

Federal Court



Cour fédérale

**Date: 20161123**

**Docket: T-699-15**

**Citation: 2016 FC 1289**

[ENGLISH TRANSLATION]

Montréal, Quebec, November 23, 2016

**PRESENT: The Honourable Madam Justice St-Louis**

**BETWEEN:**

**UNION OF CANADIAN CORRECTIONAL  
OFFICERS - SYNDICAT DES AGENTS  
CORRECTIONNELS DU CANADA - CSN  
(UCCO-SACC-CSN)**

**Applicant**

**and**

**ATTORNEY GENERAL OF CANADA**

**Respondent**

**and**

**PRIVACY COMMISSIONER OF CANADA**

**Intervener**

**JUDGMENT AND REASONS**

I. Introduction

[1] On October 20, 2014, the *Standard on Security Screening* [the Standard], adopted by the Treasury Board, came into effect and replaced the *Personnel Security Standard* [PSS], which had been in effect since 1994.

[2] The Standard sets out, in particular, the three security screening levels for federal public service employees, that is, reliability status, “secret” security clearance and “top secret” security clearance, as well as the activities and practices associated with each of these levels.

[3] Under the Standard, although security screening activities vary based on the reliability status or the security clearance sought, all of the levels now require a *financial inquiry* [the Inquiry] of the individual for whom the reliability status or security clearance is sought. For the Inquiry, individuals must first consent to having their credit report sent to their employer, and the employer will then obtain the report from the appropriate private agency and analyze its results. Before the Standard was adopted, Inquiries were only obligatorily conducted for “top secret” clearances.

[4] On February 9, 2015, *Commissioner’s Directive 564-1 – Individual Security Screening* [the Directive] came into effect. It extends the Inquiry to the security screening for renewing the reliability status of Correctional Service of Canada [CSC] employees, because the intent of the screening is to evaluate the honesty and trustworthiness of an individual. Thus, because

correctional officers at the CXI and CXII levels must have reliability status, they become subject to the Inquiry and must consequently consent to having their employer, CSC, obtain their credit report.

[5] The applicant, Union of Canadian Correctional Officers – Syndicat des agents correctionnels du Canada – CSN [the Union], represents all CSC correctional officers at the CXI and CXII levels. It characterizes the new requirement as a [TRANSLATION] “search and seizure” and uses the term [TRANSLATION] “Search” to refer to it, a term that will be repeated in this judgment. The applicant objects to this Search being imposed on its members. It is asking the Court to declare that the part concerning financial inquiries in Appendix B of the Standard and paragraph 3(d) of the Directive are contrary to section 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act, 1982* (U.K.), 1982, c 11 [the Charter]. It is also seeking a declaration that paragraph 3(d) of the Directive breaches section 4 of the *Privacy Act*, RSC, 1985, c P-21 [the Act]. Those provisions are attached hereto.

[6] The respondent, the Attorney General of Canada [AGC], first responds that the contested provisions of the Standard and the Directive, while they constitute a Search, do not necessarily infringe on a right to privacy under section 8 of the Charter because they are reasonable. The AGC also contends that the impugned provisions of the Directive do not violate section 4 of the Act because the information collected from the credit reports *relates directly* to the activity of security screening.

[7] The intervener, the Privacy Commissioner of Canada [the Commissioner], is not taking a position on the issue of compliance with section 4 of the Act in light of the specific facts of this case. However, he outlines what he considers to be the appropriate analytical framework for the implementation of section 4, and argues in this regard that the words *relates directly* create a necessity test. He also discusses certain relevant considerations in connection with the implementation of section 4 in this case, that is, the nature and the scope of the personal information contained in credit reports and the nature of the relationship between credit reports and assessing an employee's trustworthiness, and he argues that correctional officers have a reasonable expectation of privacy. Lastly, without taking a position, he also outlines certain considerations that the Court should, in his opinion, consider in its analysis of sections 8 and 1 of the Charter.

[8] For the following reasons, the Court will dismiss this application for judicial review.

[9] In short, regarding section 8 of the Charter, the Court is of the opinion that the decisions of the Treasury Board and CSC to adopt the contested provisions of the Standard and the Directive are reasonable and do not violate section 8 given the state's objective, the nature of the prison environment, the type of possible threats, the responsibilities of correctional officers, the manner in which the information is obtained, the nature of the information disclosed, the possibility of providing explanations prior to a decision and the avenues of recourse available in the event of a denial of reliability status.

[10] Concerning section 4 of the Act, the Court finds that this section does not contain a necessity test, that it is reasonable to conclude that there is a direct relationship between, first, the Inquiry and obtaining a credit report, and, second, security screening activities, and that CSC's decision to adopt the contested decision of the Directive is consequently reasonable.

## II. Legislative context

[11] Section 7 of the *Financial Administration Act*, RSC, 1985, c F-11 [FAA], sets out that the Treasury Board may act for the Queen's Privy Council for Canada on certain matters, including those relating to general administrative policy in the federal public administration and human resources management in the federal public administration. These matters involve, namely, the determination of terms and conditions of employment (paragraphs 7(1)(a) and (e) of the FAA, attached hereto).

[12] Pursuant to section 7 of the FAA, the Treasury Board issues policies, including the *Policy on Government Security* [the Policy]. According to the wording of section 3 of the Policy, attached hereto, the Policy is rooted in the contextual premise that government security is the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence. Thus, there is a need to ensure that those having access to government information, assets and services are trustworthy, reliable and loyal. Furthermore, according to section 5, attached hereto, the objectives of the Policy are to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management.

[13] Lastly, section 6 of the Policy, also attached hereto, states, *inter alia*, that deputy heads of all departments are responsible for appointing a *departmental security officer* and for ensuring that all individuals who will have access to government information and assets are security screened at the appropriate level and are treated in a fair and unbiased manner.

[14] Obtaining and maintaining a valid reliability status or security clearance is a condition of employment, contract, appointment or assignment within the Government of Canada, including CSC, and employees must consent to it. It requires the collection of personal information on individuals, which is done after they have provided their informed consent. In the case at bar, correctional officers express that consent by signing the Personnel Screening, Consent and Authorization Form [the Form].

[15] Over the years, the Treasury Board has adopted various standards enacting security screening activities, including the Standard, which came into effect on October 20, 2014. The Standard applies to all departments defined in section 2 of the FAA and all federal agencies included in Schedules IV and V of the FAA, and they must all implement it by October 20, 2017. CSC is included in that list.

[16] The objectives of the Standard are to ensure that security screening in the government is effective, efficient, rigorous, consistent and fair and to enable greater transferability of security screening between departments and agencies (section 5 of the Standard). The Standard states that security screening can be standard or enhanced, and describes the associated screening activities.

[17] According to the Standard, the purpose of the Inquiry is to assess whether an individual poses a security risk on the basis of financial pressure or a history of poor financial responsibility (section 7).

[18] In 2015, the Directive came into effect. It incorporates the Standard's requirements for CSC and states, in paragraph 3(d), that one of the responsibilities of the departmental security officer is to ensure that credit checks are conducted at the national level.

[19] For the purposes of this case, this means that all correctional officer members of the Union must, since April 1, 2015, consent to having CSC obtain their credit report, from which data will be analyzed in the security screening associated with the renewal of their reliability status. It should be immediately noted that pursuant to paragraph 4(h) of the Directive, attached hereto, CSC managers will "provide the individual with an opportunity to explain any adverse information".

### III. Position of the parties

#### A. *The Union*

[20] The Union essentially submits (1) that the adoption of the Standard and the Directive is subject to the standard of reasonableness; (2) that the relevant provisions of the Standard and the Directive are unreasonable and violate section 8 of the Charter; (3) that their adoption is not saved by section 1 of the Charter; and (4) that its members' credit reports do not relate directly to

CSC's programs and activities and that as a result, the relevant provisions of the Directive violate section 4 of the Act.

[21] The Union indicates that there is an error in part IV of its memorandum, for the order sought, when it refers to paragraph 2(d) of the Directive and not paragraph 3(d) of the Directive. The Court agrees that that is a clerical error and accepts the correction.

[22] In support of its submissions, the Union submits a total of five affidavits: the affidavit of Kevin Grabowsky, its national president; the affidavit of Laurent Vaillancourt, a correctional officer at level 2 (CXII) and member of the Union; the affidavit of Manon Leblanc, a correctional officer at level 1 (CXI); the affidavit of Dwaynes Soles, a correctional officer at level 2 (CXII); and the affidavit of David Mellor, a correctional officer at level 1 (CXI).

(1) The standard of review is reasonableness

[23] The Union initially contended, in its memorandum, that the correctness standard should apply, but it modified its position at the hearing and agrees with the respondent and the intervener on this point. Thus, the Union accepts that the Standard and the Directive are subject to the reasonableness standard.



(2) The provisions of the Standard and the Directive for checking the credit reports of all employees violate section 8 of the Charter

[24] The Union submits that section 8 of the Charter applies in this case because that provision ensures privacy and the protection of personal information, because requiring correctional officers to consent to a credit report check in order to obtain or renew their reliability status constitutes a Search, and because the Search must be presumed to be unreasonable, which thus imposes on the state the burden of establishing that it is reasonable. However, according to the Union, the state has not satisfied this burden in this case.

[25] The AGC does not object to the application of section 8 of the Charter, but argues that it is not a Search or an *unreasonable* intrusion. It therefore seems appropriate for the Court to reiterate only the last component of the Union's argument, effectively the only issue in dispute.

[26] The Union admits that the Treasury Board may, pursuant to section 7 of the Act, determine the conditions of employment of federal public servants and adopt a standard. It also admits that CSC has the power to adopt a directive. However, it argues that that standard and that directive must comply with the Charter, which is not the case here.

[27] The Union first notes that warrantless Searches are always presumptively unreasonable (*Goodwin v British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46 at para 56 [*Goodwin*]) and that the state has the onus of establishing that the search was reasonable, which can only be done by establishing the following three elements: (1) the Search was authorized by

the law; (2) the law itself is reasonable; and (3) the Search was not conducted in an unreasonable manner. In this case, the Union argues that the state has not established the second element, that is, that the Standard and the Directive are not unreasonable.

[28] To determine the reasonableness of the Standard and the Directive, the Union refers the Court to *Reference re Marine Transportation Security Regulations*, 2009 FCA 234 [*Reference*] and to the following contextual criteria: (1) the strength of the individual privacy interests at stake; (2) the manner in which the Search is conducted; (3) the pressing nature of the public interest served by the statutory scheme authorizing the Search; and (4) to what extent the information sought is likely to further that interest.

