



**National Security  
and Intelligence  
Review Agency**

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

# **Review of the Communications Security Establishment's Use of the Polygraph for Security Screening**

---

**NSIRA // Review 21-05**

---

# Table of Contents

---

<b>List of Acronyms .....</b>	<b>ii</b>
<b>Executive Summary .....</b>	<b>iii</b>
<b>1. Introduction .....</b>	<b>1</b>
Authority.....	1
Scope of the review .....	1
Methodology .....	1
Review statements.....	3
<b>2. Background .....</b>	<b>3</b>
What is the polygraph? .....	3
Past review of the polygraph in Canada .....	5
CSE's authority to use the polygraph.....	6
CSE's use of the polygraph for security screening.....	7
<b>3. Findings, Analysis, and Recommendations .....</b>	<b>10</b>
Privacy implications .....	10
Polygraph operations.....	19
Security screening decision-making.....	22
Treasury Board Standard on Security Screening.....	26
<i>Canadian Charter of Rights and Freedoms</i> .....	30
<b>4. Conclusion.....</b>	<b>33</b>
<b>Annex A. Findings and Recommendations .....</b>	<b>34</b>

## List of Acronyms

---

**APA** American Polygraph Association

**CQT** Comparison Question Technique

**CSE** Communications Security Establishment

**CSIS** Canadian Security Intelligence Service

**DI** Deception Indicated

**ETS** Enhanced Top Secret (security clearance)

**GC** Government of Canada

**HR** Human Resources

**LERC** Law Enforcement Records Check

**MD** Ministerial Directive

**NDI** No Deception Indicated

**NSIRA** National Security and Intelligence Review Agency

**PIA** Privacy Impact Assessment

**PSO** Personnel Security Officer

**QC** Quality Control

**RCMP** Royal Canadian Mounted Police

**SAP** Suitability Assessment Panel

**SIRC** Security and Intelligence Review Committee

**TBS** Treasury Board of Canada Secretariat



SECRET//CEO

## Executive Summary

---

This review examined the Communications Security Establishment's (CSE) use of the polygraph for security screening, as well as the Treasury Board of Canada Secretariat's (TBS) role in establishing the Standard on Security Screening (the Standard) which governs the use of the polygraph as a security screening activity for the Government of Canada (GC).

The National Security and Intelligence Review Agency (NSIRA) found that the policies and procedures in place at CSE governing the use of the polygraph for security screening inadequately address privacy issues. In particular, CSE did not conduct a Privacy Impact Assessment (PIA) to assess the implications of the collection and use of personal information via the polygraph. CSE did not consider whether all information collected during a polygraph exam, such as detailed personal and medical information, was directly related to or necessary for security screening. Additionally, CSE polygraph examiners applied an ad hoc approach in the assessment of medical information collected during polygraph exams. Furthermore, CSE's use of personal information collected during polygraph exams for staffing purposes may have exceeded the consent provided and may not have complied with section 7 of the *Privacy Act*. Finally, CSE obtained the consent of subjects to undergo a polygraph exam based on inaccurate or misleading information about the reliability or validity of the polygraph.

NSIRA also found issues with the way in which CSE operated its polygraph program. Repetitive and aggressive questioning by CSE polygraph examiners, often prompted by an initially negative assessment, risks causing some subjects to inadvertently fabricate information in an effort to explain an unfavourable polygraph assessment. As well, quality control measures were not always in line with CSE policy and were insufficient to ensure that CSE made security screening decisions that were based on the highest quality and most reliable polygraph assessments. CSE also experienced significant retention issues as approximately 20% of audiovisual recordings of polygraph exams requested by NSIRA were unavailable due to technical errors.

NSIRA also found issues with the way in which CSE used the results of polygraph exams to inform security screening decision-making. CSE conducted multiple polygraph exams to resolve doubt, such as that raised by a deception indicated or inconclusive result alone, rather than conducting a resolution of doubt process as provided for under the Standard. CSE placed an inordinate importance on the polygraph in security screening decision-making, to the extent that other, less intrusive security screening activities were insufficiently used or not used at all. Moreover, the results of polygraph exams were *de facto* determinative in security screening decision-making and CSE's practices regarding record-keeping for security screening decisions may not comply with



SECRET//CEO

requirements outlined in the Standard. Finally, NSIRA found that the way in which CSE uses the polygraph in security screening makes uncertain the opportunity to challenge denials of security clearances pursuant to the *National Security and Intelligence Review Agency Act* (NSIRA Act) and the Standard.

As it relates to TBS's role in establishing the government-wide policy on the use of the polygraph for security screening, NSIRA found serious issues as well. TBS failed to adequately consider the privacy or *Canadian Charter of Rights and Freedoms* (Charter) implications that could result from the use of the polygraph for security screening. Furthermore, the Standard lacks appropriate safeguards to sufficiently address Charter and privacy implications resulting from the use of the polygraph for security screening by the GC.

When taken as a whole, these findings indicate more broadly that CSE's use of the polygraph for security screening, and TBS's authorization of the polygraph as a security screening activity under the Standard, raise serious concerns related to the Charter.

In light of these findings, NSIRA recommends that CSE and TBS both urgently address the fundamental issues related to the legality, reasonableness and necessity of the use of the polygraph for security screening detailed in this report. If these issues are not urgently addressed, TBS should remove the polygraph from the Standard and CSE should cease using it for security screening altogether.

# 1. Introduction

---

## Authority

1. This review was conducted under the authority of paragraphs 8(1)(a) and 8(1)(b) of the *National Security and Intelligence Review Agency Act* (NSIRA Act).

## Scope of the review

2. NSIRA began this review in March 2021. According to the original terms of reference, it was intended to be a “comprehensive review [of the Communications Security Establishment’s (CSE) internal security programs] to assess whether CSE’s internal policies and procedures are compliant with applicable laws, Ministerial Directives and are reasonable and necessary.”
3. As this work progressed, NSIRA determined that a review of all internal security programs at CSE would be too broad. NSIRA limited the scope of this review to an assessment of the legality, reasonableness, necessity and efficacy of CSE’s use of the polygraph for security screening. The Treasury Board of Canada Secretariat’s (TBS) role in developing the Standard on Security Screening (the Standard), and the justification for inclusion of the polygraph in the Standard, remained within scope.
4. NSIRA focused on polygraph operations at CSE between January 1, 2018 and July 1, 2021. Relevant documentation from outside the period under review was also included, such as legal advice and internal policies and procedures. For instance, the majority of material related to the development and implementation of the Standard by TBS dated from before 2014.

## Methodology

5. NSIRA analyzed information primarily from CSE and TBS over the course of this review. It also analyzed some information from the Department of Justice and the Royal Canadian Mounted Police (RCMP). NSIRA obtained relevant information through regular requests for information, but also further written explanations, verbal briefings from subject matter experts and a demonstration of CSE’s security screening information management system.
6. A comprehensive and independent review of the use of the polygraph at CSE required a factual understanding of the operational realities of the polygraph. Access to detailed security screening files, including audiovisual recordings of polygraph exams, was critical to NSIRA’s understanding of how CSE conducts



SECRET//CEO

polygraph examinations and its assessment of CSE's practices for compliance with the law and existing policy.

7. To accomplish this, NSIRA reviewed a sample of recorded polygraph examinations and associated security screening files at CSE. This sample consisted of 51 security files and was selected based on the reason for administering the polygraph (new applicant, five-year update, etc.) rather than on any personally identifiable information, such as name, age, ethnicity, sex, gender or other personal characteristics. Some of the files included multiple polygraph exams. From the larger sample, NSIRA reviewed 15 of the security files in greater detail, which included observing the audiovisual recordings of polygraph exams.
8. NSIRA recognized the sensitivity of personal information subjects provide to CSE throughout the security screening process. In consideration of the privacy of individuals, NSIRA authorized CSE to take the following steps to de-identify and anonymize the files reviewed:
  - a) CSE applied visual blurring and voice modulation techniques to the recordings so that visual or auditory identification of subjects depicted would not be possible;
  - b) CSE redacted personally identifiable information<sup>1</sup> from the polygraph examination report and security screening files; and,
  - c) CSE notified subjects whose files were selected by NSIRA for review. CSE provided them with an opportunity to consult their files and to identify potential conflicts of interest or to express any specific objections to NSIRA's access. No objections were raised to NSIRA's attention. A small number of potential conflicts were raised, such as CSE employees supporting external review activities. When this occurred, NSIRA selected an alternate file.
9. NSIRA is confident that the above-noted procedures and limitations struck an appropriate balance between respect for the privacy of individuals and access to the information required to review CSE's use of the polygraph for security screening.

---

<sup>1</sup> This included the subject's name, date and place of birth, address, personal telephone and email selectors, and related family details.



## Review statements

10. TBS met NSIRA's expectations for responsiveness during this review. However, CSE only partially met NSIRA's expectations for responsiveness. For 11 months, CSE resisted providing NSIRA with access to audiovisual recordings of polygraph exams which NSIRA had determined relevant for this review. This delay prevented NSIRA from completing this review in a timely manner.<sup>2</sup>
11. NSIRA was able to verify information for this review in a manner that met NSIRA's expectations.

