88] CSIS Procedure: Internal Security Inquiries and Investigations, 3.3.3.

In this context, NSIRA notes that CSIS has not used this provision directly in any cases reviewed

Assessment of adverse information

With respect to any type of criminality or misconduct assessed as part of the screening or update process, certain themes and characteristics are present in most cases. In the context of the SSS, the relevant factors to be considered when making decisions on an individual's ability to hold reliability status or a security clearance are:

1. the type of infraction and its seriousness or nature;
2. the passage of time and the infraction's recentness;
3. the surrounding circumstances, such as the regularity or scale of the infraction committed;[93] and
4. the implications for the individual's reliability and their openness and cooperation with regard to disclosing it.[94]

NSIRA notes, however, that the Procedure on Individual Security Screening only states that adverse information concerning an individual be assessed with respect to its nature and seriousness – i.e. is only one of the assessment criteria stipulated by the SSS.[95] NSIRA also notes that this Procedure is used as operational guidelines by IS interviewers,[96] and that IS informally

[90] CSIS Procedures: Surveillance, s.3.4. NSIRA further notes that this procedure still refers to IS administrative investigations, and in the context of updated terminology (i.e. inquiry and investigations), it is unclear whether the reference is to either of the two, or to both.
[91] NSIRA meeting with IS, April 24, 2019.
[92] Refer to file

Further clarity was provided in an ERC Memo to NSIRA. "ERC Response to 2018-15 – SIRC Memo – Questions for IS – 5 23 2019." June 17, 2019:

[93] Other relevant circumstances to be considered include: the individual's willingness to participate, their maturity at the time of the incident(s), the degree of rehabilitation since the incident(s), and the potential for pressure, coercion, exploitation, or duress. (SSS, Appendix D.2)
[94] Standard on Security Screening, Appendix D.2
[95] Procedure on Individual Security Screening, S.7.3. The SSS also stipulates consideration of the relevant factors noted above.
[96] In response to NSIRA's question regarding the guidance materials used by IS interviewers, IS responded with the Procedure on Internal Security Inquiries and Investigations. Refer to E-mail from ERC, "2018-15 – SIRC Memo – Questions for IS – 5 23 2019 (3)," June 24, 2019.

incorporates the four assessment criteria in their decision-making process.[97]

Thresholds for criminality and misconduct

The cases reviewed by NSIRA typically revolved around elements of criminality by the individuals being screened, with decisions made based on the four relevant criteria outlined above. NSIRA was informed in a briefing with IS that the SSS only provides very broad guidance with respect to criminality thresholds, and does not offer guidance relating to admissions of involvement of criminal activity unknown to law enforcement in the context of adverse information.[98] As a result, CSIS must apply its own standards in evaluating such admissions in the context of security screening.[99] In this regard, CSIS noted the following:

> Since there is no official threshold outlined in the TBS SSS, IS conducts their assessment by leveraging tools and resources at their disposal. This includes but is not limited to:

However, NSIRA did not observe evidence of standards being comprehensively codified in the guidance materials used by investigative staff. For example, the CSIS Subject Interview Questionnaire Reference Guide could include more comprehensive guidance to interviewers regarding criminality or misconduct uncovered through the interview.

[97] In response to a question by NSIRA regarding a particular case file, IS clarified their decision-making Refer to E-mail from ERC, "SIRC ANSWERS – Additional Questions for IS," June 24, 2019.
[98] ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security, 17 June 2019.
[99] IS further noted that minor types of criminality are less of a concern as compared to serious, indictable offences such as murder and viewing of child pornography. Refer to meeting with 14 May 2019.
[100] ERC Memo to NSIRA, "ERC Response to 2018-15 – SIRC Memo – Questions for IS – 5 23 2019," June 17, 2019.
[101] Refer to CSIS Subject Interview Questionnaire Reference Guide, Page 1.
[102] Refer to CSIS Subject Interview Questionnaire Reference Guide, Page 7.