[29] Regarding the strength of the individual privacy interests at stake, the Union notes that the details of an individual's financial situation represents precisely the type of information for which individuals should be able to determine when, how and to what extent it is communicated. The reasonable expectation of privacy is thus very important for such interests.

[30] Regarding the manner in which the Search is conducted, which refers to how the information is collected, the Union admits that the checking of credit reports is not the most intrusive measure. However, it is somewhat more intrusive than asking an individual to provide the information him- or herself. The Union also points out that managers in various institutions can be called upon to question correctional officers to obtain explanations for some of the

information collected, and that those managers would then have access to their employees' financial information.

[31] Regarding the pressing nature of the public interest served by the statutory scheme, the Union notes the objective of the Standard, which is to contribute to national security, is valid and important.

[32] However, with respect to the last of the four factors identified, the Union doubts that the information sought is likely to further the purpose of contributing to national security. Instead, it contends that CSC did not present any evidence that financial pressure or a history of financial responsibility has already given rise to incidents that compromised national security, or that that factor has represented a particular risk. The Union adds that CSC has not established the benefits of the Inquiry in the overall assessment of the honesty and trustworthiness of officers, that it has failed to explain how this new measure would establish elements that are not covered by other existing measures, and that it has not established a correlation between the information in credit reports and the number of corrupt employees.

[33] The Union points out that none of the approximate 200 inquiries that have been conducted each month since 2015 has led to the non-renewal of the reliability status of a correctional officer because of information discovered in the officer's credit report. The Union infers from this that the collection of information seems to have minimal impact on the final result.

[34] In summary, the Union argues that the systematic checking of the credit reports of members of the Union constitutes an unreasonable Search, contrary to section 8 of the Charter.

(3) The violation of section 8 of the Charter is not saved by section 1 of the Charter

[35] Finding that the Search is unreasonable, the Union turns to section 1 of the Charter, attached hereto, and argues in this regard that the violation of section 8 is not justified. It submits that the AGC must demonstrate, on a balance of probabilities, that a credit check is a pressing and substantial objective and that the means chosen to achieve that objective are proportional.

[36] The means chosen are proportional if (1) there is a rational connection between the means adopted and the objective; (2) the law impairs the right guaranteed by the Charter as little as possible; and (3) there is proportionality between the deleterious effects and the beneficial effects of the law (*R v Oakes*, [1986] 1 SCR 103).

[37] Regarding the first point, the Union acknowledges that the objective of the contested measure is to protect national security by ensuring that dishonest or untrustworthy individuals do not have access to restricted assets or facilities or privileged information of the government, in particular as employees. At the same time, it admits that that objective is pressing and substantial and includes the existence of a rational connection between the checking of employees' credit and the objective (paragraphs 55 and 56 of the Applicant's Memorandum).

[38] However, concerning the second point, the Union argues that the measure does not impair the Charter right as little as possible because the scope of the Standard is excessive and the category of persons concerned is too broad. The government could have achieved its objective by restricting the categories of persons for which [TRANSLATION] “that type of check is necessary” (paragraph 58 of the Applicant’s Memorandum).

[39] Regarding the third point, the Union maintains that the deleterious effects from checking the credit reports outweigh the benefits. In fact, there seems to be minimal benefits with respect to the objective of the Search, namely, because a reliability status has never been revoked because of adverse information in a credit report, while the measure has caused increased stress among Union members.

(4) The provisions providing for credit report checks set out in the Standard and the Directive are contrary to section 4 of the Act

[40] The Union argues, lastly, that the contested measures violate section 4 of the Act, which limits the information that a government institution may collect on an individual to that which relates directly to an operating program or activity of the institution.

[41] The Union cites the *Larousse en ligne* French dictionary’s definition of “direct” [[TRANSLATION] “direct”]: “*qui est en relation immédiate avec quelque chose d’autre, qui y est étroitement lié*” [[TRANSLATION] “that which immediately relates to something, that which is closely connected”] and refers the Court to section 5 of Quebec’s *Act respecting the Protection*

*of Personal Information in the Private Sector*, CQLR, c P-39.1, which states that the information collected must be *necessary*.

[42] The Union submits that there is no *direct relationship* between its members' credit reports and CSC's activities. To support its statement, the Union points out that its members do not manage money or budgets as part of their jobs and that, for that reason, their personal financial practices in no way demonstrate their trustworthiness or ability to act as correctional officers.

[43] In that respect, at the hearing, the Union tried to minimize the scope of certain passages of its memorandum by stating that they were not admissions that a credit check could be justified in the assessment of the clearance level for certain positions, or even that a credit report could be related to the assessment of an individual's trustworthiness and honesty. The Court will revisit this aspect in its analysis.

[44] The Union refers to the four-part test used by this Court to determine whether the use of surveillance cameras was acceptable in *Eastmond v Canadian Pacific Railway*, 2004 FC 852 [*Eastmond*]. According to the test, to determine whether the purpose for which the personal information is collected is reasonable, there must be an assessment of (1) whether the measure is demonstrably necessary to meet a specific need; (2) whether it is likely to be effective in meeting that need; (3) whether the loss of privacy is proportional to the benefit gained; and (4) whether there is a less privacy-invasive way of achieving the same end.

[45] The Union submits that the contested measures do not meet this test. First, the measure is not necessary to meet a specific need at CSC because there is no evidence that employees who experience some difficulty in managing their personal finances are less honest or represent a heightened risk for CSC. Furthermore, there are no cases where economic vulnerability factors have played a role in an incident in which an inmate has bribed a correctional officer, and the scale of any corruption problems has not been demonstrated.

[46] Second, the Union argues that this measure does not meet the effectiveness criterion with respect to the objective, namely, because since April 2015, no correctional officers have been denied the renewal of their reliability status after information, even adverse, was obtained from their credit report.

[47] Third, because there are minimal benefits to this measure, the deleterious effects become disproportionate to a loss of privacy.

[48] Fourth, the Union argues that there are alternate ways to assess the trustworthiness of its members without having to make a credit report inquiry.

#### B. *The AGC*

[49] The AGC essentially submits that the Standard and the Directive constitute reasonable [TRANSLATION] “decisions”. Concerning section 8 of the Charter, the AGC contends that they essentially represent a proportionate balancing of the objectives of the legislative scheme and the

value of privacy. Regarding section 4 of the Act, he advances that the partial information collected, in the credit report, *relates directly* to security screening activities carried out by CSC.

[50] The AGC submits three affidavits: the affidavit of Charles Taillefer, Director, Policy Development and Performance Measurement, Security and Identity Management, at the Treasury Board of Canada Secretariat; the affidavit of Nick Fabiano, Director General, CSC Security; and the affidavit of Dorothy Sicard, Manager, Personnel Security Screening, CSC Departmental Security.

[51] The AGC is first concerned about rectifying the facts presented by the Union to provide the Court with the appropriate factual background, which is at the heart of the analysis the Court must conduct. The AGC therefore describes the purpose of security investigations, the historical background of security screening, the evolution of threats to security in Canada since 1994, the implementation of a technological working environment, the development of the 2014 Standard, the content of the 2014 Standard, details on CSC and on the work of its employees (including correctional officers), details on the prison population and the content of credit reports.

[52] According to the AGC, the Court must determine four issues: (1) the applicable standard of review; (2) whether CSC's decision to adopt the Directive implementing the Standard is reasonable regarding the credit report checks, with respect to section 4 of the Act; (3) whether the Treasury Board's decision to adopt the Standard and that of CSC to adopt the Directive implementing it are reasonable regarding the credit report checks, with respect to the right to



privacy in section 8 of the Charter, that is, whether they are the result of a proportionate balancing of the importance of ensuring the security of government operations through security screening and the right to privacy of correctional officers; and (4) whether section 1 of the Charter is engaged.

[53] The Court will follow the Union's order of presentation for ease of reading, that is, (1) the applicable standard of review; (2) section 8 of the Charter; (3) section 1 of the Charter; and (4) section 4 of the Act.

(1) The standard of review is reasonableness

[54] The AGC submits, like the Union, that the standard of "reasonableness" should apply in this case because the Standard and the Directive constitute discretionary decisions adopted by the Treasury Board and CSC, and the Treasury Board and CSC have particular expertise in the area of the information that is required to determine the trustworthiness of public servants.

[55] The AGC emphasizes the consequences of choosing this standard of review and, in particular, the fact that the Court must show deference, that it must recognize the expertise of the Treasury Board and CSC in the area of the information that is required to determine the trustworthiness of public servants and that it cannot substitute its own decision for that of the Treasury Board and CSC.

(2) The Standard and the Directive are reasonable with respect to the credit checks pursuant to section 8 of the Charter

[56] The AGC does not contest that it constitutes a Search or that section 8 of the Charter applies, but argues that it is not an *unreasonable* Search. In fact, the AGC contends that the Standard and the Directive are not unreasonable because they represent a proportionate balancing of the objectives of the legislative scheme and the value of privacy.

[57] According to the AGC, the analysis to be conducted when the Charter value that is engaged is privacy is akin to that which is aimed at determining the reasonableness of a statute authorizing a Search under section 8 of the Charter. This analysis consists in balancing the state's legitimate interest in achieving legislative objectives with its effect on individual personal rights.

[58] Thus, having admitted that it constitutes a Search, the AGC argues that the factors to be examined regarding the value of privacy that supports section 8 of the Charter are similar to those examined in support of section 4 of the Act. They are (a) the nature and the purpose of the legislative scheme, including the administrative context, objective and finality of the public interest; (b) the manner in which the credit report was obtained; (c) the degree of intrusiveness; and (d) the review subsequent to a decision (*Goodwin* at paras 55 to 57; *Reference* at paras 50 to 53). The AGC also examines (e) the balancing of competing interests and states that the decisions involved are the result of a reasonable balancing that takes all of these factors into account.

(a) *The nature and purpose of the statutory scheme, including the administrative context, objective and finality of the public interest*

[59] The AGC notes certain contextual factors such as those related to the adoption of the Standard by the Treasury Board, security screening, the working environment of correctional officers, the risks of fraud, corruption, threats and manipulation that they face and access to databases. Thus, given the controlled and regulated environment, correctional officers should expect to be under increased surveillance.

(b) *The manner in which credit reports are obtained*

[60] The Form used by CSC includes a warning informing its signatories of why they agree to provide their information, what the information will be used for, the location in which the information will be stored and when the information will expire. Thus, correctional officers are informed that CSC will obtain their credit report, and that they may contact the credit reporting agency to obtain their credit report beforehand and ask that any erroneous information be corrected or add explanations, if applicable.