## 2. Background

---

### What is the polygraph?

12. The Government of Canada (GC) defines a polygraph as "an examination that uses questioning techniques and technology to record physiological responses which might indicate deception by an individual."<sup>3</sup> To do this, the polygraph records "physiological... phenomena – typically, respiration, heart rate, blood pressure, and electrodermal response (electrical conductance at the skin surface)."<sup>4</sup> Practitioners claim that the systems of the human body associated with these physiological phenomena are the most likely to react when threatened, and these reactions can be measured to detect deception.<sup>5</sup>
13. Proponents of the polygraph, such as practitioners represented by the American Polygraph Association (APA), argue that it is an effective and reliable means to assess deception. A central tenet behind the polygraph is the belief that deception is intrinsically linked with human physiology. The polygraph measures observable and recordable physiological responses, such as cardiovascular, respiratory, and electro-dermal activity. The underlying assumption is that these physiological responses translate into indicators of deception or truth-telling. Proponents also

---

<sup>2</sup> NSIRA's expectations for responsiveness in reviews are available online at <https://nsira-ossnr.gc.ca>.

<sup>3</sup> Treasury Board of Canada. 2014. *Standard on Security Screening, appendix A – Definitions*.

<sup>4</sup> United States, National Research Council. 2003. *The polygraph and lie detection*. Washington, DC: The National Academies Press.

<sup>5</sup> Krapohl, D.J. and Shaw, P.K. (2015). *Fundamentals of Polygraph Practice*. Elsevier, Inc.

SECRET//CEO

cite high accuracy rates for the detection of deception based on peer-reviewed field and laboratory testing.<sup>6</sup> In briefings, CSE indicated that the balance of scientific research is in favour of the polygraph as a legitimate activity for security screening.

14. However, almost all of the available research supporting the reliability of the polygraph consulted by NSIRA was conducted by or in association with the APA. The APA is an American professional association that provides certification to polygraph examiners primarily in the United States, but also Canada.<sup>7</sup> The APA also produces and funds research that is often used as the basis to support arguments in favour of the polygraph as an effective and reliable means of detecting deception. Independent scholars question the validity of APA-funded research, citing that it can be biased or based on unreliable or incomplete data.<sup>8</sup>
15. The linkage between physiology and deception is openly disputed in the scientific community. Many researchers are unconvinced of the inherent link between physiology and deception and emphasize physiological uniqueness and the potential for varied responses across individuals. Many of these researchers also claim that the polygraph captures physical reactions of fear and stress, which are not unique to lying or truth-telling. Furthermore, there is evidence that would suggest that neuro-diverse individuals, people diagnosed with mental illness or those who live with anxiety, or other social stigmas may demonstrate varied physiological responses not accounted for in existing polygraph methodology.<sup>9</sup>
16. Unlike the APA, the American Psychological Association has been critical of the polygraph. It has stated that "there is no evidence that any pattern of physiological reactions is unique to deception... One reason that polygraph tests may appear to be accurate is that subjects who believe that the test works... may confess or will

---

<sup>6</sup> Nelson, R. 2015. Scientific basis for polygraph testing. *Polygraph* 44(1); and Krapohl, D.J. and Shaw, P.K. (2015). *Fundamentals of Polygraph Practice*. Elsevier, Inc.

<sup>7</sup> American Polygraph Association. 2023. *About the APA*. [https://www.polygraph.org/about\\_the\\_apa.php](https://www.polygraph.org/about_the_apa.php).

<sup>8</sup> Iacono, W.G. and Ben-Shakar, G. 2019. Current status of forensic lie detection with the comparison question technique: an update of the 2003 national academy of sciences report on polygraph testing. *Law and Human Behavior*. 43(1).

<sup>9</sup> Saxe, L. 1991. Science and the CQT polygraph: a theoretical critique. *Integrative Psychological and Behavioral Science*. 26(3); Saxe, L. 1994. Detection of deception: polygraph and integrity tests. *Current Directions in Psychological Science*. 3(3); Grubin, D. 2010. The polygraph and forensic psychiatry [editorial]. *Journal of the American Academy of Psychiatry and the Law*. 38(4); Synnott, J, Dietzel, D, and Ioannou, M. 2015. A review of the polygraph: history, methodology and current status. *Crime Psychology Review*. 1(1); and White, R. 2001. Ask me no questions, tell me no lies: examining the uses and misuses of the polygraph. *Public Personnel Management*. 30(4).



SECRET//CEO

be very anxious when questioned. If this view is correct, the lie detector might be better called a fear detector."<sup>10</sup>

17. In 2003, the National Research Council of the US National Academy of Sciences (NAS) released a comprehensive and wide ranging study of the polygraph.<sup>11</sup> This study has often been cited by both proponents and detractors as supporting arguments both for and against the polygraph. In 2018, Researchers from the University of Minnesota and the Hebrew University of Jerusalem revisited the findings of the 2003 study and found that:

The NAS report concluded that the scientific basis of the comparison question technique (CQT) was weak, the extant research was of low quality, the polygraph profession's claims for the high accuracy of the CQT were unfounded, and, although the CQT has greater than chance accuracy, its error rate is unknown. Polygraph proponents argue that current research indicates that the CQT has 90% or better accuracy, [that] the... [NAS] analysis supports this accuracy claim, and the CQT qualifies as legally admissible scientific evidence. [However]... the NAS report has been misrepresented and misinterpreted by those who support use of the CQT in forensic settings... [T]he quality of research has changed little in the years elapsing since the release of the NAS report, and... the report's landmark conclusions still stand.<sup>12</sup>

18. In briefings provided to NSIRA, both CSE and TBS stated that the reliability and efficacy of the polygraph when used in the security screening context is supported by valid scientific research. However, neither CSE nor TBS were able to produce any such studies to justify their position, including those cited above. The research consulted by NSIRA simply does not support the existence of a scientific consensus supporting the reliability or validity of the polygraph as a means to detect deception.

## Past review of the polygraph in Canada

19. Dating back to 1985, the Security Intelligence Review Committee (SIRC) found deficiencies related to the Canadian Security Intelligence Service's (CSIS) use of the polygraph, including privacy and reliability concerns. SIRC called on CSIS to stop using the polygraph test in seven consecutive annual reports from 1985-1992. SIRC also raised serious doubts about the accuracy and reliability of polygraph

---

<sup>10</sup> American Psychological Association. 2004, accessed 2023 (Oct). *The Truth about Lie Detectors (aka Polygraph Tests)*. <https://www.apa.org/topics/cognitive-neuroscience/polygraph>.

<sup>11</sup> United States, National Research Council. 2003. *The polygraph and lie detection*. Washington, DC: The National Academies Press.

<sup>12</sup> Iacono, W.G. and Ben-Shakar, G. 2019. Current status of forensic lie detection with the comparison question technique: an update of the 2003 national academy of sciences report on polygraph testing. *Law and Human Behavior*. 43(1).



SECRET//CEO

results, questioned the acceptable error rate in polygraph exams and recommended the government conduct an in-depth study of the implications of using the polygraph in the screening of prospective and current employees.

20. In 2019, NSIRA completed a review of the Internal Security Branch of CSIS. This review included an assessment of CSIS' use of the polygraph and identified several issues with the way in which it was employed by CSIS in the screening and internal investigations context. That review found that the polygraph can have profound negative impacts on an employee's mental health if not used appropriately. CSIS was unable to justify the merits of examiners – who are not medical practitioners – to ask medical-related questions. NSIRA also found that the polygraph was a determinative factor for external applicants in obtaining an enhanced top secret (ETS) security clearance from CSIS and that the outcomes or consequences for polygraph exams conducted on external applicants differed from those for CSIS employees. Finally, CSIS did not conduct a Privacy Impact Assessment related to its use of the polygraph for security screening.<sup>13</sup> As outlined below, many of these issues were similar to those found by NSIRA specific to the CSE context in this review.

## CSE's authority to use the polygraph

21. In 2014, TBS implemented the Standard, establishing the GC's policy for the use of the polygraph to conduct screening for ETS security clearances. Section 7 of the *Financial Administration Act* grants the Treasury Board the authority to establish policies and procedures related to general administrative matters for the GC, including those related to security. Under the Standard, the polygraph is the only additional activity used when conducting a security clearance at the ETS level.<sup>14</sup>
22. During the period under review, CSE also operated its polygraph program in accordance with a 2005 Ministerial Directive (MD) issued pursuant to subsection 273.62(3) of the *National Defence Act*. This MD formalized the practice of conducting polygraph exams for all new candidates for indeterminate and term employment, Co-op students, secondees, and contractors, a practice which had been in place at CSE since 2003. The MD also expanded the use of the polygraph to five-year security screening updates for employees hired after January 1, 2006. According to the MD "this will align CSE's hiring and security practices with those

---

<sup>13</sup> NSIRA, Review of CSIS's Internal Security Branch (NSIRA Study 2018-15), 2019. For an unclassified summary, see NSIRA 2019 Annual Report, available online at [https://www.nsira-ossnr.gc.ca/html/2018-2019/index.eng.html#section\\_5\\_3](https://www.nsira-ossnr.gc.ca/html/2018-2019/index.eng.html#section_5_3).

<sup>14</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, appendix B, section 1.

SECRET//CEO

of CSIS and its most critical international partner, the US National Security Agency.”

23. The MD placed certain limitations on the way in which CSE was to conduct polygraph examinations. First, the program was to be “implemented and managed in compliance with the *Canadian Charter of Rights and Freedoms* (the Charter), the *Canadian Human Rights Act*, the *Privacy Act* and other relevant legislation and existing government policies.” Second, the program was to be “rigorously managed, with professionals administering the tests, strict procedures and quality assurance, tightly controlled dissemination, storage, retention and destruction of information resulting from the tests, and periodic review.” Third, the polygraph was to be used “only as an investigative tool (i.e. there is no pass/fail applicable to polygraph results).” Fourth, polygraph results were not to be used as the “sole determinant” in security screening decisions or selection. Fifth, test questions were to “relate to loyalty only (i.e. they may not relate to questions of lifestyle and/or personal reliability).” Sixth, CSE was to report to the Minister annually regarding the results of the Polygraph.
24. This MD became of no force with the enactment of the *Communications Security Establishment Act* in 2019. Although the MD was only in force for a portion of the period under review, CSE’s polygraph operations continued largely unchanged between the MD and the Standard.

