AECL EACL

# Évaluation de base des facteurs relatifs à la vie privée pour :

## Système d’identification en temps réel

Énergie atomique du Canada limitée
Bureau de l’accès à l’information et de la protection des renseignements personnels

Mai 2013

# ÉVALUATION DE BASE DES FACTEURS RELATIFS À LA VIE PRIVÉE

## Table des matières

# Références


1. Directive sur l'évaluation des facteurs relatifs à la vie privée, SCT, 1er avril 2010 http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=18308
2. Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle, Commissariat à la protection de la vie privée du Canada, novembre 2010.
3. Publications Info Source, Sources de renseignements du gouvernement fédéral et sur les fonctionnaires fédéraux pour 2010, SCT, http://www.infosource.gc.ca/emp/emp00-fra.asp
4. Directive sur les pratiques relatives à la protection de la vie privée, SCT, 1er avril 2010, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=18309
5. Politique sur la protection de la vie privée, SCT, 1er avril 2008, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=12510
6. Norme sur la sécurité du personnel, SCT, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12330&section=text
7. Sommaire de l'évaluation des facteurs relatifs àa la vie privée – Système d'identification en temps réel, Gendarmerie royale du Canada, http://www.rcmp-grc.gc.ca/pia-efvp/rtid-pia-itr-efpv-fra.htm
8. *Loi sur la protection des renseignements personnels* (L.R.C, 1985, ch.P-21), ministère de la Justice, http://laws-lois.justice.gc.ca/fra/lois/P-21/
9. *Loi sur le Service canadien du renseignement de sécurité*, 31 août 2004, http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp
10. *La loi sur la sûreté et la réglementation nucléaires*, 31 mai 2000, http://laws-lois.justice.gc.ca/fra/lois/N-28.3/index.html
11. Retention Scheduling policy d'EACL, CW-511300-012-414 Rév. 0
12. Guide de l'utilisateur du système d'identification en temps réel, version 1.0
13. Real Time Identification Technical Guidelines for Agencies, GRC, 2009-05-15
14. RTID SMTP-NIST Message Guidelines, GRC, 2008-04-18
15. RTID Best Practices for the Implementation of Civil Electronic Fingerprint Capture Devices Workflows, GRC, 2009-05-19
16. RTID Security Policy and Guidelines for Non-Law-Enforcement Agencies, GRC, 2009-08-31
17. RTID Introduction for Agencies, GRC, 2009-01-19
18. Document de contrôle d'interface NIST (National Institute of Standards and Technology) des services nationaux de police pour les collaborateurs externes, GRC, DCI NIST des SNP, 2010-07-30, version 1.7.7 Rév. E2

# Acronymes et abréviations

| **Acronyme / Abréviation** | **Définition** |
|---|---|
| EACL | Énergie atomique du Canada limitée |
| AIPRP | Accès à l'information et protection des renseignements personnels |
| ASFC | Agence des services frontaliers du Canada |
| VECJ | Vérification de l'existence d'un casier judiciaire |
| CCSN | Commission canadienne de sûreté nucléaire |
| CIPC | Centre d'information de la police canadienne |
| LCR | Laboratoires de Chalk River |
| CSIS | Service canadien du renseignement de sécurité |
| LGFP | *Loi sur la gestion des finances publiques* |
| RH | Ressources humaines |
| TI | Technologie de l'information |
| PE | Protocole d'entente |
| NIST | National Institute of Standards in Technology |
| SNP | Services nationaux de police |
| CPVP | Commissariat à la protection de la vie privée |
| AP | Activité de programme |
| AAP | Architecture des activités de programme |
| RP | Renseignements personnels |
| EFVP | Évaluation des facteurs relatifs à la vie privée |
| FRP | Fichier de renseignements personnels |
| ASP | Agent(e) de la sécurité du personnel |
| SSP | Services de sécurité du personnel |
| GRC | Gendarmerie royale du Canada |
| SITR | Système d'identification en temps réel |
| SCS | Système consultatif de sécurité |
| S et T | Sciences et technologies |
| SCT | Secrétariat du Conseil du Trésor |
| EMR | Évaluation des menaces et des risques |

# Sommaire

La collecte de renseignements personnels est indispensable à la réalisation des vérifications de la fiabilité, à l'établissement des autorisations de sécurité et aux vérifications du casier judiciaire. Ces contrôles sont requis afin que les employés d'EACL aient le droit d'accéder à toute aire de travail à laquelle ils ont besoin d'accéder pour exécuter leur travail, et pour qu'ils obtiennent l'autorisation de sécurité appropriée. L'identification en temps réel (ITR) permet la soumission électronique fluide de données dactylaires qui servent aux enquêtes sur la sécurité du personnel d'EACL. Les processus électroniques prévus pour l'ITR sont principalement une refonte technique des services existants, à savoir que les renseignements reçus des candidats ne changeront que très peu. En conséquence, l'EFVP est axée sur deux éléments de programme : la collecte plus intensive de renseignements personnels, des changements majeurs aux processus et/ou aux systèmes qui influent sur la séparation physique ou logique des renseignements personnels, et les mécanismes de sécurité utilisés pour gérer et contrôler l'accès aux renseignements personnels qui ont été reçus par le SITR