[103] These criteria are referring overall to the four general assessment criteria outlined in the SSS, Appendix D.

Decision-making in security assessments

In its review of security assessments, NSIRA observed that it was difficult to arrive at a conclusive assessment on the consistency of the application of criminality and conduct standards between cases.

In a memo to NSIRA, CSIS wrote:

While NSIRA accepts this explanation, it is also important to note that in several cases CSIS shared information, obtained during a screening process, with other Government departments, which may have resulted in an adverse impact on the individual. This means that a negative decision on their file by CSIS could have career repercussions for those individuals with their original workplaces, some of which may not involve access to information as sensitive as that of the Service.[105] As such, these decisions carry significant potential impacts for individuals, and imply a great degree of responsibility for CSIS to make security status decisions that are procedurally fair and reflect accurately and consistently the degree of risk faced by the organization.

In employee cases, some variation was also observed in decisions rendered with respect to review and/or revocation of reliability status.[106] NSIRA accepts that no two cases center around exactly the same issues, making direct cross-comparisons difficult. However, for criminality issues uncovered as part of the screening process, it is important that case file documentation clearly and consistently differentiate the threshold at which a particular case crosses into unacceptable territory.

That said, NSIRA observed no evidence to suggest that these variations in decision-making are a result of favouritism or intentional bias on the part of IS interviewers. Indeed, NSIRA believes that CSIS has made improvements in reducing bias and subjectivity, and notes the as an example of such efforts.[108] Still, the decision-making in some of the cases of denials and revocations could be strengthened with an explanation regarding how each piece of adverse information is considered in the context of all four SSS assessment criteria referenced earlier, and in the context of general risk tolerance at CSIS, which was not consistently present in

[104] ERC Memo to NSIRA, "Confirmation of Facts and Questions for Internal Security, 17 June 2019.
[105] Refer to files
[106] The vast majority of issues underlying the cases reviewed by NSIRA pertained to reliability. Security clearance denials and revocations made up a small part of the cases reviewed.
[107] Refer to files

[108] Refer to

the case files.

Consistent evaluation of risk indicators

Guidance that is incomplete as to the criteria for assessing criminality and adverse information may result in decisions being rendered inconsistently across cases with similar issues. Further, this guidance needs to be consistent throughout the screening or update process to ensure relevant information is collected from the beginning of a case. The SSS principles of ensuring that the rendering of negative decisions on a security file are qualified and that consideration be given to exculpatory information are crucial throughout the assessment process, not only at its conclusion.

While NSIRA considers the as a positive step toward more consistent and reliable decision-making in case files, it is noteworthy that the tool itself is also subject to a degree of bias given that the weights assigned to the types of adverse issues are derived from the interpretation of IS management.

NSIRA believes that fair and consistent standards for interpreting criminality, including admissions to minor criminality would ensure that CSIS applies its judgements equally given the primacy of its role in security assessment for the Government of Canada. NSIRA notes that IS is undertaking macro-level tracking of decisions rendered and their associated rationale, which will improve the ability of IS interviewers to locate relevant previous decisions rendered as well as the considerations and circumstances involved. NSIRA supports IS's decision to solidify this responsibility within a new position to be created, and believes this will be a strong step toward improved documentation and definition of the practical threshold.[111]

[109] Refer to meeting with IS, April 24, 2019, and Deck entitled '

[111] Refer to E-mail from ERC, "FW: SIRC ANSWERS - Additional Questions for IS," June 24, 2019.

NSIRA recommends that IS further align its overarching policy suite with the assessment criteria for adverse information outlined in the SSS, Appendix D, as well as update the Questionnaire Guidebook with clear definitions to align to risk indicators

Finding no. 6: Provision of Information for NSIRA's Consideration

NSIRA received several pertinent legal opinions and legal documents only once the review was substantially written and complete, preventing their timely incorporation and consideration in the final report.