### CSE’s use of the polygraph for security screening

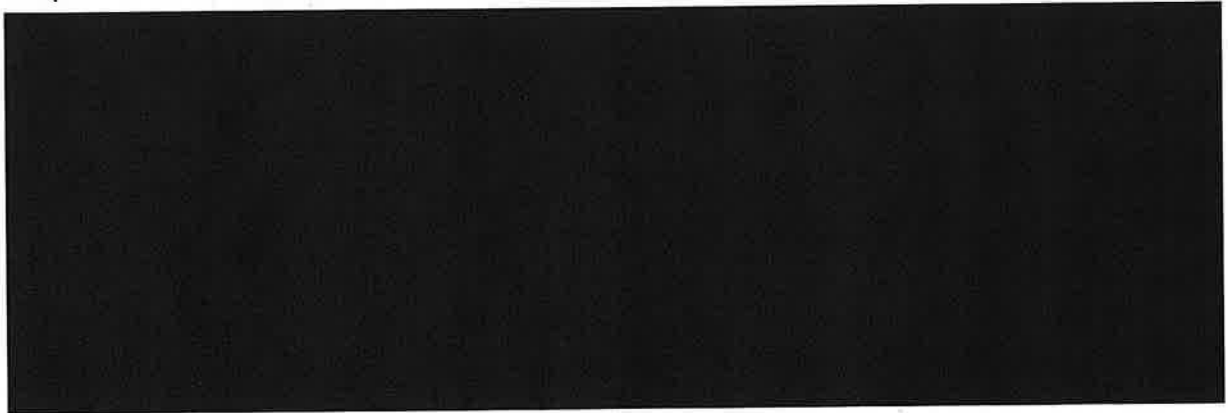
25. During the period under review, CSE conducted 3,187 polygraph exams for [REDACTED] individuals. CSE uses [REDACTED] [REDACTED] polygraph exam format. According to CSE, the [REDACTED] is a validated format for multiple-issue polygraph examinations approved by the American Polygraph Association (APA) and the Canadian Association of Police Polygraphists.
26. The [REDACTED] is a variation of the comparison question technique (CQT) style of polygraph exam. A CQT polygraph exam uses relevant and comparison questions to assess deception. Relevant questions are related to the issues of primary concern to the examiner, which, according to the Standard, are criminality and/or loyalty to Canada. The CQT style of polygraph assumes that an examinee seeking to be deceptive about the relevant issues of the exam will react physiologically more strongly to these questions rather than to the comparison questions. Conversely, the truthful examinee is likely to respond less significantly to the relevant questions, as they have nothing to conceal related to these issues, but will react more significantly to the comparison questions. A polygraph examiner will



SECRET//CEO

base their assessment of deception on the comparison of physiological responses between the relevant questions and the comparison questions.<sup>15</sup>

27. CSE conducts a polygraph exam in three stages. The first stage is a pre-polygraph interview where the examiner collects detailed biographical and medical information about the subject. The pre-polygraph interview focuses on the development of the relevant and comparison questions. Its purpose is to determine the precise wording of the questions that will appear on the polygraph exam. Examiners follow CSE's Polygraph Assessment Booklet to conduct the pre-polygraph interview. The second stage is the actual polygraph exam where the subject's physiological reactions are measured and recorded, while being questioned by the examiner. The third stage is the post-polygraph interview, where the examiner makes their initial assessment of the subject's truthfulness or deception regarding the relevant questions on the exam. CSE uses the post-polygraph interview as an opportunity for the examiner to explore any adverse information that the subject may have disclosed during the exam.
28. CSE polygraph exams include [REDACTED] relevant questions and [REDACTED] comparison questions. [REDACTED] relevant questions is the maximum number of questions allowed under the [REDACTED] format.<sup>16</sup> CSE refers to the relevant questions as "[REDACTED] questions" and to the comparison questions as "[REDACTED] questions" when discussing them with a subject. For this review, NSIRA will use the terms relevant and comparison when referring to these questions.
29. CSE has chosen relevant questions related to espionage, support for extremist violence, information handling practices and the withholding of information. During the period under review, CSE used the following [REDACTED] relevant questions:




---

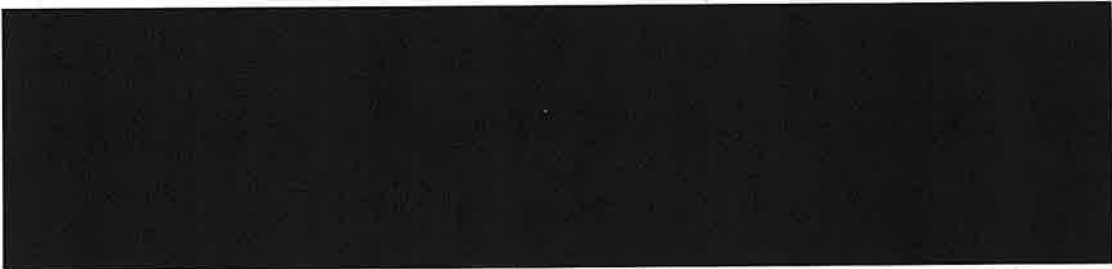
<sup>15</sup> United States, National Research Council. 2003. *The polygraph and lie detection*. Washington, DC: The National Academies Press.

<sup>16</sup> Krapohl, D.J. and Shaw, P.K. (2015). *Fundamentals of Polygraph Practice*. Elsevier, Inc.



SECRET//CEO

- 
30. The first [REDACTED] relevant questions are each supported by a section of the polygraph assessment booklet containing sub-questions exploring various aspects of each issue. Each of the sections allow the examiner to ensure that the subject has disclosed any specific information related to the final version of the question.
  31. The [REDACTED] relevant question is known as a [REDACTED] question, meaning that it is used, in part, to introduce the relevant issues on the exam, and to “absorb” any initial physiological response, such as surprise, a subject may have to the other relevant issues on the exam. This question is [REDACTED] in that it is not scored for deception as are the other [REDACTED] relevant questions.<sup>17</sup>
  32. CSE has chosen comparison questions related to forthrightness and honesty, self-discipline and rule-following, and commitment and personal loyalty. Responses to the comparison questions are not scored for truthfulness but rather are only used to compare physiological responses to the relevant questions.<sup>18</sup> During the period under review, CSE used the following [REDACTED] comparison questions:

- 
33. A polygraph exam can have four possible outcomes: no deception indicated (NDI), deception indicated (DI), inconclusive or incomplete. An assessment of NDI is achieved when the subject’s physiological responses to one or more relevant questions are measurably lower than their responses to the associated comparison question. An assessment of DI is achieved when the subject’s physiological responses to one or more relevant questions are higher than the associated comparison question. An inconclusive result is achieved when the examiner is unable to make a determination one way or the other. An incomplete result is achieved should the examiner determine that the polygraph is malfunctioning or the test is terminated prior to completion for other reasons.

---

<sup>17</sup> *Ibid.*

<sup>18</sup> Krapohl, D.J. and Shaw, P.K. (2015). *Fundamentals of Polygraph Practice*. Elsevier, Inc.

### 3. Findings, Analysis, and Recommendations

---

#### Privacy implications

**Finding 1.** NSIRA found that CSE's governance of the use of the polygraph for security screening inadequately addresses privacy issues.

34. The Treasury Board Standard on Security Screening (the Standard) requires that "the collection, use, disclosure, retention and disposal of personal information for the purpose of security screening is done in accordance with the *Privacy Act* and other applicable legislation, policies and directives."<sup>19</sup>
35. CSE's internal policy governing the use of the polygraph states that "CSE implements and manages its polygraph program in compliance with the... *Privacy Act*, and other relevant legislation and existing government policies..."
36. However, in practice, CSE's use of the polygraph for security screening falls short of these requirements. This insufficient governance is demonstrated through the following four findings.

**Finding 2.** NSIRA found that CSE did not conduct a Privacy Impact Assessment related to its use of the polygraph for security screening.

37. The 2010 Treasury Board Directive on Privacy Impact Assessment (PIA Directive), issued pursuant to the *Privacy Act*, requires a government organization to conduct a Privacy Impact Assessment (PIA) for any new or substantially modified program or activity involving the creation, collection and handling of personal information.<sup>20</sup>
38. The purpose of a PIA is to identify, assess and resolve the privacy implications of government programs involving personal information. It is designed to aid in meeting the GC commitment to ensure "that privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information."<sup>21</sup>

---

<sup>19</sup> Treasury Board of Canada. 2014. Standard on Security Screening, section 5.2.3.

<sup>20</sup> Treasury Board of Canada. 2010. *Directive on Privacy Impact Assessment*, para. 5.1.1.

<sup>21</sup> *Ibid.*, para. 3.1.



SECRET//CEO

39. CSE's polygraph policy states that the program is operated in accordance with relevant legislation, such as the *Privacy Act*, as well as existing government policies, which include the PIA Directive.
40. Despite the implementation of the PIA Directive in 2010 and continuing throughout the period under review, CSE did not complete a PIA. As of October 2021, analysis work for one had started with an anticipated completion date in March 2023. However, as of April 2023, CSE indicated that "upon further analysis, [CSE's] Privacy Policy and Governance Office has determined that a more thorough PIA is required." CSE was unable to provide an expected completion date for this more thorough PIA.