[61] According to the AGC, this approach is a lot less intrusive than a Search or a third party collection without prior consent.

(c) *Degree of intrusiveness*

[62] The AGC submits that credit reports are held by third parties that collect information on the credit history of millions of individuals, and that they contain information for third parties. Thus, correctional officers should expect the information therein to be shared with third parties. Furthermore, according to the AGC, the reports contain less information than is claimed by the Union. They do not contain banking transactions, transaction statements or credit scores. In addition to biographical data, the reports essentially reveal the individual's available credit, used credit and payment history.

[63] The AGC argues that credit reports are requested and reviewed only by security division staff at CSC headquarters in Ottawa and states that institution managers never have access to credit reports at the interview level.

*(d) Post-decision review*

[64] Lastly, the AGC argues that correctional officers have recourse to explain any adverse information in their credit report and to contest any decision to revoke their reliability status. The availability of such recourse supports the finding of reasonableness.

*(e) Balancing of interests*

[65] The AGC argues that CSC put in place a regime that strikes a proper balance between the value of privacy protected by section 8 of the Charter and the legitimate objectives of the government's legislative scheme.

[66] The Standard's objective is not only to ensure national security, but also to provide reasonable assurance that individuals can be trusted to safeguard government information, assets and facilities and to reliably fulfil their duties.

[67] The Inquiry set out in the Standard was added further to the determination that the trustworthiness of public servants, without a credit report, was not adapted to the realities and threats we face today. According to the evidence, greed is one of the main sources of motivation inciting employees to commit a security violation.

[68] The fact that correctional officers do not have access to sums of money as part of their work is irrelevant. They perform their work in an environment where they could be influenced or forced to disclose sensitive information, move contraband in institutions or engage in other reprehensible conduct for financial gain likely to present a security risk.

[69] The Inquiry and how CSC uses the resulting information constitute reasonable measures that minimally affect the privacy of correctional officers, because (1) there is no mention in the credit reports that CSC obtained a copy thereof, so credit scores are not affected; (2) credit reports obtained by CSC do not have a risk assessment concerning the credit score; (3) credit reports identify only information concerning debt repayments; (4) credit reports are documents that are readily available to those who request them; (5) credit reports are kept in a secure environment; and (6) correctional officers have the opportunity to explain any adverse information.

(3) The measure is justified by section 1 of the Charter

[70] The AGC argues that even if the Court finds that the Standard and the Directive breach section 8 of the Charter, the measure they put in place is saved by section 1 of the Charter.

Obtaining credit reports actually pursues an important, rational objective, infringing the Charter right minimally and proportionately.

(4) CSC's decision to adopt the Directive implementing the Standard is reasonable with respect to credit report checks under section 4 of the Act

(a) *Preliminary issue*

[71] The AGC submits that this judicial review is premature because there is another appropriate recourse for contesting a breach of section 4 of the Act: not an application for judicial review, but a complaint to the Commissioner pursuant to paragraph 29(1)(h) of the Act (attached hereto). The AGC points out that such complaint is already before the Commissioner. Even though he has not yet rendered a decision, this is another adequate recourse (*Strickland v Canada (Attorney General)*, 2015 SCC 37 [*Strickland*]) for obtaining findings and recommendations.

[72] At the hearing, the AGC clarified his position. Relying on, in particular, *Canada (Auditor General) v Canada (Minister of Energy, Mines and Resources)*, [1989] 2 SCR 49 [*Auditor General*], he contends in essence that Parliament did not intend to render the rights justiciable, that the Commissioner has the desired power and can make a report to Parliament, and that

recourse to the Court is limited to the refusal of access set out in section 41 of the Act (attached hereto).

(b) *The relevant provisions of the Standard and the Directive regarding the credit report checks are reasonable and do not breach section 4 of the Act*

[73] In the alternative, if the Court decides to hear the case pursuant to section 4 of the Act, the AGC argues that the information collected clearly *relates directly* to security screening because that information contributes to assessing an individual's vulnerability, verifying the elements of his or her conduct, identifying indicators of other problems that impact security and ensuring that correctional officers are trustworthy and honest.

[74] The AGC submits that the decisions at issue are not unreasonable because of an alleged breach of section 4 of the Act, which, together with section 5 of the Act (attached hereto), provides for two conditions for obtaining personal information, that is (1) the information collected *relates directly* to an operating program or activity of the institution; and (2) the information is collected directly from the correctional officer or the correctional officer has consented to it being collected.

[75] Regarding the first condition, the AGC submits that the words *relates directly* do not give rise to a difficulty of interpretation and do not mean *necessary*. In this respect, he advances that the information collected by CSC using credit reports "relates directly" to security screening. In fact, there is, in the opinion of the AGC, a direct relationship between obtaining a correctional

officer's credit report and the review of his or her trustworthiness because even if officers do not have access to sums of money, they nevertheless work in a highly secure environment where they are exposed to corruption.

[76] Thus, credit reports are relevant because they make it possible to assess four aspects of an individual (paragraph 61 of the Respondent's Memorandum), and the AGC contends that the evidence demonstrates that there is a direct relationship between reviewing a correctional officer's credit report and assessing his or her trustworthiness.

[77] The AGC also argues that correctional officers are informed of what they are consenting to when they sign the Form and that they are thus providing informed consent, which can be set aside only on basis of error, fear or injury.

[78] The AGC rejects the parallel with section 5 of the *Act respecting the Protection of Personal Information in the Private Sector* (attached hereto) raised by the Union because that section uses the word *necessary* and consequently integrates a necessity test. The AGC also rejects the parallel with *Eastmond* because that dispute concerned the installation of cameras without the employees' consent, which is not the issue here, and because the wording of the statute at the centre of that case was different from that of section 4 of the Act.



[79] At the hearing, the AGC specified that credit reports do not indicate credit scores, that there is no trace of the checks in the reports, that there is no cash flow element and that credit reports are an instrument used for evaluating the factor or the likelihood of vulnerability.

C. *The Commissioner - Intervener*

[80] The Commissioner argues that the Court must determine whether the requirement of a credit report check is consistent with section 4 of the Act and section 8 of the Charter. After a concise statement of facts, the Commissioner first addresses the preliminary issue of the premature recourse raised by the AGC by submitting that the Union may raise a violation of section 4 of the Act in the application for judicial review. The Commissioner then examines the framework of analysis and the relevant considerations for the implementation of section 4 of the Act and ends with the reasonable expectation of privacy of correctional officers and the infringement of section 8 of the Charter, a point that he, however, does not take a position on. The Court will follow the following order in the presentation of the arguments of the intervener: (1) the reasonable expectation of privacy of correctional officers and section 8 of the Charter; and (2) the framework of analysis for section 4 of the Act.

- (1) Correctional officers have a reasonable expectation of privacy with respect to their credit report

[81] The Commissioner submits that correctional officers have a reasonable expectation of privacy with respect to their credit report and cites the criteria set out in *R v Edwards*, [1996] 1 SCR 128 at para 31. Those criteria support the finding that there is a legitimate

expectation of privacy because personal information is protected by federal and provincial privacy legislation in both the private and public sectors. Individuals subject to the Standard and the Directive cannot knowingly choose to not provide their consent to disclose their credit report without running the risk of losing their job. As stated above, the Commissioner does not, however, take a position on the issue of a reasonable expectation of privacy under section 8 of the Charter.

(2) Section 4 of the Act imposes a framework of analysis

(a) *Preliminary issue*

[82] The Commissioner objects to the AGC's position with respect to the prematurity of the recourse of the Union. The Commissioner concedes that the Court may refuse to hear the application for judicial review if the Union failed to pursue an adequate alternative remedy (*Buenaventura Jr v Telecommunications Workers Union (TWU)*, 2012 FCA 69 at para 24), but argues that there is no such adequate remedy in this case.

[83] The Commissioner raises five arguments in support of his position, that is, (1) the Commissioner's authority under the Act is limited to providing non-binding findings and recommendations on complaints (*H.J. Heinz Co. of Canada Ltd. v Canada (Attorney General)*, 2006 SCC 13 at paras 35-37); (2) once the Commissioner has published his findings, the Act does not provide for any subsequent recourse, and the complainant must thus file an application for judicial review before this Court to obtain a binding decision; (3) this Court is the most

effective forum providing the most expeditious procedural avenue for processing the issues raised in this application; (4) there is no risk of contradictory decisions in this case because the Commissioner's findings are not binding; and (5) it is appropriate in the circumstances for the Court to decide this issue.

[84] The Commissioner rejects the arguments proposed by the AGC and the parallel drawn with *Auditor General* and *Strickland*. According to the Commissioner, those decisions were made in an extremely specific context that cannot be imported in this case.

(b) *The appropriate framework of analysis for the implementation of section 4 of the Act*

[85] The notion of *relates directly* in section 4 of the Act is not defined in the Act and, according to the Commissioner, this notion must be interpreted considering that the objective of section 4 of the Act is to limit the amount of personal information collected by government institutions.

[86] The Commissioner raises principles of statutory interpretation to support the proposal that *relates directly* means necessary in this context. According to the Commissioner, this interpretation is more consistent with the ordinary meaning of section 4 of the Act, with the interpretation that the AGC previously provided, and with the overall context and purpose of the Act. In this regard, the Commissioner specifically notes comments made by a legal representative for the Minister of Justice, directives of the Treasury Board Secretariat, the

Commissioner's past findings and an *obiter* of this Court in *Canada (Privacy Commissioner) v Canada (Labour Relations Board)*, [1996] 3 FCR 609.

[87] According to the Commissioner, this interpretation also requires that the employer demonstrate that there is no adequate less intrusive measure.

[88] In the alternative, the Commissioner argues that if the Court does not accept that the aspect of necessity exists in section 4 of the Act, this aspect must nonetheless be interpreted in a restrictive manner so that irrelevant personal information that could lead to the collection of other possibly relevant information is not collected.

(c) *Relevant considerations for the implementation of section 4 of the Act in this matter*

(i) Nature of the personal information in a credit report

[89] The Commissioner notes basically that credit reports contain highly sensitive personal information, the disclosure of which must be limited. In addition, correctional officers could be forced to explain some of the information and thus disclose additional personal information. Credit reports contain information on an individual's current debt and financial history.