Throughout the course of the review, NSIRA requested from CSIS relevant legal opinions pertaining to various Internal Security processes and practices. Specifically, legal opinions were sought consistently throughout the month of May, and were only received by NSIRA in July once the drafting of the report was substantially complete.

As a result of delayed disclosure, a total of five pertinent legal opinions, and two other pertinent legal documents, were received after the report was drafted and sent through for internal review. NSIRA was able to make some amendments to the draft on certain specific issues in order to properly reflect the recently obtained information. However, these legal opinions were relevant to the issues covered in the report and the review would have benefitted from their full consideration.[112]

NSIRA notes that access to all of the other information pertaining to this review was provided efficiently and effectively both electronically and on paper files. This was no easy feat, given that much of the internal file information is classified as NTK. NSIRA commends CSIS for their effective disclosure in this regard and notes that only the legal opinions and legal documents were subject to late disclosure.

[112] This is not the first time that a review body has observed that CSIS has had difficulty accessing legal opinions and/or advice. In the Close Access Review (2015-01), SIRC observed that there was no clear process within CSIS for accessing legal opinions and/or advice that have been issued by CSIS's Directorate of Legal Services. Therefore, SIRC recommended that CSIS implement a process to ensure that relevant CSIS stakeholders have knowledge of, and access to, legal opinions and/or advice.

ANNEX A: Meetings and Information Sessions

April 5, 2019: Meeting on Program Overview with Internal Security

DDG IS, Chief Deputy Chief DDG Infrastructure Security, Chief Infrastructure Security, ERC Chief, Chief Management Services, ERC Review Officer, NSIRA Senior Research Advisor, NSIRA Research Analyst, NSIRA Director of Research, NSIRA Legal Counsel

April 24, 2019: Meeting on the Insider Threat and Internal Security

DDG IS, Chief ERC Chief, ERC Review Officer, NSIRA Senior Research Advisor, NSIRA Research Analyst, NSIRA Director of Research, NSIRA Legal Counsel

May 1, 2019: Meeting on Internal Inquiries and Investigations with Internal Security

DDG IS, Chief Head Investigations, ERC Chief, ERC Review Officer, NSIRA Senior Research Advisor, NSIRA Research Analyst, NSIRA Director of Research, NSIRA Legal Counsel

May 14, 2019: Meeting on Polygraph with Internal Security's

DDG IS, Chief Deputy Chief ERC Chief, ERC Review Officer, ERC Head of Complaints, NSIRA Senior Research Advisor, NSIRA Research Analyst, NSIRA Legal Counsel

June 17, 2019: Meeting on Polygraph Methodology with Internal Security's

A/DG IS, Chief Deputy Chief NSIRA Senior Research Advisor, NSIRA Research Analyst, NSIRA Director of Research, NSIRA Legal Counsel

June 21, 2019: Meeting on Polygraph Statistics with Internal Security's

Chief Deputy Chief NSIRA Senior Research Advisor, NSIRA Research Analyst, NSIRA Legal Counsel

DDG: Deputy Director General

ERC: External Review and Compliance

ANNEX B: Case Files Reviewed

As part of this review, NSIRA conducted in-depth analysis of the case files listed below. These files include a random and selected sample from the Complex Case file list received from IS; other IS case files; some of the individuals' associated polygraph files; and denials and revocations issued within the last five years. The case file review included a review of dozens of pieces of documentation within each file, including e-mails exchanged between management, IS interviewers, and polygraph examiners responsible for the files – with a view to determine decision-making patterns and documentation. The documentation reviewed also included IS reports, polygraph reports, briefing notes to the DG/IS, memos to the Director, other ad-hoc documents and reports, and letters issued to individuals who had their security status denied or revoked.

ANNEX C: FIVE EYES Use of the Polygraph

Use of the Polygraph by Five Eyes States for Enhanced Top Secret Clearances[113]				
Australia	Canada	New Zealand	United Kingdom	United States
	Yes			