---

**Finding 3.** NSIRA found that CSE may not have considered whether all information collected during the polygraph is directly related or necessary to the assessment of loyalty to Canada or criminality, as required by the *Privacy Act* and the Directive on Privacy Practices.

**Finding 4.** NSIRA found that polygraph examiners applied an *ad hoc* approach as they assessed medical information collected during the polygraph.

---

41. Information collected during security screening, and, in particular, via the polygraph exam, is personal information and its collection is subject to the protections and restrictions set out in the *Privacy Act*.
42. The *Privacy Act* defines personal information as identifiable information about an individual, which can include any information about, for example, the individual's race, religion, or marital status, their medical, employment, or criminal history, or their personal opinions or views.<sup>22</sup>
43. Section 4 of the *Privacy Act* requires that personal information collected by a government institution relate directly to an operating program or activity of the institution.<sup>23</sup> This has been interpreted by the Federal Court as "establishing a direct, immediate relationship with no intermediary between the information collected and the operating program or activities of the government."<sup>24</sup> Based on

---

<sup>22</sup> *Privacy Act*, R.S.C., 1985, c. P-21, s. 3.

<sup>23</sup> *Ibid.*, s. 4.

<sup>24</sup> *Union of Canadian Correctional Officers – Syndicat des Agents Correctionnels du Canada – CSN (UCCO-SACC-CSN) v. Canada (Attorney General)*, 2016 FC 1289 (UCCO) at para. 141.



SECRET//CEO

- the Standard, the activity in question is the assessment of criminality and/or loyalty to Canada.<sup>25</sup>
44. The Treasury Board Directive on Privacy Practices requires that government limit “the collection of personal information to what is directly related to and demonstrably necessary for the government institution’s programs or activities.”<sup>26</sup> In that regard, this Directive is even more restrictive than the *Privacy Act*, as it adds the requirement that personal information be demonstrably necessary for the security screening program or activity.
  45. Under the Standard, the purpose of security screening as a program is to assess an individual’s “loyalty to Canada, and their reliability as it relates to loyalty.” Reliability status “appraises an individual’s honesty and whether he or she can be trusted to protect the employer’s interests.”<sup>27</sup> This is understood to include elements of an individual’s honesty, trustworthiness and personal integrity. Reliability status (including enhanced reliability status) is assessed via screening activities such as, for example, financial inquiries (credit check), law enforcement inquiries (criminal record and law enforcement record checks), a security questionnaire and/or security interview and open source inquiries.<sup>28</sup>
  46. The Standard reserves the use of the polygraph to the highest level of security clearance (ETS).<sup>29</sup> According to the Standard, the purpose of information collected during the polygraph is limited to an assessment of “criminality and/or loyalty to Canada”, not reliability.<sup>30</sup> This distinction is important as the Standard identifies specific screening activities for specific purposes in order to ensure that the invasiveness of these activities is balanced against the level of security screening required.
  47. However, CSE collects detailed personal information during the polygraph that may not be directly related to or necessary for the assessment of criminality and/or loyalty to Canada. One example is the collection of personal medical information. As part of the pre-polygraph interview, CSE collects detailed information related to a subject’s medical history. CSE collects this information to determine if there are any pre-existing medical issues of a physical, psychological or pharmacological nature that could impact the quality of the physiological readings required by the

---

<sup>25</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, Appendix B, section 7.

<sup>26</sup> Treasury Board of Canada. 2014 (updated in 2022). *Directive on Privacy Practices*, section 6.2.9.

<sup>27</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, Appendix A.

<sup>28</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, Appendix B, section 1.

<sup>29</sup> *Ibid.*

<sup>30</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, Appendix B, section 7.

SECRET//CEO

examiner. According to CSE, the collection of this information is limited only to what is necessary to determine the suitability of subjects to undergo a polygraph exam at that moment.

48. Medical information collected by CSE ranges from general, and relatively non-intrusive questions such as "how do you feel today" and "how much sleep did you get last night" to the more intrusive "have you ever consulted with a psychologist, psychiatrist or counsellor for any reason?" and "if not, have you ever felt the need to consult one but didn't?" Of note, some subjects provided information about spousal or other family members' interactions with mental health professionals in response to these questions. Other medical information collected includes a history of hospitalizations and medical check-ups for any reason, use of medications, both prescribed and over-the-counter, how a subject deals with stress, and alcohol, smoking and drug use (both recreational and illegal). CSE did not demonstrate how this medical information is directly related to, nor necessary for, an assessment of loyalty or criminality.
49. In addition to the collection of this information, NSIRA observed a range of outcomes based on information collected by the pre-polygraph medical questionnaire. CSE polygraph examiners are trained by the Canadian Police College, which focuses on the operation of the polygraph and interviewing techniques, and includes basic instruction on physiology and anatomy. They are not medical professionals and are not qualified to assess the nature and significance of the medical and health information they collect during a polygraph exam.
50. Furthermore, CSE has neither standards nor guidelines for what constitutes medical suitability to take a polygraph exam. Polygraph examiners applied an *ad hoc* approach as they collected and assessed medical information in the pre-polygraph interview. Other than in the event that a subject was pregnant, in which case the exam would be rescheduled, the assessment of medical information was entirely at the polygraph examiner's discretion.
51. In some situations, the polygraph examiner determined that a lack of sleep sufficiently impacted a subject's suitability to undergo the exam on that day. Generally, this resulted in a decision to reschedule the exam for a later date when the issue was less likely to impact the polygraph exam. Despite the fact that this information was disclosed at the outset of the exam, CSE polygraph examiners chose to conduct the remainder of the pre-polygraph interview. This included the collection of personal information, with the knowledge that the subject may not have been suitable to take a polygraph exam at that time.



SECRET//CEO

52. In other situations, the polygraph examiner decided to attempt to administer an exam even when the subject disclosed information related to diagnosed medical or neurological conditions. Despite the disclosure of this specific medical information, and without any consultation with qualified medical personnel, CSE polygraph examiners chose to proceed with the exam from beginning to end. In several instances, this resulted in an incomplete or inconclusive result on the exam and required subsequent exams before a clearance decision could be made.
53. Another example of CSE collecting personal information not directly related to the assessment of criminality and/or loyalty to Canada were the comparison questions on the polygraph exam, which are very broad and cover a subject's entire life.<sup>31</sup> The section of the pre-polygraph interview focused on developing the comparison questions is introduced to the subject via a preamble, which states:

Recognizing that there cannot be loyalty without full personal and professional integrity, the issue of integrity is obviously another important aspect when assessing the loyalty of anyone who has expressed an interest in / or is currently working at CSE. When one thinks of a person with integrity, what comes to mind is the picture of someone who carries a basket of desirable qualities that are highly appreciated and sought by employers; CSE is not [*sic*] exception. That said, given CSE's nature and mandates, some items in this basket are of primary importance. It is important for you (the applicant/employee) that you do not put in any filters. Be open about what comes to mind and tell me about them.
54. CSE does not inform subjects of the difference in purpose between the relevant and comparison questions. Instead, the polygraph examiner instructs subjects to respond truthfully to all questions during the exam as if they were all equally relevant to the assessment of criminality and/or loyalty to Canada.
55. CSE attempts to link the comparison questions to the central issue of loyalty to Canada as described in this preamble. However, CSE collects this very broad personal information in order to elicit physiological responses, to compare to the physiological responses to the relevant questions. Based on the functioning of the [REDACTED] polygraph format, CSE does not assess the truthfulness of the responses to the comparison questions. The scoring of the polygraph is based only on the responses to the relevant questions.
56. Due to the breadth of the comparison questions and the expectation that subjects provide even irrelevant information during the polygraph exam to achieve an NDI outcome, CSE risked collecting personal information during the polygraph not directly related to or necessary for CSE's assessment of criminality and/or loyalty to Canada. Individual responses to the comparison questions often included

---

<sup>31</sup> See para. 26 for the specific comparison questions used by CSE during the period under review.

SECRET//CEO

information such as academic dishonesty, instances of petty childhood theft, minor motor vehicle infractions, infidelity in relationships and other personal disloyalty such as lying to family, friends and/or colleagues.

57. Additionally, some CSE employees expressed to NSIRA, both directly and indirectly, that they considered the polygraph process to be traumatic. For example, during an April 2022 meeting with NSIRA, the union representing a majority of CSE employees indicated that some of their members had expressed concern at NSIRA's access to the personal and, at times, traumatic information they had disclosed during polygraph exams. Furthermore, during internal town hall meetings with CSE Management in May and June 2022, CSE employees expressed similar concern at the nature and degree of personal information disclosed during polygraph exams.<sup>32</sup>
58. Subjects are frequently advised and reminded during a polygraph exam that withholding any information during the exam could negatively impact their security clearance. They are advised to disclose anything that may come to mind at any point during any stage of the exam to the polygraph examiner who will determine if the information is relevant to the exam or not. While NSIRA observed situations in which subjects felt compelled to share personal information not relevant to an assessment of their loyalty, CSE's methodology also risks the collection of irrelevant and potentially traumatic personal information, causing unnecessary mental distress for subjects.
59. When asked to comment on the factual accuracy of a draft of this report, CSE stated that the collection of personal information via the polygraph, such as in the examples above, is authorized because the purpose of the overall security screening program is to make decisions on granting or denying any level of security status (Reliability or Enhanced Reliability) or clearance (Secret or Top Secret) based on an assessment of "loyalty to Canada and reliability as it relates to loyalty." However, this interpretation is overly broad because the program of security screening is comprised of multiple distinct activities carried out for various purposes. The Standard differentiates between assessments for reliability status and an ETS security clearance. Moreover, the comparison questions, which include qualifiers such as "in any way in your entire life," are so broad that they can result in the collection of information that is not directly linked even to an assessment of reliability under the Standard.