(ii) Direct relationship between credit reports and the assessment of an individual's trustworthiness

[90] The Commissioner is asking the Court to consider whether the AGC effectively established that credit reports constitute an effective means of assessing the trustworthiness of employees and that no other reasonable, less intrusive means exist.

[91] Regarding the first point, the Commissioner submits that there is no empirical evidence that a credit report is an effective measure for achieving the objective of assessing an employee's trustworthiness.

[92] Regarding the second point, the Commissioner submits that there are less intrusive and more effective ways to allow organizations to assess whether their employees are trustworthy. Those measures include, for example, interviews or even checking references from former employers.

#### IV. Issues

[93] The Court must first determine the appropriate standard of review and then address the following issues:

- (1) Does the part of the Standard's Appendix B and paragraph 3(d) of the Directive that include the Inquiry as a screening activity for the reliability status of correctional officers breach section 8 of the Charter?
- (2) If the answer is yes, is that breach saved by section 1 of the Charter?
- (3) Does paragraph 3(d) of the Directive, which includes the Inquiry as a screening activity for the reliability status of correctional officers, breach section 4 of the Act?

V. Analysis

A. *Standard of review*

[94] The Treasury Board's decision to adopt the Standard and CSC's decision to adopt the Directive implementing the Standard constitute discretionary administrative decisions. Thus, the standard of review that should be applied in this case is reasonableness, even if section 8 of the Charter is engaged (*Dunsmuir v New Brunswick*, 2008 SCC 9 at para 53; *Thomson v Canada (Attorney General)*, 2015 FC 985 at para 38, affirmed by 2016 FCA 53 at para 24).

B. *Does the part of the Standard's Appendix B and paragraph 3(d) of the Directive that include the Inquiry as a security screening activity for the reliability status of correctional officers violate section 8 of the Charter?*

(1) Elements to determine

[95] According to the principles set out by the Supreme Court of Canada in 2015 in *Goodwin*, to address this issue, it must be determined (1) whether section 8 is engaged; (2) whether the Search is authorized by law; (3) whether the Search set out in the law is unreasonable; and (4) whether the Search was carried out in an unreasonable manner.

[96] It is not in dispute in this case that section 8 is engaged because the collection of credit reports constitutes a Search under section 8 and correctional officers have a certain expectation of privacy concerning the information in their credit report.

[97] It is also undisputed that the Search is authorized by law and that, while the provisions in question are not those of a law but of a standard and a directive, the same criterion can be used (See for example *Jackson v Joyceville Penitentiary*, [1990] 3 FC 55, and *Fila Canada Inc v Untel*, [1996] 3 FC 493; see also *Myers v Canada (Attorney General)*, 2007 FC 947 at paras 30 and 31).

[98] Lastly, it is also undisputed that the Search was not conducted in an unreasonable manner and there is no evidence to the contrary.

[99] Thus, it is up to the Court to determine whether the Search set out in the law is unreasonable.

(2) The reasonableness of the Search

[100] We find no determinative test for assessing the reasonableness of a Search (*Goodwin; Thomson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 SCR 425 [*Thomson Newspapers*]), but understand that the assessment of reasonableness must be conducted with flexibility and considering the purpose of the law in question (*R v McKinlay Transport Ltd*, [1990] 1 SCR 627). The conclusion will also depend on “the importance of the state objective and the degree of impact on the individual’s privacy interest” (*R v Rodgers*, 2006 SCC 15 at para 27). In this regard, as discussed in *Hunter et al v Southam Inc*, [1984] 2 SCR 145 [*Hunter*] and noted by the Union, the Court will assess “whether in a particular situation the public’s interest in being left alone by government must

give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.”

[101] Because warrantless Searches are presumptively unreasonable (*Goodwin* and *Hunter*), the state has the burden of establishing the reasonableness of the Search that is at issue in this dispute.

[102] The Court is guided by the criteria reiterated by the Supreme Court of Canada in *Goodwin* in 2015 and those to which the Federal Court of Appeal referred in *Reference*, and will therefore examine (a) the purpose of the Standard and the Directive, including the pressing nature of the public interest and to what extent the information sought is likely to further that interest; (b) the nature of the Standard and the Directive; (c) the seizure mechanism, that is, the manner in which a credit report is obtained, and the degree of intrusiveness; (d) the review subsequent to a decision or the availability of judicial supervision.

- (a) *The objective of the Standard and the Directive, including the pressing nature of the public interest and to what extent the information sought is likely to further that interest*

[103] The review of the objective of the law will make it possible to militate for or against its reasonableness. For example, the purpose of preventing death and serious injuries on public highways was recognized as “compelling” and as weighing “heavily in favour of the reasonableness of the breath seizure” (*Goodwin* at para 60).



[104] It seems appropriate to note here that the objectives of the Policy governing the Standard are to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management.

[105] The objectives stem from the contextual premise that government security is the assurance that information, assets and services are safeguarded from compromise and individuals are protected against workplace violence. Thus, the government must ensure that all individuals who have access to government information and assets are security screened at the appropriate level and are treated in a fair and unbiased manner.

[106] The objective of the Standard is to carry out security screening and enable its transferability within the government. Lastly, the objective of the Inquiry is to assess whether an individual poses a security risk on the basis of financial pressure or history of poor financial responsibility.

[107] According to the Union, the Standard contributes to national security, which, it admits, constitutes a valid and important pressing and substantial objective. The Court accepts this proposal and also considers that national security or government security, that is, safeguarding assets, information and services and protecting individuals against workplace violence, was recognized as a compelling objective that supports the reasonableness of the Standard and the Directive (*R v Simmons*, [1988] 2 SCR 495 at paras 48-49; *Reference* at para 53).

[108] The Court agrees with the AGC's position that it is likely that the information obtained will further the objective of national security. It is important, at this stage, to examine the responsibilities of correctional officers at the CXI and CXII levels. The positions involve the safety and protection of the public, staff members, inmates and the institution as well as the functional supervision of activities for CSC. Correctional officers at the CXII level are also responsible for case management services and the safe reintegration of offenders into society. These two groups are in direct contact with inmates, their families and visitors to the prison. They must prepare reports, from which information is used by CSC staff and other organizations to make decisions concerning security and the reintegration of inmates into society.

[109] The Union admits that employment in the public service, particularly in CSC, is considered a relatively regulated field (paragraph 31 of its memorandum). It also admits that there may be a rational connection between checking employees' credit reports and the objective of the contested measure of protecting national security by ensuring that dishonest and untrustworthy individuals have access to restricted assets or facilities or privileged information of the government (paragraphs 55 and 56 of its memorandum). In addition, the Union does not dispute that Inquiries can be justified [TRANSLATION] "in the context of security investigations of individuals in certain job categories" (paragraph 2 of its memorandum). However, it stresses that the job of correctional officers does not fall under such category because correctional officers do not manage money or budgets and that, in that context, their personal financial practices do not demonstrate their trustworthiness or their ability to act in their position. Access to sums of money is thus a determinative element for the Union.

[110] However, while correctional officers do not manage money or budgets, they may nonetheless have access to sums of money resulting from corruption. In fact, the Court in this regard accepts the AGC's proposal that correctional officers hold [TRANSLATION] "the keys to the prison", protect the public and inmates, have access to sensitive information in the Offender Management System and are the main point of contact for inmates. This position is confirmed by the information in the work descriptions for correctional officers at the CX1 and CXII levels, submitted with the affidavit of Nick Fabiano, attesting to officers' duties of surveillance, verifications and security.

[111] In the words of the AGC, correctional officers work in an environment where the imperatives of security measures are primordial and constant and where they are likely to be the subject of attempted bribery, threats and manipulation.

[112] Thus, if, as the Union admits, conducting Inquiries and analyzing the credit reports of employees who manage sums of money or budgets is justified, it seems evident that it would also be justified for employees to whom money may be offered as a bribe or who, even absent the monetary factor, could be threatened, manipulated or coerced, as described, for example, by Nick Fabiano in his affidavit (at paras 37-39).

[113] The likelihood that the information provided furthers the objective of the Standard and the Directive favours its reasonableness.

(b) *The nature of the Standard and the Directive*

[114] The Court recognizes that the criminal or regulatory characterization of a Search is relevant in assessing its reasonableness (*Goodwin* at para 60). A regulatory law will thus give rise to a lower expectation of privacy than a criminal law (*Thomson Newspapers* at paras 95 and 122). However, in this case, the contested provisions are administrative in nature and are thus regarded as less intrusive (*Reference* at para 52), which supports the reasonableness of the Standard and the Directive.

(c) *The seizure mechanism, that is, the manner in which a credit report is obtained, and the degree of intrusiveness*

[115] Regarding the choice of the seizure mechanism used, it is interesting the note that demands for personal information, a photograph and fingerprints are among the least intrusive forms of search (*Reference* at para 61), versus, for example, breath demands or even blood samples (*Goodwin* at para 65).

[116] In the case at bar, the employer obtains the individual's credit report following the signing, by that individual, of the Personnel Screening, Consent and Authorization Form, on which the individual checked the box confirming his or her consent. Completing a questionnaire, even when a refusal to sign it may jeopardize the person's employment, constitutes a lesser intrusion on privacy than other types of searches (*Reference* at paras 48 and 51) and thus supports the reasonableness of the impugned provisions.

[117] Concerning the degree of intrusiveness, the evidence, including a document by the Financial Consumer Agency of Canada entitled “Understanding your credit report and credit score” (2016), at pages 8 *et seq.*, shows that a credit report may disclose the following information:

- The individual’s biographic information (name, date of birth, current and previous addresses, current and previous telephone numbers, current and previous employers, social insurance number, driver’s licence number, passport number);
- Credit history information, such as credit accounts and transactions (credit cards, lines of credit or loans) and telecommunications accounts; negative banking information; public records (bankruptcy and registered items); debts sent to collection agencies; information on lenders; and remarks (consumer statements, fraud alerts and identity verification alerts);
- Mortgage information and history of mortgage payments;
- The codes attributed to various credit accounts, including a letter (R) and a number (from 1 to 9), indicating the individual’s payment history for each item.

[118] Adverse information is generally kept for up to seven years.

[119] Credit reports therefore do not disclose an individual’s credit score, cash flow, or even the balance of the individual’s bank accounts. In short, as its name indicates, a credit report discloses the credit granted to an individual, the level of use of that credit and the associated payment history. Apart from speculation on the level of debt and the existence of a mortgage loan identifying the individual as a property owner, credit reports do not disclose details on an individual’s lifestyle, contrary to what the Union claims.