Le SITR permet la saisie et le traitement électroniquement des données démographiques et des empreintes digitales de qualité juridique. Le système regroupe les renseignements en des dossiers normalisés de format NIST et les transmet au système de la Gendarmerie royale du Canada (GRC), compatible au système du National Institute of Standards in Technology (NIST).

En automatisant les processus de vérification des empreintes et de vérification du casier judiciaire, le SITR offre une solution aux divers défis auxquels sont actuellement confrontés les Services de vérification de sécurité du personnel d'EACL. Le passage de l'infrastructure actuelle sur papier à un système électronique permettra d'effectuer en seulement quelques heures ce qui auparavant prenait des mois.

Le SITR est également capable de traiter des données classées « Protégé B », ce qui améliore la sécurité et la protection des renseignements personnels connexes. Tous les renseignements personnels échangés avec le SITR seront aussi chiffrés. EACL a obtenu la certification nécessaire à la soumission de ce type de transaction par l'intermédiaire de la GRC.

La portée des travaux compris dans la présente EFVP est la mise en œuvre du SITR. Le système est limité, dans sa portée, à la réception et au traitement de diverses demandes d'identification, et, en particulier, il permettra aux services de sécurité d'EACL de procéder à des enquêtes de sécurité du personnel civil pour son effectif existant et des postulants qui pourraient devenir des employés d'EACL. La portée de la présente EFVP est limitée à l'analyse de la collecte, de l'utilisation, de la conservation et de la divulgation de renseignements personnels au moyen du SITR.

Les renseignements personnels sauvegardés dans le SITR ne sont accessibles qu'aux personnes autorisées d'EACL. Les articles 10 et 11 de la *Loi sur la protection des renseignements personnels* obligent les institutions gouvernementales à saisir dans des fichiers de renseignements personnels (FRP) tous les renseignements en leur possession et qu'elle publie un index de tous les fichiers de renseignements personnels qu'elle possède. Ces renseignements sont recueillis conformément au FRP POU 917 d'AECL. Les dispositions de la *Loi sur la protection des renseignements personnels* relatifs à l'accès aux données, à leur collecte, à leur exactitude, à leur exhaustivité et à leur correction si elles sont incorrectes, sont ici appliquées.

Il est obligatoire d'obtenir le consentement de la personne dont on recueille les empreintes digitales pour les transactions civiles. Ce consentement est obtenu au moyen d'un formulaire de consentement distinct. Les images dactylaires qui se rattachent aux transactions civiles ne sont pas conservées dans le SITR. Elles sont supprimées une fois la transaction terminée.

Le SITR est un système hautement sécurisé qui comprend d'importantes fonctions et procédures relatives à la sécurité. Toute fonctionnalité mise en production fait l'objet d'essais approfondis afin de s'assurer que les résultats générés par le SITR respectent la loi et les politiques en matière de dactyloscopie. De plus, il existe des procédures manuelles et des vérifications régulières qui garantissent que les renseignements communiqués sur une personne donnée sont exacts et transmis uniquement aux entités autorisées.

En conclusion : il est possible de régler les problèmes de sécurité décrits dans cette évaluation des facteurs relatifs à la vie privée (EFVP) en développant et en consignant les procédures et processus appropriés qui garantissent le respect de la *Loi sur la protection des renseignements personnels*. Les données biométriques de nature délicate utilisées dans le SITR serviront uniquement aux fins pour lesquelles elles ont été recueillies. EACL a fait preuve d'un engagement continu envers la sécurité et la protection de son SITR et des renseignements personnels impliqués.

# 1 SECTION I – APERÇU ET INTRODUCTION DE L'EFVP

**Institution gouvernementale**

Énergie atomique du Canada limitée (EACL)

| **Agents responsables de l'évaluation des facteurs relatifs à la vie privée (EFVP)** | **Chef de l'institution fédérale ou son délégué pour l'application de l'article 10 de la *Loi sur la protection des renseignements personnels*** |
|---|---|
| Lee-Anne Johns, coordinatrice du Programme des services de sécurité du personnel<br><br>Jean Boulais, directeur, Accès à l'information et Protection des renseignements personnels | Robert Walker (PhD), président-directeur général |

**Nom du programme ou de l'activité de l'institution gouvernementale**

Services de sécurité du personnel – Système d'identification en temps réel (SITR)