---

<sup>32</sup> In anticipation of these concerns, NSIRA proposed to CSE measures to de-identify and anonymize a subject's personal information, which were implemented as described in para 8.



**Finding 5.** NSIRA found that CSE may not have complied with section 7 of the *Privacy Act* by using information collected during polygraph exams for suitability and hiring decisions without the consent of the subject.

60. Section 7 of the *Privacy Act* prohibits the use of personal information collected without the consent of the individual to whom it relates, except “for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose.”<sup>33</sup> For use of personal information to be consistent, an individual should “reasonably expect that the information could be used in the manner proposed.”<sup>34</sup>
61. Information from the CSE website available at the time of application for employment distinguishes between the security clearance process and the Human Resources (HR) hiring process, known within CSE as a “global assessment”, which focuses on a candidate’s suitability to work at CSE, rather than loyalty to Canada or criminality. CSE’s website further sets out that the polygraph will be conducted as part of the security clearance process only.<sup>35</sup> CSE also conveyed the separation of the security assessment from the suitability assessment in briefings and other documentation provided to NSIRA. According to the Standard, the collection of personal information must be conducted with the informed consent of individuals.<sup>36</sup> Furthermore, the Standard does not provide for the use of information collected during security screening activities for suitability assessment purposes.
62. During the period under review, CSE obtained consent at the outset of each polygraph examination through a consent form. According to this form, the use of information collected was limited to the purpose of conducting the security assessment or for other internal security-related activities, such as security investigations and the re-assessment of security clearance or site access permissions.
63. Based on the above, a subject would not reasonably expect that information collected during the polygraph examination could be used in suitability and hiring decisions.

---

<sup>33</sup> *Privacy Act*, R.S.C., 1985, c. P-21, s. 7.

<sup>34</sup> *Bernard v. Canada (Attorney General)* [2014] 1 S.C.R. 227 at para. 31.

<sup>35</sup> CSE Website. 2022, accessed September 26, 2023. *Hiring process and security*. [www.cse-cst.gc.ca/en/careers/hiring-process-and-security](http://www.cse-cst.gc.ca/en/careers/hiring-process-and-security).

<sup>36</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, section 3.

SECRET//CEO

64. However, NSIRA observed multiple examples where CSE used information collected during a polygraph exam in the HR suitability process, when, in the opinion of the polygraph examiner, that information related to a subject's suitability to work at CSE. This information did not result in a decision to deny the security clearance.
65. CSE's assessment of suitability is the responsibility of HR and is supposed to be separate from the security assessment. CSE's suitability assessment includes interviews, reference checks and the psychological assessment. CSE assesses suitability based on seven values found in the CSE ethics charter: lawfulness, integrity, innovation, agility, sustainability, collaboration and dependability.
66. As part of the hiring process, CSE can refer specific files to a Suitability Assessment Panel (SAP). This panel is "responsible for the review of individual cases... which have been identified as requiring further consideration." A SAP is comprised of the Director, HR Recruitment, and representatives from Psychological Services, Labour Relations and Staffing and Recruitment. It also includes a representative from Personnel Security. Earlier versions of the SAP, which were known as Hiring Panels, included the team leader, Polygraph Services, or their delegate directly.
67. NSIRA reviewed files where a polygraph examiner included a recommendation in their final report to not hire a subject or to refer the file to a SAP based on risk identified during the polygraph exam, such as a DI or inconclusive assessment, or other information relevant to HR's suitability assessment. Additionally, records of decisions of SAPs provided by CSE included examples where information collected during the polygraph, such as a DI or inconclusive assessment, featured in SAP decision-making.
68. A SAP can result in the decision to continue or not with a candidate's application. If a SAP decides to not continue with a candidate's application, CSE provides a letter of regret explaining that CSE conducted a "Global Assessment Process" designed to determine the overall suitability of candidates to work for CSE. It also states that the decision to not proceed with a candidate's application may "be based on other elements involved in the CSE hiring decision, such as changes in skill requirements, budgetary constraints or the identification of more suitable candidates." There is no reference in the letter to the consideration of issues related to the polygraph or security clearance process in CSE's "global assessment."



**Finding 6.** NSIRA found that CSE provides subjects with information that overstates the reliability and validity of the polygraph prior to obtaining consent.

69. The Standard requires that security screening activities, including the polygraph, are conducted with the informed consent of individuals.<sup>37</sup> Among the factors that could help establish that consent was fully informed, an individual should reasonably understand the facts about the screening activity to which they are consenting. As it relates to the polygraph, this should include a balanced assessment of its validity, reliability and effectiveness.
70. CSE advised candidates and employees to refrain from conducting any personal research in order to avoid misleading or inaccurate information about the polygraph. This is also designed to mitigate against the risk that subjects will utilize known or potential countermeasures to defeat the polygraph. However, in practice it prevents individuals from being fully informed about the risks associated with the polygraph prior to consenting to undergo the exam.
71. At the outset of a polygraph exam, CSE provides the subject with information about the polygraph in the form of a frequently asked questions (FAQ) document. In it, CSE addresses issues of accuracy and the potential for false positives by stating that “the polygraph examination procedure has proven through research to be a highly reliable and accurate means to assess truthfulness,” but does not address any contrary research or the general lack of scientific consensus regarding the reliability of the polygraph. When subjects asked additional questions during an exam, examiner responses tended to be cursory, repeated the information provided in the booklet and FAQ document and discounted any information critical of the polygraph.
72. CSE chose to provide subjects only with information that supports the reliability, validity and efficacy of the polygraph rather than a balanced and factual assessment of it. To claim, as does CSE, that “a polygraph examination is a scientific, objective means of assessing veracity or truthfulness” is not factually accurate and risks being misleading. For consent to be appropriately informed, factually accurate information related to the validity and reliability of the polygraph is required.
73. When asked to comment on the factual accuracy of a draft of this report CSE stated that:

---

<sup>37</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, sections 3.2 and 5.

SECRET//CEO

Individuals do not provide their consent for the direct collection of personal information during any step of the security screening process, as this is neither required under the *Privacy Act* nor an appropriate mechanism for the direct collection of personal information in the public sector. Consent, even if informed, is unlikely to be meaningful in any state-individual interaction involving the direct collection of personal information given the significant power disparity between the parties and the lack of other meaningful options for the individual.

## Polygraph operations

**Finding 7.** NSIRA found that, in some instances, the way in which CSE conducted polygraph exams risked prompting subjects to fabricate information in an effort to clear themselves when faced with an unfavourable polygraph assessment.

74. In several instances, NSIRA observed that when a polygraph examiner's initial assessment indicated that a subject was being deceptive when responding to one or more of the exam questions, or the results were trending towards an inconclusive result, there was a marked change in the demeanour and style of the polygraph examiner. Interviews which started in a friendly and genial manner often turned aggressive and adversarial in the face of potentially negative results. This change in tone was, at times, accompanied by veiled or even overt threats that any deception by the subject would negatively affect their ability to obtain or maintain the required level of security clearance. There is a risk that this change is based solely on the examiner's interpretation of the results and not necessarily on any specific information provided by a subject which raises doubt about their loyalty to Canada.
75. Subjects often appeared to be fearful or agitated by this change in tone. Some subjects indicated that the change in the examiner's demeanour had caused an increase in their stress level. Other subjects expressed a lack of understanding at the initial polygraph result because, according to them, they had been fully forthcoming and truthful to the best of their ability.
76. An initial assessment indicating potential deception, even if related to one of the comparison questions, resulted in further questioning by the examiner to uncover any new information which may have caused the subject to react physiologically to a specific question, or questions. The implication was that the physiological responses indicated deception or were evidence that the subject was withholding some information which was affecting the polygraph readings. In some instances, this questioning became repetitive and aggressive if no new information was disclosed.



SECRET//CEO

77. At times, this type of repetitive and aggressive questioning placed subjects in a position where the onus was on them to volunteer new information or explanations for the polygraph readings. Furthermore, when asked for additional explanations, subjects continually searched their memory for new examples. Many subjects disclosed unnecessary and irrelevant information, including highly personal details of their private lives in order to respond to the polygraph examiner's questioning.
78. When faced with repeated questions about their alleged dishonesty, based on an initial and unscientific assessment by an examiner, subjects who initially claimed to have been fully forthcoming eventually disclosed information about which they appeared to be uncertain, but provided it to satisfy the examiner. In some circumstances, subjects volunteered "possible" examples or things that might have happened, such as possible information handling errors, as opposed to definitive memories or specific events from their past. However, polygraph examiners often appeared to accept these responses as factual disclosures supporting their initial assessment.
79. Subjects are told that the polygraph can accurately detect deception. In the face of a deceptive or inconclusive result and when paired with an aggressive or confrontational style of questioning, NSIRA observed subjects who, when prompted by the polygraph examiner to satisfy any doubt raised by the polygraph readings, may have been pressured to explain negative polygraph readings with answers that appeared hypothetical or speculative. This information, whether accurate or not, could then be used against the subject in future polygraph exams, the wider security clearance process or other internal security investigations.

---

**Finding 8.** NSIRA found instances where CSE's quality control practices for polygraph exams were not always consistent with CSE policy.