[120] The Court is aware that the reliability of the results can undermine the reasonableness of the seizure (*Goodwin* at para 66). However, in this case, individuals have the opportunity to

check the content of their credit report before its disclosure, to correct inaccurate information if applicable and to ensure the reliability of the information disclosed.

[121] The seizure mechanism via the Form signed by the individual, the less invasive degree of intrusiveness considering the information concerned, and the possibility that the individual can verify the reliability of the information disclosed favour the reasonableness of the provisions of the Standard and the Directive.

(d) *Review subsequent to a decision or the availability of judicial supervision*

[122] Bear in mind that “[w]hile less exacting review may be sufficient in a regulatory context, the availability and adequacy of review is nonetheless relevant to reasonableness under s. 8” (*Goodwin* at para 71). Thus, the existence of judicial supervision allowing for a review of the seizure will support the reasonableness of the law, while contrarily, “[a] provision authorizing such an unreviewable power would clearly be inconsistent with s. 8 of the Charter” (*Hunter* at page 166). Note that the possibility of a reconsideration of the negative decision and an application for judicial review proved sufficient in *Reference* at para 60.

[123] The individual will have the opportunity to provide explanations for any adverse information at a meeting, which supports reasonableness. However, although Ms. Sicard testified that such meetings have never been conducted by institutional managers, the Directive itself indicates this possibility because paragraph 4(h) states that managers will provide the individual with an opportunity to explain any adverse information. It is indeed possible and likely that

institutional managers will be provided with their employees' financial information and their employees' will consequently be required to disclose additional personal information to them.

[124] Paragraph 4(g) of the Directive sets out the review procedure and the availability of redress before this Court or the Canadian Human Rights Commission based on the facts, allegations and remedies sought. Appendix E of the Standard also states the procedure for contesting the denial or revocation of a reliability status or security clearance.

[125] Thus, even though the responsibility given to managers to conduct interviews with officers is debatable, the possibility that the ultimate decision to deny reliability status could be reviewed by this Court and/or another tribunal according to the circumstances favours the reasonableness of the Standard and the Directive.

### (3) Conclusion

[126] Thus, the Court considers, in particular, the valid and important objective of the Standard and the Directive; the likelihood that the information provided furthers the objective of public interest; the administrative nature of the impugned provisions; the choice of seizure mechanism; the degree of intrusiveness; the possibility of providing explanations for adverse information; as well as the review and reconsideration procedures and the availability of judicial supervision. A review of these criteria makes it possible for the Court to find that the provisions of the Standard and the Directive that include the Inquiry as a security screening activity for the reliability status of correctional officers do not violate section 8 of the Charter and that the Treasury Board's

decision to adopt the Standard and CSC's decision to adopt the Directive are, in this respect, reasonable.

[127] The Union and the AGC discussed applying section 1 of the Charter in this application. However, because the Court finds that there was no violation of section 8 of the Charter, it is not necessary to examine whether the violation is justified by section 1 of the Charter or to determine whether "the decision reflects a proportionate balancing of the Charter protections at play" (*Doré v Barreau du Québec*, 2012 SCC 12 at para 57).

C. *Does paragraph 3(d) of the Directive, which includes the Inquiry as a security screening activity for the reliability status of correctional officers, violate section 4 of the Act?*

[128] The Court will first address the AGC's argument that this redress is premature.

(1) Premature redress

[129] The Court accepts the Commissioner's position that the complaint process set out in paragraph 29(1)(h) of the Act should not be considered an adequate alternative remedy because the Commissioner's findings and recommendations with respect to complaints are not binding and the Act does not provide for any subsequent recourse, requiring that the applicant file an application for judicial review to obtain a binding decision. Furthermore, because the issues specific to section 4 of the Act are similar to those related to section 8 of the Charter, it seems appropriate for the Court to rule on these two issues simultaneously.



(2) Section 4 protection

(a) *General principles*

[130] According to section 2, the purpose of the Act is to “extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information”. It concerns government institutions, defined as any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule, and any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the FAA. This includes CSC.

[131] The Supreme Court of Canada addressed the purpose of the Act specifically as “limit[ing] the government’s ability to collect, use and disclose personal information” (*Dagg v Canada (Minister of Finance)*, [1997] 2 S.C.R. 403 at para 47, Laforest J (dissenting on other points)). To achieve this objective, “Parliament has created a detailed scheme for collecting, using and disclosing personal information. First, the Act specifies the circumstances in which personal information may be collected by a government institution, and what use the institution may make of it: only personal information that relates directly to an operating program or activity of the government institution that collects it may be collected (s. 4)” (*Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53 at para 27 [*Lavigne*]).

[132] Personal information includes information on an individual's employment history or financial transactions in which he or she participated. Regarding the *collection* of personal information, which is at issue here, section 4 of the Act states that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

[133] The Court is aware of the importance of protecting an individual's personal information and cites a passage from the decision of the Supreme Court of Canada in *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19:

The focus is on providing an individual with some measure of control over his or her personal information: Gratton, at pp. 6 ff. The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society: *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, at para. 24; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, at paras. 65-66; *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, [2006] 1 S.C.R. 441, at para. 28.

(b) *Direct relationship*

[134] Under section 4 of the Act, a government institution shall collect only information that "relates directly to an operating program or activity of the institution". It is thus important to

define the expression *relates directly*, identify the personal information collected and the operating program or activity of the government institution, and examine whether they are directly related.

[135] Because the terms *relates directly*, or *lien direct* in French, give rise to a different interpretation by the parties and are not defined in the Act, it is helpful to use methods of interpretation to establish their meaning. In accordance with the modern approach to statutory interpretation, the words of an act are to be read “in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament” (Elmer Driedger, *Construction of Statutes*, 2nd ed, 1983, at p 87; *Rizzo & Rizzo Shoes Ltd (Re)*, [1998] 1 SCR 27 at para 21).

[136] If we look first at the grammatical and ordinary sense of the words, three rules must guide our interpretation in accordance with the grammatical method: “(1) words must be given their ordinary meaning; (2) words must be given the meaning they had on the day the statute was enacted; (3) adding to the terms of the statute, or depriving them of effect, should be avoided” (Pierre-André Côté in collaboration with Stéphane Beaulac and Mathieu Devinat, *The Interpretation of Legislation in Canada*, 4th ed., Toronto: Carswell, 2011, at p 277). As previously stated, the *Larousse en ligne* French dictionary defines the term “*direct*” [[TRANSLATION] “direct”] as “*qui est en relation immédiate avec quelque chose d’autre, qui y est étroitement lié*” [[TRANSLATION] “that which immediately relates to something, that which is closely connected”. The *Canadian Oxford Dictionary* defines the term “directly” as “in a direct

manner”; the term “direct” is defined as “without intermediaries or the intervention of other factors”. The *Larousse en ligne* French dictionary defines the term “*nécessaire*” [[TRANSLATION] “necessary”] as “*dont on ne peut se passer*” [[TRANSLATION] “that which is required”]; “*qui est très utile ou obligatoire, indispensable, qui doit être fait, qui s'impose*” [[TRANSLATION] “that which is very useful or obligatory, indispensable, that which must be done, is imperative”]. Its synonyms include “*obligatoire*” [[TRANSLATION] “obligatory”], “*obligé*” [[TRANSLATION] “inescapable”], “*inévitabile*” [[TRANSLATION] “unavoidable”] and “*essentiel*” [[TRANSLATION] “essential”].

[137] To specify the meaning of the terms *relates directly*, the Union refers to section 5 of the *Act respecting the Protection of Personal Information in the Private Sector*, which instead uses the term *necessary*. The wording of subsequent laws should therefore be considered with caution. The Supreme Court of Canada stated that “[a] comparison [sic] of like statutes enacted by the same Legislature is at most of peripheral assistance in determining the proper interpretation of the statute before the Court.” (*Corp. of Goulbourn v Regional Municipality of Ottawa-Carleton*, [1980] 1 SCR 496 at page 515). In addition, the law to which the Union refers was not enacted by Parliament, but by the province of Quebec, and its argument can therefore be rejected.

[138] To complete the purpose of the Act stated in section 2 of the Act, it is possible to consider the administrative interpretation thereof, although such interpretation is not binding on the Court.

[139] For example, the Commissioner refers to the parliamentary business for the Act's reform and to the report by the Standing Committee on Access to Information, Privacy and Ethics dated June 2009 to support his claim that the expression *relates directly* includes a necessity test (paragraph 25 of his memorandum). In fact, as part of the parliamentary business for the Act's reform, the Department of Justice took the position that section 4 need not be amended to include a necessity test because the test was already contained therein. The Department of Justice's legal representative provided the following explanation: "[t]he Treasury Board guidelines have said this expression 'unless it relates directly' should mean a necessity test. Arguably, that's the only legal interpretation that's possible. If we say you shall not collect information unless it directly relates to a program, then basically it's saying you can't collect information you don't need".

[140] The Commissioner also refers to an *obiter* of this Court in *Canada (Privacy Commissioner) v Canada (Labour Relations Board)*, [1996] 3 FCR 609, which states: "[t]he Act limits the collection of private information by government to what is necessary for its operations" (at para 94).

[141] However, the Court finds that the ordinary meaning of the words *relates directly* is clearly not *necessary*. Because the words must be given their ordinary meaning and because it would have been easy for Parliament to use the word *necessary* and to create a necessity test, the Court finds that that was not Parliament's intent. Despite the arguments of the Union and the Commissioner, the Court finds that section 4 does not contain a necessity test, but a less onerous test of establishing a direct, immediate relationship with no intermediary between the

information collected and the operating programs or activities of the government. This interpretation considers the purpose of the Act, which is to protect the personal information of individuals within defined parameters, specifying the circumstances in which that information can be collected (*Lavigne* at para 27). The parameters are defined in section 4, which allows government institutions to collect personal information “that relates directly to an operating program or activity of the institution”, and not “that is necessary” to an operating program or activity of the institution.

[142] The information collected, that is, the information in an individual’s credit report, has been described in detail above. The activities involved are related to security screening, to ensure government security, that is, the safety and protection of the public, staff, inmates and the institution as well as the functional supervision of activities for CSC.

[143] With this in mind, the Court finds that there is a direct relationship between the information collected and the activities of the government. Correctional officers are in direct daily contact with individuals located inside penitentiaries and out in the community. These two groups are likely to put pressure on correctional officers. The information in correctional officers’ credit reports thus contributes to assessing their trustworthiness and vulnerability.

[144] As a result, CSC’s decision to adopt paragraph 3(d) of the Directive, which includes the Inquiry as a security screening activity for the reliability status of correctional officers is reasonable, and the provision does not violate section 4 of the Act.