---

80. CSE's internal policy governing polygraph operations was initially issued in January 2006 and was last amended in December 2013. It requires that "all polygraph tests will be reviewed [for quality control] by the Supervisor, Polygraph Assessment Services, or a senior Polygraphist. In addition, a random sample of all polygraph tests will be subject to the quality-control process of an external accredited polygraph specialist."
81. During the period under review, CSE's quality control practices were not compliant with CSE policy. CSE did not conduct quality control on "all polygraph tests". Of the files included in NSIRA's sample, documentation provided by CSE could only confirm that quality control had been completed for just over half of the exams conducted. CSE explained that despite its own policy, CSE's practice was to reserve quality control for the last exam performed on a file. However, NSIRA

SECRET//CEO

reviewed multiple files which contained no quality control, including for the last exam on file.

82. Quality control was documented on separate scoring sheets which contained the quality controller's independent scoring of the physiological measurements taken during the exam.<sup>38</sup> The quality control sheets included space for the quality controller to sign and indicate the date on which it was completed. The sheets were then placed on file with the original polygraph examiner's score sheet for reference. According to a statement of work outlining expectations for quality control, it was to be conducted within five working days following a polygraph exam. However, of the files reviewed by NSIRA, seldom were quality control sheets signed or dated by the quality controller. This made it impossible to determine who conducted the check or even when it was completed.

---

**Finding 9.** NSIRA found that approximately 20% of security files from the sample reviewed were missing audiovisual recordings of polygraph exams.

---

83. As previously mentioned, NSIRA selected a sample of polygraph exams for more detailed review. This sample was comprised of 95 individual polygraph exams conducted for the 51 security screening files selected. Of the 95 exams, NSIRA found that 21 were either missing audio or video content, or both. This amounts to just over 20% of polygraph exams which were not retained by CSE, contrary to GC retention requirements.
84. CSE attributed the missing or corrupted content to the use of the innate recording functionality contained in the polygraph system. This system's primary task is to read and record the physiological readings, not to record the exams for retention purposes. However, at least during the period under review, CSE was using the polygraph system to do both. CSE indicated that "it is possible that the system is not sufficiently robust to perform multiple tasks simultaneously, leading to occasional failures to record audio/visual."

---

<sup>38</sup> According to CSE, quality control was conducted on the physiological measurements alone and without access to the original polygraph recordings or polygraph examiner's notes.



## Security screening decision-making

**Finding 10.** NSIRA found that in all cases, when initial polygraph exam results indicated deception or were inconclusive, CSE's practice was to conduct multiple polygraph exams rather than a resolution of doubt process as provided for under the Standard.

85. Security screening activities may uncover possible adverse information about a subject which may raise doubt as to their loyalty to Canada and/or reliability, as it relates to loyalty. The Standard outlines that adverse information, "is to be used as the basis for further investigation, including a security interview"<sup>39</sup> and states that such an interview can be used "as a means to resolve doubt or to address adverse information that is uncovered during security screening."<sup>40</sup>
86. The Standard also requires that any adverse information, unless subject to an exemption, be presented to the individual in writing and that they be provided with an opportunity to address the information resulting in doubt.<sup>41</sup> To do this, organizations are entitled to conduct multiple security interviews to resolve the doubt, or to make a decision to deny the clearance, if the doubt is substantiated and sufficient. The Standard does not provide for the use of multiple polygraph exams to resolve doubt.
87. In practice, CSE often treated a DI or inconclusive result on a polygraph as adverse information in its own right. These results sometimes were accompanied with specific disclosures made by a subject during an exam which may have accounted for the DI or inconclusive result. However, in many cases, polygraph exams resulted in a DI or inconclusive assessment absent any specific disclosures by the subject.
88. When adverse information arose prior to a polygraph exam, such as during credit or criminal records checks, CSE conducted subsequent security interviews to address any adverse information. However, once a file progressed to the polygraph stage, CSE conducted multiple polygraph exams, rather than security interviews, as the primary means to resolve doubt.
89. This approach requires subjects to undergo a highly intrusive polygraph on more than one occasion, rather than focusing the follow-up on the specific adverse

---

<sup>39</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, appendix D, section 6.

<sup>40</sup> *Ibid.*, appendix D, section 8.

<sup>41</sup> *Ibid.*, appendix D, section 7.

SECRET//CEO

information of concern, if any. CSE does not resolve a DI or inconclusive polygraph result with a security interview as provided for in the Standard, but rather conducts one or more follow-up polygraphs until the subject achieves an NDI result, withdraws, or is removed from consideration.

**Finding 11.** NSIRA found that the polygraph had an inordinate importance in security screening decision-making at CSE and other less-intrusive security screening activities were under-used or not used at all.

90. Although this review did not explore the entirety of CSE's security screening regime, NSIRA did have access to security screening files associated with polygraph exams selected as part of the sample for this review. These files included records of the results of the other security screening activities conducted by CSE. NSIRA reviewed these files to the extent that they informed or may have influenced the conduct of polygraph examinations.
91. The Standard outlines several specific screening activities that are to be conducted for each level of security clearance. For an ETS security clearance, these include the verification of identity and background information; educational and professional credentials and personal and professional references; a financial inquiry (credit check); law enforcement inquiries (criminal record checks and Law Enforcement Records Checks (LERC)); a security questionnaire and/or security interview(s); an open source inquiry; a CSIS security assessment; and a polygraph examination.<sup>42</sup>
92. Taken as a whole, the information collected through these activities should provide the deputy head of the organization granting the clearance a reasonable assurance as to the subject's loyalty to Canada, and their reliability, as it relates to loyalty. According to the Standard, "adverse information obtained pursuant to a CSIS security assessment is the primary determinant of whether a security clearance... can be granted."<sup>43</sup> Otherwise, "decisions about a subject's security status or clearance are based on information gathered during the security screening process."<sup>44</sup> Furthermore, a decision made on a security clearance "must be based on an adequate amount of verifiable information to ensure that it is fair, objective and defensible."<sup>45</sup> This was also a requirement of the 2005 MD for CSE.

---

<sup>42</sup> *Ibid.*, appendix B, section 7.

<sup>43</sup> *Ibid.*, appendix D, section 7.

<sup>44</sup> *Ibid.*, appendix D, section 1.

<sup>45</sup> *Ibid.*



SECRET//CEO

93. CSE conducted no LERCs during the period under review. It only started conducting LERCs in 2022 following the establishment of a Memorandum of Understanding with the RCMP but provided no explanation for the eight year delay in setting up the agreement.
94. CSE's open source checks were cursory, and primarily consisted of the results of basic search engine queries and surface-level review of known social media accounts. Often the results of open source inquiries documented on file were limited to screen captures of relevant information with no detailed notes or assessment recorded in the security files.
95. CSE has developed a dedicated security interview questionnaire which is used to conduct the security interview. Questions of security relevance, including those related to the topics which will eventually appear as one of the relevant questions on the polygraph exam – espionage, support for radical or extremist ideology and information handling practices – are often dealt with at various places throughout the security interview. However, these topics are not explored in as much depth or detail during the security interview as they are during the polygraph exam.
96. CSE asserted that subjects disclose new information during the polygraph that is not disclosed during earlier stages of security screening, such as the security interview. However, the pre-polygraph interview is shorter than the security interview and more focused on CSE's specific security concerns. This allows the polygraph examiner to probe the subject's responses in more detail, and to collect more information. The length and breadth of the security interview restricts CSE's ability to collect sufficient information in an efficient manner.
97. The polygraph takes place at the end of the security screening process. Insufficiently using other less intrusive security screening activities, or not using them at all places an inordinate importance on the polygraph. This renders the polygraph as the gatekeeper of security screening decision-making at CSE, rather than as one screening activity amongst many, as it expected under the Standard.

---

**Finding 12.** NSIRA found that the polygraph was *de facto* determinative in security screening decisions at CSE.

---

98. The 2005 MD respecting the use of the polygraph at CSE, which was in effect for part of the period under review, required that "the polygraph may be used only as an investigative tool (i.e. there is no pass/fail applicable to polygraph results)" and that "results shall not be used as the sole determinant in the security screening or selection process." Polygraph best practice also supports that the polygraph is only

SECRET//CEO

effective when used as an investigative tool reinforced by other sources of information and analysis.<sup>46</sup>

99. Although the Standard is silent about the weight of the polygraph in security screening decision-making, it does require that “all decisions must be made on the basis of the quality, quantity, relevance and credibility of information and intelligence.”<sup>47</sup> It does not require that a subject “pass” a polygraph in order to obtain an ETS security clearance.
100. In practice, CSE required that subjects must pass a polygraph, which equates to achieving an NDI assessment. Polygraph examiners were often noted referring to passing or failing a polygraph during polygraph exams.
101. With the exception of a small number of exams where medical issues, such as physical or mobility restrictions, prevented the collection of accurate physiological measurements, there were no examples during the period under review where CSE decided to grant a security clearance without an NDI assessment from a polygraph exam.

---

**Finding 13.** NSIRA found that CSE’s security screening decision-making may not comply with record-keeping requirements of the Standard on Security Screening.

---

102. The Standard requires that decision-making be supported by “an assessment from the official or organization responsible for conducting the security screening.”<sup>48</sup> It also requires that “all information considered in rendering a decision, along with any follow-up action and the decision itself, must be recorded in the individual’s security screening file.”<sup>49</sup>
103. A CSE personnel security officer (PSO) conducts an assessment of the information collected prior to the polygraph and summarizes their initial findings prior to referring the file to the polygraph unit. Following the polygraph exam, the polygraph examiner produces a polygraph report which is included in the subject’s security screening file.
104. While CSE produces separate reports following both the security interview and the polygraph exam, NSIRA found no final report or assessment in either the security screening file or in CSE’s case management system that outlined a balanced

---

<sup>46</sup> Krapohl, D.J. and Shaw, P.K. (2015). *Fundamentals of Polygraph Practice*. Elsevier, Inc.