VI. Conclusion

[145] In light of the foregoing, the decisions of the Treasury Board and CSC are reasonable. The part of the Standard's Appendix B that concerns a financial inquiry and paragraph 3(d) of the Directive are not contrary to section 8 of the Charter, and paragraph 3(d) of the Directive is not contrary to section 4 of the Act.

**JUDGMENT**

**THIS COURT’S JUDGMENT is that:**

1. The application for judicial review is dismissed.
2. Costs are awarded in favour of the respondent.

“Martine St-Louis”

---

Judge



## ANNEX

### *Standard on Security Screening, Appendix B*

### *Norme sur le filtrage de sécurité, Annexe B*

#### **1. Security Screening Model**

#### **1. Modèle de filtrage de sécurité**

Security screening requirements are determined by the duties to be performed and by the sensitivity of information, assets or facilities to be accessed, and in accordance with the Position Analysis tool and guidance issued by the Secretariat.

Les exigences en matière de filtrage de sécurité sont déterminées compte tenu des tâches à exécuter et du caractère délicat des informations, des biens ou des installations auxquels l'accès est requis, et conformément à l'outil d'analyse des postes et des orientations émis par le Secrétariat.

Standard screening is conducted for all duties or positions in the federal government and for other individuals with whom there is a need to share or provide access to sensitive or classified information, assets or facilities, when responsibilities do not relate to security and intelligence functions.

Le filtrage ordinaire est effectué pour toutes les fonctions ou tous les postes au sein du gouvernement fédéral et à l'égard de tout autre particulier à qui il faut communiquer ou donner accès à des informations délicates, des biens ou des installations, lorsque les responsabilités ne se rapportent pas à des fonctions de sécurité ou de renseignement de sécurité.

Enhanced screening is conducted in limited and specific circumstances, and in accordance with the following criteria:

Le filtrage approfondi est effectué dans des circonstances précises et limitées, conformément aux critères suivants:

- When duties or positions involve, or directly support, security and intelligence (S&I) functions, including access to sensitive law

- lorsque les fonctions ou les postes impliquent des activités liées à la sécurité et au renseignement de sécurité (S et R) ou

enforcement or intelligence-related operational information, (i.e., sources or methodologies);

appuient directement celles-ci, y compris l'accès à des informations opérationnelles de nature délicate liées à l'exécution de la loi ou au renseignement de sécurité (sources ou méthodologies);

•When duties or positions involve direct joint operational activity with S&I departments or agencies;

•lorsque les fonctions ou les postes comportent des activités opérationnelles conjointes et directes avec des ministères ou organismes de S et R;

•When duties or positions involve the provision of services to S&I departments or agencies which include management of, or access to, an aggregate of S&I information; or

•lorsque les fonctions ou les postes impliquent la fourniture de services aux ministères et organismes de S et R qui comportent la gestion d'ensembles de renseignements de S et R, ou l'accès à ceux-ci; ou

•When duties or positions, and related access to sensitive information, create a high risk that an individual may be influenced by criminal or ideologically motivated persons or organizations.

•lorsque les fonctions ou les postes, et l'accès à des informations délicates, entraînent un risque élevé qu'un particulier soit susceptible d'être influencé par des personnes ou organisations criminelles ou qui ont des motivations idéologiques.

There are three levels of security screening: reliability status, Secret security clearance, and Top Secret security clearance. Whenever the terms "status" or "clearance" are used, they encompass both standard and enhanced screening, unless otherwise specified.

Il existe trois niveaux de filtrage de sécurité : la cote de fiabilité, l'autorisation de sécurité de niveau Secret et l'autorisation de sécurité de niveau Très secret. À moins d'indication contraire, les termes « cote » ou « autorisation » désignent le filtrage ordinaire et le filtrage approfondi.

The following table describes the standard and enhanced security screening activities.

Le tableau suivant décrit les activités de filtrage de sécurité ordinaire et approfondi.

<b>Reliability Status</b>	<b>Secret Clearance</b>	<b>Top Secret Clearance</b>
5 year background information <ul style="list-style-type: none"> <li>• Verification of identity and background</li> <li>• Verification of educational and professional credentials</li> <li>• Personal and professional references</li> <li>• Financial inquiry (credit check)</li> <li>• Law enforcement inquiry (criminal record check)</li> </ul>	10 year background information <ul style="list-style-type: none"> <li>• Reliability status</li> <li>• CSIS security assessment</li> </ul>	10 year background information + foreign travel, foreign assets, character references, education, military service <ul style="list-style-type: none"> <li>• Reliability status / Secret clearance</li> <li>• CSIS security assessment</li> </ul>
<b>Enhanced</b> <ul style="list-style-type: none"> <li>• Law enforcement inquiry (Law enforcement record check (LERC))</li> <li>• Security questionnaire</li> </ul>		<b>Enhanced</b> <ul style="list-style-type: none"> <li>• Security questionnaire and/or security interview</li> <li>• Open source inquiry</li> </ul>

<p>and/or security interview</p> <ul style="list-style-type: none"> <li>• Open source inquiry</li> </ul>		<ul style="list-style-type: none"> <li>• CSIS security assessment</li> <li>• Polygraph examination</li> </ul>
<p>Validity Period 10 years</p>	<p>Validity Period 10 years</p>	<p>Validity Period 5 years</p>
<p><b>Cote de fiabilité</b></p>	<p><b>Autorisation de niveau Secret</b></p>	<p><b>Autorisation de niveau Très secret</b></p>
<p><i>Contexte de cinq ans</i></p> <ul style="list-style-type: none"> <li>• Vérification de l'identité et des antécédents</li> <li>• Confirmation des titres de scolarité et des désignations professionnelles</li> <li>• Vérification des références personnelles et professionnelles</li> <li>• Enquête sur la situation financière (vérification de crédit)</li> <li>• Enquête sur l'exécution de la loi (vérification du casier judiciaire)</li> </ul>	<p><i>Contexte de 10 ans</i></p> <ul style="list-style-type: none"> <li>• Cote de fiabilité</li> <li>• Évaluation de la sécurité par le SCRS</li> </ul>	<p><i>Contexte de 10 ans + déplacements, biens à l'étranger, références morales, études, service militaire</i></p> <ul style="list-style-type: none"> <li>• Cote de fiabilité/Autorisation de niveau Secret</li> <li>• Évaluation de la sécurité par le SCRS</li> </ul>

<p><b>Approfondi</b></p> <ul style="list-style-type: none"> <li>• Enquête sur l'exécution de la loi (vérification des documents sur le respect de la loi)</li> <li>• Questionnaire sur la sécurité et/ou entrevue sur la sécurité</li> <li>• Enquête de sources ouvertes</li> </ul>		<p><b>Approfondi</b></p> <ul style="list-style-type: none"> <li>• Questionnaire sur la sécurité et/ou entrevue sur la sécurité</li> <li>• Enquête de sources ouvertes</li> <li>• Évaluation de la sécurité par le SCRS</li> <li>• Test polygraphique</li> </ul>
<p><b>Période de Validité</b></p> <p>10 ans</p>	<p><b>Période de Validité</b></p> <p>10 ans</p>	<p><b>Période de Validité</b></p> <p>5 ans</p>

***Commissioner's Directive 564-1 – Directive du commissaire 564-1 – Individual Security Screening Filtrages de sécurité sur les personnes***

3. The Departmental Security Officer has the following responsibilities:

...

d. ensure that criminal record checks, credit checks, law enforcement record checks, open source inquiries and Canadian Security Intelligence Service (CSIS) security assessments, as appropriate, are conducted at the national level

4. Managers will :

...

h. provide the individual with an

3. L'agent de sécurité du Ministère a les responsabilités suivantes :

[...]

d. veiller à ce que des vérifications du casier judiciaire, des vérifications du crédit, des vérifications des documents sur le respect de la loi, des enquêtes de sources ouvertes et des évaluations de la sécurité par le Service canadien du renseignement de sécurité (SCRS), selon le cas, soient effectuées à l'échelle nationale

4. Les gestionnaires :

[...]

h. donneront à la personne

opportunity to explain any adverse information

l'occasion d'expliquer toute information défavorable la concernant

***Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11***

***Charte canadienne des droits et libertés, partie I de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11***

1. The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

1. La Charte canadienne des droits et libertés garantit les droits et libertés qui y sont énoncés. Ils ne peuvent être restreints que par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique.

8. Everyone has the right to be secure against unreasonable search or seizure.

8. Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

***Privacy Act, RSC 1985, c P-21***

***Loi sur la protection des renseignements personnels, LRC (1985), ch P-21***

4 No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

4 Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités.

5 (1) A government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where personal information may be disclosed to the institution

5 (1) Une institution fédérale est tenue de recueillir auprès de l'individu lui-même, chaque fois que possible, les renseignements personnels destinés à des fins administratives le concernant, sauf autorisation contraire de l'individu ou autres cas d'autorisation prévus au paragraphe 8(2).

under subsection 8(2).

(2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.

(3) Subsections (1) and (2) do not apply where compliance therewith might

(a) result in the collection of inaccurate information; or

(b) defeat the purpose or prejudice the use for which information is collected.

29 (1) Subject to this Act, the Privacy Commissioner shall receive and investigate complaints

...

(h) in respect of any other matter relating to

(i) the collection, retention or disposal of personal information by a government institution,

(ii) the use or disclosure of personal information under the control of a government institution, or

(iii) requesting or obtaining access under subsection 12(1) to personal information.

41 Any individual who has been refused access to personal

(2) Une institution fédérale est tenue d'informer l'individu auprès de qui elle recueille des renseignements personnels le concernant des fins auxquelles ils sont destinés.

(3) Les paragraphes (1) et (2) ne s'appliquent pas dans les cas où leur observation risquerait :

a) soit d'avoir pour résultat la collecte de renseignements inexacts;

b) soit de contrarier les fins ou de compromettre l'usage auxquels les renseignements sont destinés.

29 (1) Sous réserve des autres dispositions de la présente loi, le Commissaire à la protection de la vie privée reçoit les plaintes et fait enquête sur les plaintes :

[...]

h) portant sur toute autre question relative à :

(i) la collecte, la conservation ou le retrait par une institution fédérale des renseignements personnels,

(ii) l'usage ou la communication des renseignements personnels qui relèvent d'une institution fédérale,

(iii) la demande ou l'obtention de renseignements personnels en vertu du paragraphe 12(1)

41 L'individu qui s'est vu refuser communication de renseignements

information requested under subsection 12(1) may, if a complaint has been made to the Privacy Commissioner in respect of the refusal, apply to the Court for a review of the matter within forty-five days after the time the results of an investigation of the complaint by the Privacy Commissioner are reported to the complainant under subsection 35(2) or within such further time as the Court may, either before or after the expiration of those forty-five days, fix or allow.