<sup>47</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, appendix D, section 9.

<sup>48</sup> *Ibid.*, appendix D, section 10.

<sup>49</sup> *Ibid.*, appendix D, section 1.



assessment of all the security screening activities, including a recommendation and related rationale for the final security screening result.

---

**Finding 14.** NSIRA found that CSE's use of the polygraph in security screening decisions makes more uncertain the opportunity to challenge denials of security clearances pursuant to the NSIRA Act and the Standard.

---

105. Section 18 of the NSIRA Act provides individuals a right to recourse "if, by reason only of the denial of a security clearance required by the Government of Canada, a decision is made by a deputy head to deny employment to an individual or to dismiss, demote or transfer and individual or to deny a promotion or transfer to an individual."
106. However, the Chief of CSE, who is the deputy head, has never denied a security clearance, either during or outside the period under review. When coupled with CSE's practice of considering potentially adverse security information during the HR suitability assessment as discussed in finding 5, this amounted to a denial of the right of recourse granted to individuals by the NSIRA Act. Because no security clearances are ever denied, and adverse information is instead dealt with through the HR suitability assessment process, applicants are not informed of their right to challenge a decision. Therefore, individuals may be prevented from accessing this important recourse mechanism.<sup>50</sup>

## Treasury Board Standard on Security Screening

---

**Finding 15.** NSIRA found that TBS did not adequately consider privacy or Charter implications when it included the polygraph as a security screening activity under the Standard on Security Screening.

---

107. The Treasury Board's decision to include the polygraph in the Standard, and to expand its application to any department or agency with requirements for ETS security clearances was a significant departure from past security screening practice in the GC. Prior to 2014, the polygraph was only in use for security

---

<sup>50</sup> NSIRA's practice in complaint investigations is to examine closely the record in order to determine the actual basis for a decision and whether it has jurisdiction in cases where a security clearance decision is appealed to the Agency.

SECRET//CEO

screening at select security and intelligence agencies, such as CSE and CSIS.<sup>51</sup> According to TBS, the addition of the polygraph to the Standard was, in part, designed to enhance the GC's ability to appropriately assess the loyalty of employees requiring access to the Government's most sensitive information, assets and facilities.

108. TBS did not conduct a PIA related to the inclusion of the polygraph in the Standard. According to TBS, "at the time the Standard was approved, there was no requirement to conduct a... PIA on a policy instrument." However, following the implementation of the Standard, TBS did conduct a "Privacy Assessment" related to the conduct of security screening as outlined in the Standard. This assessment acknowledged that the polygraph collects personal information and noted that polygraph examinations are "administered by qualified personnel, and according to recognized and documented standards designed to protect the individual's legal rights under the [Charter]." However, this assessment did not address any specific privacy implications or the operational realities specific to the polygraph, such as those outlined above. Nor did it describe any of the "recognized and documented standards" that were allegedly designed to protect individual privacy rights.
109. The Standard was endorsed by Deputy Heads at a May 2, 2014 Public Service Management Accountability Committee (PSMAC). The presentation provided to PSMAC indicated that TBS had considered privacy issues related to the polygraph, in part, by consulting a PIA conducted by the RCMP in 2005. That PIA was related to the RCMP's use of the polygraph in its Pre-employment Polygraph Testing Initiative.
110. TBS was unable to provide a copy of the RCMP's PIA to NSIRA and upon further inquiry by NSIRA, had no record of the full PIA having actually been shared by the RCMP. TBS could only confirm that it had consulted an executive summary of this PIA. This executive summary provides only background information about the PIA and does not provide any detail as to the actual impact assessment or any of the detailed considerations made by RCMP.<sup>52</sup> Furthermore, it should be noted that the 2005 RCMP PIA was specific to the RCMP's use of the polygraph as a pre-employment screening tool to assess suitability for employment, not as a security screening activity to assess loyalty to Canada, which is the purpose of the

---

<sup>51</sup> NSIRA was not able to determine conclusively if any other department or agency was using the polygraph exam for security screening prior to 2014, as TBS does not maintain statistics on ETS security clearance requirements for the GC.

<sup>52</sup> RCMP. 2005, accessed 2023 (Oct). *Pre-employment polygraph (PEP) testing initiative*. <https://www.rcmp-grc.gc.ca/en/pre-employment-polygraph-pep-testing-initiative>.



SECRET//CEO

polygraph under the Standard. As such, endorsement of the Standard by PSMAC appears to have been based on incomplete, inaccurate and even misleading information.

111. TBS affirmed that while it was developing the Standard, it conducted "broad community consultations... with interdepartmental working groups representing large, medium and small departments..." However, TBS was unable to provide evidence demonstrating that the polygraph featured in any of these consultations.
112. One exception was a disposition log for a draft version of the Standard which included specific comments made by departments/agencies consulted by TBS. The majority of input provided by departments in this log was unrelated to the polygraph. However, input provided by CSE was notable in that it recommended that pre-employment polygraph testing:
  - ... should not become a part of the clearance process per se because this would place this testing under the review of redress entities such as SIRC. It is preferable that... [the] polygraph remain under special suitability testing reserved for sensitive police and security positions...
113. TBS did not conduct an independent assessment of the effectiveness and reliability of the polygraph, the science underpinning it, or consider any alternatives. TBS stated that it consulted "publicly available literature" regarding the reliability and validity of the polygraph, but provided no specific examples. TBS also stated that it relied on "engagement with experts in departments and agencies that used polygraph examinations." Similarly, TBS did not provide any examples of this engagement, or information considered during these consultations.
114. TBS considered the privacy and Charter implications of conducting security screening. However, legal advice provided to TBS during the development of the Standard did not address any issues specific or unique to the polygraph. When asked to comment on the factual accuracy of a draft of this report, TBS stated that "the absence of a formal legal opinion does not equate to a policy or program being in violation of legal instruments, nor does it constitute lack of due diligence for legal and privacy concerns; on the contrary, the lack of any legal concerns being raised is a positive indicator."
115. TBS indicated that one of the primary considerations behind including the polygraph in the Standard was a desire to bring the Canadian security screening regime into line with Five Eyes best practices. In support of this consideration, TBS provided NSIRA with a chart comparing the security screening regimes of the United States, United Kingdom, Australia and New Zealand to that in Canada. This chart indicates that the polygraph is used for security screening purposes on an "agency/position specific" basis by all members of the Five Eyes.

116. However, NSIRA consulted available information detailing the security screening regimes of Five Eyes nations. With the sole exception of the United States, which uses the polygraph extensively to conduct security screening, NSIRA could find no information to support the claim that the polygraph is used by any other member of the Five Eyes. In light of this, TBS' stated goal of "bringing Canada into line with Five Eyes security screening best practices" would not have included the use of the polygraph.
117. When asked to comment on the factual accuracy of a draft of this report, TBS indicated that "Five Eyes security screening best practices are to a large extent typified by the practices of the United States [and] the practices of all other nations are generally compared to US practice." However, bringing Canadian security screening practices into line with the United States was never put forward as the prime motivator behind the decision to include the polygraph in the Standard by TBS at any other point during the review.

**Finding 16.** NSIRA found that the Standard on Security Screening insufficiently addresses Charter and privacy implications related to the use of the polygraph.

118. According to the Standard, a polygraph examination is designed to "assess an individual's criminality and/or loyalty to Canada." In order to do this:
- a) Polygraph examinations use questioning techniques and technology to record physiological responses which might indicate deception by the individual;
  - b) Testing questions relate to relevant details of the individual's behaviour collected through other Security verifications, inquiries or assessments; and
  - c) Examinations are administered by qualified personnel according to recognized techniques and written standards that are designed to protect individuals' legal rights and rights under the [Charter].<sup>53</sup>
119. The Standard was designed to regulate security screening across the GC. However, as it relates to the polygraph, the Standard does not indicate whether departments should use single or multiple issue exams or any other procedures or best practices required to conduct a "fair, objective and defensible" assessment as

---

<sup>53</sup> Treasury Board of Canada. 2014. *Standard on Security Screening*, appendix B, section 7.



SECRET//CEO

required by the Standard.<sup>54</sup> Specificity as to type of polygraph equipment departments should use, could further assist in this regard.

120. Furthermore, the Standard provides no direction or guidance on how security officials should consider the results of a polygraph examination when making decisions or recommendations on security screening cases, as is the case for other activities, such as the CSIS Security Assessment.<sup>55</sup> This can result in an over-reliance or determinative application of the results of a polygraph examination, as was found to be the case at CSE.
121. TBS indicated that because “only a very limited number of organizations used the polygraph, and these organizations already had specific protocols in place regarding how the polygraph would be conducted, TBS did not issue additional guidance to support its use.” As demonstrated by this review, the failure to consider more robust standards or guidelines specific to the use of the polygraph contributed to the development of practices that present very serious concerns with Charter and *Privacy Act* compliance.

## Canadian Charter of Rights and Freedoms

**Finding 17.** NSIRA found that the Government of Canada’s current use of the polygraph for security screening in the manner described in this review may raise serious concerns in relation to the *Canadian Charter of Rights and Freedoms*.

122. The central constitutional protection of privacy is found in s. 8 of the Charter, which guarantees that “[e]veryone has the right to be secure against unreasonable search and seizure.” A search or seizure occurs “when a person has a reasonable privacy interest in the object or subject matter of the state action and the information to which it gives access.”
123. Section 8 “seek[s] to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle personal choices of an individual.”<sup>56</sup>

<sup>54</sup> *Ibid.*, appendix D, section 1.