***Financial Administration Act,  
RSC 1985, c F-11***

7 (1) The Treasury Board may act for the Queen's Privy Council for Canada on all matters relating to

(a) general administrative policy in the federal public administration;

...

(e) human resources management in the federal public administration, including the determination of the terms and conditions of employment of persons employed in it

***Policy on Government Security***

3. Context

3.1 Government security is the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence. The extent to which

personnels demandés en vertu du paragraphe 12(1) et qui a déposé ou fait déposer une plainte à ce sujet devant le Commissaire à la protection de la vie privée peut, dans un délai de quarante-cinq jours suivant le compte rendu du Commissaire prévu au paragraphe 35(2), exercer un recours en révision de la décision de refus devant la Cour. La Cour peut, avant ou après l'expiration du délai, le proroger ou en autoriser la prorogation.

***Loi sur la gestion des finances  
publiques, LRC (1985), ch F-11***

7 (1) Le Conseil du Trésor peut agir au nom du Conseil privé de la Reine pour le Canada à l'égard des questions suivantes:

a) les grandes orientations applicables à l'administration publique fédérale ;

[...]

e) la gestion des ressources humaines de l'administration publique fédérale, notamment la détermination des conditions d'emploi

***Politique sur la sécurité du  
gouvernement***

3. Contexte

3.1 La sécurité du gouvernement, c'est l'assurance que l'information, les biens et les services ne sont pas compromis et que les personnes sont protégées contre la violence en milieu de travail. La



government can ensure its own security directly affects its ability to ensure the continued delivery of services that contribute to the health, safety, economic well-being and security of Canadians.

mesure dans laquelle le gouvernement peut assurer sa propre sécurité influe directement sur sa capacité de garantir que les services qui contribuent à la santé, à la sécurité et au mieux-être économique des Canadiennes et des Canadiens continuent d'être fournis.

3.2 Security begins by establishing trust in interactions between government and Canadians and within government. In its interactions with the public when required, the government has a need to determine the identity of the individuals or institutions. Within government, there is a need to ensure that those having access to government information, assets and services are trustworthy, reliable and loyal. Consequently, a broad scope of government activities, ranging from safeguarding information and assets to delivering services, benefits and entitlements to responding to incidents and emergencies, rely upon this trust.

3.2 La sécurité commence en établissant une confiance dans les interactions impliquant le gouvernement et les Canadiens ainsi que dans celles prenant place au sein du gouvernement lui-même. Dans ses interactions avec la population, comme requise, le gouvernement a besoin de connaître l'identité de la personne ou de l'institution avec laquelle il transige. Au sein du gouvernement, il est nécessaire de veiller à ce que les personnes qui ont accès aux renseignements, aux biens et aux services gouvernementaux soient dignes de confiance, fiables et loyales. Ainsi, un large éventail d'activités gouvernementales, qu'il s'agisse de protéger l'information et les biens, de fournir des services, des prestations ou des indemnités, ou encore d'intervenir en cas d'incident ou d'urgence, reposent sur ce lien de confiance.

3.3 In a department, the management of security requires the continuous assessment of risks and the implementation, monitoring and maintenance of appropriate internal management controls involving prevention (mitigation), detection, response and recovery. The management of security intersects with other

3.3 Dans un ministère, la gestion de la sécurité exige une évaluation continue des risques ainsi que la mise en place, la surveillance et le maintien de mécanismes appropriés de contrôle de gestion interne en matière de prévention (atténuation), de détection, d'intervention ou de rétablissement. La gestion de la

management functions including access to information, privacy, risk management, emergency and business continuity management, human resources, occupational health and safety, real property, materiel management, information management, information technology (IT) and finance. Security is achieved when it is supported by senior management—an integral component of strategic and operational planning—and embedded into departmental frameworks, culture, day-to-day operations and employee behaviours.

3.4 At a government-wide level, security threats, risks and incidents must be proactively managed to help protect the government's critical assets, information and services, as well as national security. Advice, guidance and services provided by lead security agencies support departments and government in maintaining acceptable levels of security while achieving strategic goals and service delivery imperatives.

3.5 The management of security is most effective when it is systematically woven into the business, programs and culture of

sécurité recoupe d'autres fonctions de gestion, dont l'accès à l'information, la protection des renseignements personnels, la gestion du risque, la gestion des urgences et de la poursuite des activités, la gestion des ressources humaines, la santé et la sécurité au travail, l'immobilier, la gestion du matériel, la gestion de l'information, les technologies de l'information (TI) et les finances. La sécurité est assurée lorsqu'elle est appuyée par la haute direction, une dimension qui fait partie intégrante de la planification stratégique et opérationnelle, et qu'elle est intégrée aux cadres, à la culture et aux activités courantes des ministères ainsi qu'aux comportements des employés.

3.4 À l'échelle d'un gouvernement, il faut gérer les menaces à la sécurité, les risques et les incidents de façon proactive pour faciliter la protection des biens, des renseignements et des services critiques du gouvernement, et assurer, dans le même temps, la sécurité nationale. Les conseils, l'orientation et les services que fournissent les principaux organismes responsables de la sécurité aident les ministères et le gouvernement à maintenir des niveaux acceptables de sécurité tout en réalisant les objectifs stratégiques et en satisfaisant aux impératifs liés à la prestation de services.

3.5 La gestion de la sécurité est la plus efficace lorsqu'elle fait partie intégrante des activités, des programmes et de la culture d'un

a department and the public service as a whole.

ministère et de la fonction publique dans son ensemble.

3.6 Deputy heads are accountable for the effective implementation and governance of security and identity management within their departments and share responsibility for the security of government as a whole. This comprises the security of departmental personnel, including those working in or for offices of Ministers or Ministers of State, and departmental information, facilities and other assets.

3.6 Les administrateurs généraux sont responsables de la mise en œuvre et de l'administration efficace de la gestion de la sécurité et de l'identité au sein de leur ministère, et ils partagent la responsabilité d'assurer la sécurité du gouvernement dans son ensemble. Ces responsabilités englobent la sécurité du personnel ministériel, y compris des personnes qui travaillent dans les cabinets de ministres ou de ministres d'État, ou pour ceux-ci, ainsi que des renseignements, des installations et des autres biens des ministères.

3.7 Ministers of the Crown, ministers, and Ministers of State are responsible for the security of their staff and offices as well as the security of sensitive information and assets in their custody, as directed by the prime minister.

3.7 Les ministres d'État, ministres et ministres d'État sont responsables de la sécurité de leur personnel et de leurs bureaux ainsi que de la sécurité des renseignements et des biens de nature délicate dont ils ont la garde, conformément aux directives du premier ministre.

3.8 This policy is issued under section 7 of the FAA.

3.8 La présente politique est émise en vertu de l'article 7 de la LGFP.

3.9 Treasury Board has delegated to the President of the Treasury Board the authority to amend directives that support the policy in the following subject areas:

3.9 Le Conseil du Trésor a délégué au Président du Conseil du Trésor le pouvoir de modifier les directives qui appuient la politique dans les domaines suivants :

- Departmental security management
- Identity management

- la gestion de la sécurité ministérielle;
- la gestion de l'identité;

and to issue and amend standards

et de diffuser et de modifier les

that support the policy in the following subject areas:

- Information and identity assurance
- Individual security screening
- Physical security
- IT Security
- Emergency and business continuity management
- Security in contracting

3.10 This policy is to be read in conjunction with the Foundation Framework for Treasury Board Policies, the Directive on Departmental Security Management and the Directive on Identity Management.

## 5. Policy statement

5.1 The objectives of this policy are to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management.

5.2 The expected results of this policy are:

- Information, assets and services are safeguarded from compromise and employees are protected against workplace violence;
- Governance structures, mechanisms and resources are in place to ensure effective and

normes qui appuient la politique dans les domaines suivants :

- l'assurance de l'information et de l'identité;
- les enquêtes de sécurité;
- la sécurité matérielle;
- la sécurité des TI;
- la gestion des urgences et de la continuité des activités;
- la sécurité des marchés.

3.10 La présente politique doit être lue en parallèle avec le Cadre principal des politiques du Conseil du Trésor, la Directive sur la gestion de la sécurité ministérielle, et la Directive sur la gestion de l'identité.

## 5. Énoncé de la politique

5.1 La présente politique a pour objectif de veiller à ce que les administrateurs généraux gèrent efficacement les activités de sécurité au sein des ministères et contribuent à la gestion efficace de la sécurité à l'échelle du gouvernement.

5.2 Les résultats escomptés de la présente politique sont les suivants :

- l'information, les biens et les services ne sont pas compromis et les employés sont protégés contre la violence en milieu de travail;
- les structures, mécanismes et ressources de gouvernance sont en place pour assurer la gestion

efficient management of security at both a departmental and government-wide level;

- Management of security incidents is effectively coordinated within departments and government-wide;

- Interoperability and information exchange are enabled through effective and consistent security and identity management practices; and

- Continuity of government operations and services is maintained in the presence of security incidents, disruptions or emergencies.

## 6. Requirements

6.1 Deputy heads of all departments are responsible for:

6.1.1 Establishing a security program for the coordination and management of departmental security activities that:

a. Has a governance structure with clear accountabilities

b. Has defined objectives that are aligned with departmental and government-wide policies, priorities and plans; and

c. Is monitored, assessed and reported on to measure management efforts, resources and success toward achieving its

efficace et efficiente de la sécurité, tant au sein d'un ministère que dans l'ensemble du gouvernement;

- la gestion des incidents de sécurité est efficacement coordonnée au sein des ministères et dans l'ensemble du gouvernement;

- l'interopérabilité et l'échange de renseignements sont assurés au moyen de pratiques efficaces et uniformes en matière de gestion de la sécurité et de l'identité;

- la continuité des activités et des services du gouvernement est assurée en cas d'incidents de la sécurité, de perturbations ou de situations d'urgence.

## 6. Exigences

6.1 Les administrateurs généraux de tous les ministères sont responsables de ce qui suit:

6.1.1 Mettre sur pied un programme de sécurité afin d'assurer la coordination et la gestion des activités ministérielles liées à la sécurité qui :

a. repose sur une structure de gouvernance assortie de responsabilités claires;

b. comporte des objectifs précis qui cadrent avec les politiques, les priorités et les plans ministériels et pangouvernementaux;

c. est suivi, évalué et fait l'objet de rapports afin de mesurer les efforts, les ressources et les réussites de la direction à l'égard

<p>expected results;</p>	<p>de l'atteinte des résultats escomptés;</p>
<p>6.1.2 Appointing a departmental security officer (DSO) functionally responsible to the deputy head or to the departmental executive committee to manage the departmental security program (Note: The deputy head of a small department or agency (SDA) can assume the role of DSO);</p>	<p>6.1.2 Nommer un agent de sécurité du ministère (ASM) relevant de l'administrateur général ou du comité exécutif ministériel pour gérer le programme de sécurité du ministère (Nota : l'administrateur général d'un petit ministère ou organisme (PMO) peut occuper le rôle de l'ASM);</p>
<p>6.1.3 Establishing a formal arrangement with the service provider when the role of the DSO is fulfilled by a third party (e.g., shared or clustered service provider or a portfolio department);</p>	<p>6.1.3 Prendre un arrangement formel avec le fournisseur de services quand le rôle de l'ASM est occupé par un tiers (p. ex., un fournisseur de services partagés ou regroupés ou un ministère responsable du portefeuille).</p>
<p>6.1.4 Approving the departmental security plan that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security and supporting its implementation;</p>	<p>6.1.4 Approuver le programme de sécurité ministérielle qui détaille les décisions en matière de gestion de risques liés à la sécurité et expose les stratégies, les buts, les objectifs et les échéanciers élaborés en vue d'améliorer la sécurité ministérielle et de favoriser sa mise en œuvre;</p>
<p>6.1.5 Ensuring that managers at all levels integrate security and identity management requirements into plans, programs, activities and services;</p>	<p>6.1.5 S'assurer que les gestionnaires de tous niveaux intègrent les exigences relatives à la gestion de la sécurité et de l'identité aux plans, aux programmes, aux activités et aux services;</p>
<p>6.1.6 Ensuring that all individuals who will have access to government information and assets, including those who work in or for offices of Ministers and Ministers of State, are security screened at the appropriate level</p>	<p>6.1.6 Veiller à ce que toutes les personnes qui auront accès aux renseignements et aux biens du gouvernement, y compris les personnes qui travaillent dans les cabinets de ministres ou de ministres d'État ou pour ceux-ci,</p>

before the commencement of their duties and are treated in a fair and unbiased manner;

fassent l'objet d'une enquête de sécurité appropriée avant de commencer leur travail et soient traitées de manière juste et impartiale;

6.1.7 Ensuring that their authority to deny, revoke or suspend security clearances is not delegated;

6.1.7 Veiller à ce que leur pouvoir de refuser, de révoquer ou de suspendre les autorisations de sécurité ne soit pas délégué;

6.1.8 Ensuring that when significant issues arise regarding policy compliance, allegations of misconduct, suspected criminal activity, security incidents, or workplace violence they are investigated, acted on and reported to the appropriate law enforcement authority, national security agency or lead security agency.

6.1.8 S'assurer que les enjeux importants concernant la conformité à la politique, les allégations d'inconduite, les activités criminelles soupçonnées, les incidents liés à la sécurité ou la violence en milieu de travail fassent l'objet d'une enquête, d'une intervention et d'un signalement à l'organisme approprié chargé de l'application de la loi, à l'organisme de sécurité nationale ou à l'organisme principal responsable de la sécurité;

6.2 Deputy heads of lead security agencies are responsible for:

6.2 Les administrateurs généraux des principaux organismes responsables de la sécurité sont responsables de ce qui suit :

6.2.1 Providing departments with advice, guidance and services related to government security, consistent with their mandated responsibilities;

6.2.1 Fournir aux ministères des conseils, de l'orientation et des services liés à la sécurité du gouvernement, conformément aux responsabilités qui leur sont confiées;

6.2.2 Appointing an executive or executives to coordinate and oversee the provision of support services to departments and to represent the deputy head to TBS in this regard; and

6.2.2 Nommer un ou plusieurs cadres qui seront chargés de coordonner et de superviser la prestation de services de soutien aux ministères et de représenter l'administrateur général auprès du SCT à cet égard;

6.2.3 Ensuring that the security support services provided help government departments achieve and maintain an acceptable state of security and readiness and that those services remain aligned with government-wide policies, priorities and plans related to government security.

- A list of lead security agencies and details on the nature and scope of their responsibilities under this policy are found in Appendix B—Responsibilities of Lead Security Agencies.

### 6.3 Monitoring and reporting requirements

Within departments

- Deputy heads are responsible for ensuring that periodic reviews are conducted to assess whether the departmental security program is effective, whether the goals, strategic objectives and control objectives detailed in their departmental security plan were achieved and whether their departmental security plan remains appropriate to the needs of the department and the government as a whole.

By departments

- Deputy heads are responsible for reporting periodically to TBS, on the status and progress of implementation of this policy and on the results of ongoing

6.2.3 Veiller à ce que les services de soutien à la sécurité qui sont fournis aident les ministères à atteindre et à maintenir un état acceptable de sécurité et de préparation et à ce que ces services concordent toujours avec les politiques, priorités et plans pangouvernementaux ayant trait à la sécurité du gouvernement;

- L'annexe B – Responsabilités des principaux organismes responsables de la sécurité, dresse une liste des principaux organismes responsables de la sécurité et fournit des précisions sur la nature et la portée de leurs responsabilités aux termes de la présente politique.

### 6.3 Surveillance et déclaration

Au sein des ministères

- Les administrateurs généraux doivent veiller à ce que l'on procède à des examens périodiques pour déterminer si le programme de sécurité ministérielle est efficace, si les buts, les objectifs stratégiques et les objectifs de contrôle précisés dans leur plan de sécurité ministérielle ont été atteints, et si ce plan continue de répondre aux besoins du ministère et du gouvernement dans son ensemble.

Par les ministères

- Les administrateurs généraux doivent faire rapport périodiquement au SCT sur la situation et l'état d'avancement de la mise en œuvre de la présente



performance measurement.

politique et sur les résultats concernant la mesure continue du rendement.

Lead security agencies

Principaux organismes responsables de la sécurité

• In addition to monitoring and reporting on their departmental security program Deputy heads of lead security agencies are also responsible for:

• En plus de surveiller leur programme de sécurité ministérielle et d'en rendre compte, les administrateurs généraux des principaux organismes responsables de la sécurité sont également responsables de ce qui suit :

• Ensuring that periodic reviews are conducted to assess the effectiveness of their security support services to ensure they continue to meet the needs of departments and the government as a whole; and

• s'assurer que l'on procède à des examens périodiques en vue d'évaluer l'efficacité de leurs services de soutien à la sécurité afin de veiller à ce que ces services continuent de répondre aux besoins des ministères et du gouvernement dans son ensemble;

• Reporting on their activities under this policy through current government reporting mechanisms, e.g., Management, Resources and Results Structure (MRRS), departmental performance reports (DPR) and reports on plans and priorities (RPP).

• rendre compte des activités qu'ils mènent en vertu de la présente politique, au moyen des mécanismes actuels de rapport du gouvernement, comme la Structure de gestion des ressources et des résultats, les rapports ministériels sur le rendement (RMR) et les rapports sur les plans et les priorités (RPP).

Government-wide

À l'échelle du gouvernement

• TBS is responsible for:

• Le SCT est responsable de ce qui suit :

• Monitoring compliance with this policy and the achievement of expected results in a variety of ways, including but not

• surveiller la conformité à la présente politique et l'atteinte des résultats escomptés de diverses manières, y compris, sans

limited to MAF assessments, Treasury Board submissions, DPRs, RPPs, results of audits, evaluations and studies, and ongoing dialogue and committee work; and

s'y limiter, au moyen d'évaluations fondées sur le Cadre de responsabilisation de gestion, de présentations au Conseil du Trésor, des RMR, des RPP, des résultats des vérifications, des évaluations et des études, ainsi qu'au moyen du dialogue continu et des travaux des comités;

- Reviewing and reporting to Treasury Board on the effectiveness and implementation of this policy and its directives and standards at the five-year mark from the effective date of the policy. Where substantiated by risk analysis, TBS will also ensure an evaluation is conducted.

- examiner l'efficacité et la mise en œuvre de la présente politique ainsi que de ses directives et normes cinq ans après la date d'entrée en vigueur de la politique, et en rendre compte au Conseil du Trésor. Si une analyse des risques le justifie, le SCT veillera aussi à ce qu'une évaluation soit réalisée.

***Act respecting the protection of personal information in the private sector, CQLR, c P-39.1***

***Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ, ch P-39.1***

5. Any person collecting personal information to establish a file on another person or to record personal information in such a file may collect only the information necessary for the object of the file.

5. La personne qui recueille des renseignements personnels afin de constituer un dossier sur autrui ou d'y consigner de tels renseignements ne doit recueillir que les renseignements nécessaires à l'objet du dossier.

Such information must be collected by lawful means.

Ces renseignements doivent être recueillis par des moyens licites.

**FEDERAL COURT**

**SOLICITORS OF RECORD**

**DOCKET:** T-699-15

**STYLE OF CAUSE:** UNION OF CANADIAN CORRECTIONAL  
OFFICERS - SYNDICAT DES AGENTS  
CORRECTIONNELS DU CANADA - CSN v  
ATTORNEY GENERAL OF CANADA AND  
PRIVACY COMMISSIONER OF CANADA

**PLACE OF HEARING:** MONTRÉAL, QUEBEC

**DATE OF HEARING:** JUNE 22, 2016

**JUDGMENT AND REASONS:** ST-LOUIS J.

**DATED:** NOVEMBER 23, 2016

**APPEARANCES:**

Catherine Quintal FOR THE APPLICANT  
Ioanna Egarhos

Claude Joyal FOR THE RESPONDENT  
Paul Deschênes

Sylvian Lussier FOR THE INTERVENER  
Regan Morris  
Sarah Speevak

**SOLICITORS OF RECORD:**

Laroche Martin FOR THE APPLICANT  
Confédération des syndicats  
nationaux  
Montréal, Quebec

William F. Pentney FOR THE RESPONDENT  
Deputy Attorney General of Canada  
Montréal, Quebec

Osler, Hoskin & Harcourt FOR THE INTERVENER  
Montréal, Quebec  
Privacy Commissioner of Canada  
Gatineau, Quebec