<sup>55</sup> *Ibid.*, appendix D, section 7.

<sup>56</sup> *R. v. Tessling* [2004] 3 S.C.R. 432 (*Tessling*) at para. 25.

SECRET//CEO

124. Section 8 of the Charter is only engaged if subjects have a reasonable expectation of privacy in the particular situation.<sup>57</sup> Furthermore, since “the essence of a seizure under s. 8 is the taking of a thing from a person by a public authority without that person’s consent,”<sup>58</sup> a valid consent may amount to a waiver of one’s rights under s. 8 of the Charter and therefore preclude a Charter violation.<sup>59</sup>

### Reasonable Expectation of Privacy

125. The assessment of whether polygraph subjects have a reasonable expectation of privacy in the information collected via the polygraph is based on the “totality of the circumstances”, a test guided by four questions: 1) the subject matter; 2) whether the subject has a direct interest in the subject matter; 3) whether the subject has a subjective expectation of privacy in the subject matter; and 4) if so, whether that expectation was objectively reasonable.<sup>60</sup>
126. The physiological information collected via the polygraph gives rise to a bodily privacy interest, mostly in the circumstances in which it is collected, such as answers about medical history, lifestyle and personal choices, which give rise to an informational privacy interest. This is information that would be considered to be “biographical core of information” protected by section 8 of the Charter.
127. Providing valid consent for the collection of this information in the context of seeking security screening for employment may diminish or invalidate any subjective expectation of privacy in that information and the objective reasonableness of that expectation. However, for the reasons set out below, the consent obtained from polygraph subjects may not be sufficient to vitiate their reasonable expectation of privacy or exclude the application of section 8 of the Charter to the polygraph.

### Insufficient consent

128. The consent CSE obtains prior to administering a polygraph may not be fully informed or voluntary. As described earlier in this report, information provided to subjects about the polygraph is one-sided in support of the polygraph. CSE provides information largely in favour of the reliability and validity of the polygraph and does not adequately address counter-factual information or any existing

---

<sup>57</sup> *R. v. Cole* 2012 SCC 53, [2012] 3 S.C.R. 34 (*Cole*) at para. 9.

<sup>58</sup> *R. v. Dyment*, [1988] 2 S.C.R. 417, [1988] S.C.J. No. 82, at para. 26.

<sup>59</sup> *R. v. Wills* 7 O.R. (3d) 337 [1992] O.J. No. 294 at para. 86. In *UCCO*, *supra* note 24, fully informed and valid consent to financial inquiries did not preclude a potential Charter violation, but rather was cited by the court as one factor in the reasonableness assessment of the Standard.

<sup>60</sup> *Cole*, *supra* note 57, at paras. 39 and 40.



SECRET//CEO

criticism of the polygraph. As well, subjects are not informed that the comparison questions are designed to trigger physiological responses to help the examiner analyse responses to the security questions, and are instead left with the impression that their answers to those questions will be assessed as part of the determination of criminality or loyalty to Canada.

129. Other factors that could contribute to the validity of consent are also absent. CSE does not inform applicants that information collected during the security assessment can be used during the HR suitability assessment process. In addition, the Standard does not provide that CSE will conduct multiple polygraphs in order to resolve doubt, nor are subjects informed of the requirement for multiple polygraphs on CSE's job application page.
130. As the consent provided may be insufficient, the protections afforded by section 8 of the Charter remain engaged.

### Concerns with the Standard and CSE's implementation of the polygraph

131. The administration of the polygraph must be reasonable in order to comply with section 8 of the Charter. In order to be reasonable, the conduct of the polygraph must be authorized by law; the law itself must be reasonable; and the search must be carried out in a reasonable manner.<sup>61</sup>
132. While there is no "hard and fast" test of reasonableness, it requires a balancing of privacy interests against the public interest served by the statutory scheme.<sup>62</sup> The following considerations are relevant to this assessment: the nature and purpose of the legislative scheme, the mechanism of the search and the degree of its potential intrusiveness, and the availability of judicial supervision.<sup>63</sup>
133. Taking into account these considerations, numerous issues discussed in this report raise concerns about the reasonableness of the Standard as the "law" authorizing the search or seizure and the manner in which CSE has implemented the polygraph. Information collected is over-broad, and can be unrelated to furthering the assessment of criminality or loyalty to Canada. CSE over-relies on the polygraph in security screening decisions, in particular considering the lack of scientific consensus regarding the validity or reliability of the polygraph as a means to detect deception. CSE's practices deny subjects the procedural rights afforded to them in the Standard and the recourse mechanism provided in the NSIRA Act.

---

<sup>61</sup> *R. v. Collins* 1 S.C.R. 265 at para. 23; *Schreiber v. Canada (A.G.)* [1998] 1 S.C.R. 841 at para. 50.

<sup>62</sup> *Reference Re: Marine Transportation Security Regulations* 2009 FCA 234 at para. 49.

<sup>63</sup> *Goodwin v. B.C. (Superintendent of Motor Vehicles)* [2015] 3 S.C.R. at para. 57.

SECRET//CEO

The Standard also provides insufficient guidance regarding the use of the polygraph, and CSE's use of the information collected exceeds both the limited guidance offered by the Standard as well as the consent provided by subjects.

## 4. Conclusion

---

134. The findings contained in this review indicate that CSE's use of the polygraph for security screening, and TBS's authorization of the polygraph as a security screening activity under the Standard raise serious concerns related to the *Privacy Act* as well as the Charter. When taken as a whole, CSE's use of the polygraph as a security screening activity under the TBS Standard is not being conducted in a way that is reasonable or necessary.
135. In light of the preceding findings related to CSE's use of the polygraph for security screening, and the authority to do so provided by the TBS Standard on Security Screening, NSIRA makes the following recommendations:

**Recommendation 1.** NSIRA recommends that the Treasury Board of Canada urgently remedy the issues identified by this review related to the legality, reasonableness and necessity of the use of the polygraph for security screening in Canada, or remove it from the Standard on Security Screening.

**Recommendation 2.** NSIRA recommends that CSE urgently remedy the issues identified by this review, including Charter and *Privacy Act* compliance, or cease conducting polygraph exams for security screening.



## Annex A. Findings and Recommendations

---

NSIRA made the following findings and recommendations in this review:

### Findings

#### Privacy implications

**Finding 1.** NSIRA found that CSE's governance of the use of the polygraph for security screening inadequately addresses privacy issues.

**Finding 2.** NSIRA found that CSE did not conduct a Privacy Impact Assessment related to its use of the polygraph for security screening.

**Finding 3.** NSIRA found that CSE may not have considered whether all information collected during the polygraph is directly related or necessary to the assessment of loyalty to Canada or criminality, as required by the *Privacy Act* and the Directive on Privacy Practices.

**Finding 4.** NSIRA found that polygraph examiners applied an *ad hoc* approach as they assessed medical information collected during the polygraph.

**Finding 5.** NSIRA found that CSE may not have complied with section 7 of the *Privacy Act* by using information collected during polygraph exams for suitability and hiring decisions without the consent of the subject.

**Finding 6.** NSIRA found that CSE provides subjects with information that overstates the reliability and validity of the polygraph prior to obtaining consent.

#### Polygraph operations

**Finding 7.** NSIRA found that, in some instances, the way in which CSE conducted polygraph exams risked prompting subjects to fabricate information in an effort to clear themselves when faced with an unfavourable polygraph assessment.

**Finding 8.** NSIRA found instances where CSE's quality control practices for polygraph exams were not always consistent with CSE policy.

**Finding 9.** NSIRA found that approximately 20% of security files from the sample reviewed were missing audiovisual recordings of polygraph exams.

#### Security screening decision-making

**Finding 10.** NSIRA found that in all cases, when initial polygraph exam results indicated deception or were inconclusive, CSE's practice was to conduct multiple polygraph exams rather than a resolution of doubt process as provided for under the Standard.

SECRET//CEO

**Finding 11.** NSIRA found that the polygraph had an inordinate importance in security screening decision-making at CSE and other less-intrusive security screening activities were under-used or not used at all.

**Finding 12.** NSIRA found that the polygraph was *de facto* determinative in security screening decisions at CSE.

**Finding 13.** NSIRA found that CSE's security screening decision-making may not comply with record-keeping requirements of the Standard on Security Screening.

**Finding 14.** NSIRA found that CSE's use of the polygraph in security screening decisions makes more uncertain the opportunity to challenge denials of security clearances pursuant to the NSIRA Act and the Standard.

### Treasury Board Standard on Security Screening

**Finding 15.** NSIRA found that TBS did not adequately consider privacy or Charter implications when it included the polygraph as a security screening activity under the Standard on Security Screening.

**Finding 16.** NSIRA found that the Standard on Security Screening insufficiently addresses Charter and privacy implications related to the use of the polygraph.

### Canadian Charter of Rights and Freedoms

**Finding 17.** NSIRA found that the Government of Canada's current use of the polygraph for security screening in the manner described in this review may raise serious concerns in relation to the *Canadian Charter of Rights and Freedoms*.

## Recommendations

**Recommendation 1.** NSIRA recommends that the Treasury Board of Canada urgently remedy the issues identified by this review related to the legality, reasonableness and necessity of the use of the polygraph for security screening in Canada, or remove it from the Standard on Security Screening.

**Recommendation 2.** NSIRA recommends that CSE urgently remedy the issues identified by this review, including Charter and *Privacy Act* compliance, or cease conducting polygraph exams for security screening.