## 1.1 Description du programme ou de l'activité

Les renseignements personnels sont nécessaires à la réalisation des vérifications de sécurité, à l'établissement de cotes de sécurité et à l'exécution des vérifications du casier judiciaire. Ces contrôles sont indispensables afin que les employés d'EACL aient le droit d'accéder à toute aire de travail à laquelle ils ont besoin d'accéder pour exécuter leur travail, et afin qu'ils possèdent l'autorisation de sécurité appropriée. Le SITR permet la transmission électronique fluide des données dactylaires qui serviront aux enquêtes de sécurité du personnel d'EACL. Le SITR permet la saisie et le traitement électroniquement des données démographiques et des empreintes digitales de qualité juridique. Le système regroupe les renseignements en des dossiers normalisés de format NIST et les transmet au système de la Gendarmerie royale du Canada (GRC), compatible au système du National Institute of Standards in Technology (NIST). En automatisant les processus de vérification des empreintes et de vérification du casier judiciaire, le SITR offre une solution aux divers défis auxquels sont actuellement confrontés les Services de vérification de sécurité du personnel d'EACL. Le passage de l'infrastructure actuelle sur papier à un système électronique permettra d'effectuer en seulement quelques heures et journées ce qui auparavant prenait des semaines ou des mois. Le SITR est également capable de traiter des données classées « Protégé B », ce qui améliore la sécurité et la protection des renseignements personnels connexes. Tous les renseignements personnels échangés avec le SITR seront aussi chiffrés.

Alignés sur l'Architecture des activités de programme (AAP) d'EACL, et décrits dans le chapitre d'Info Source pour 2010-2011 d'EACL, les Services de vérification de sécurité du personnel d'EACL exploiteront le SITR sous l'activité de programme (AP) 2001121 Services internes, Vérification de sécurité du personnel, comme suit :

**AP 2001121 –SERVICES INTERNES :** Les Services internes sont des groupes d'activités et de ressources liées qui sont administrées dans le but d'appuyer les besoins des programmes et des autres obligations internes d'une organisation. Ces groupes sont les suivants : Service de gestion et de surveillance, Service des communications, Services juridiques, Service des ressources humaines, Service de gestion financière, Service de gestion de l'information, Service des technologies de l'information, Service des biens immobiliers, Service de gestion du matériel, Service des acquisitions, et Service des voyages d'affaires et autres fonctions administratives. Les services internes comprennent uniquement les activités et les ressources qui s'appliquent à l'ensemble d'une organisation et non celles fournies uniquement à un programme.

**GESTION DES RESSOURCES HUMAINES**

On entend par gestion des ressources humaines des activités visant à déterminer l'orientation stratégique, à affecter les ressources entre les services et les processus, et des activités liées à l'analyse des risques et à la détermination des mesures d'atténuation appropriées à prendre. Elles permettent de veiller à ce que les activités et les programmes du gouvernement fédéral respectent les lois, les règlements, les politiques et les plans applicables.

- Recrutement et dotation
  - Vérification de sécurité du personnel

**VOYAGES ET AUTRES SERVICES ADMINISTRATIFS**

Les Services de voyage et autres services administratifs comprennent les services de voyage du gouvernement du Canada (GC) ainsi que d'autres services internes qui ne s'inscrivent pas logiquement dans les autres catégories de services internes.

- Sécurité
  - Vérification de sécurité du personnel

### 1.2 Description de la catégorie de dossiers qui se rapportent au programme ou à l'activité

Le Bureau de l'accès à l'information et de la protection des renseignements personnels d'EACL doit fournir au Secrétariat du Conseil du Trésor un inventaire complet des fonds de renseignements afin qu'ils soient inclus dans la publication Info Source. Celle-ci contient la description des catégories de documents institutionnels tenus par EACL. Les descriptions des dossiers créés, recueillis et conservés par Vérification de sécurité du personnel se trouvent dans les catégories de dossiers suivantes :

**Recrutement et dotation :**

***Description*** : Comprend des dossiers sur le recrutement de personnes et la dotation de postes à temps plein ou à temps partiel au sein de l'institution. Les documents peuvent inclure des renseignements concernant la présélection, l'interrogation, la mise à l'épreuve, le passage en entrevue, l'évaluation, la sélection, l'embauche et la promotion des candidats. Ils peuvent également inclure des renseignements sur les conditions d'emploi (y compris les conflits d'intérêts), les mutations, les affectations et les détachements, le recrutement d'étudiants, de professionnels et d'employés, les appels d'après-mandat et la zone de sélection, ainsi que des renseignements échangés avec les organismes centraux chargés du recrutement et de la dotation et avec les autres agences de placement.

***Nota :*** L'information pertinente peut être versée au dossier du personnel d'un employé si l'intéressé accepte une offre d'emploi de l'institution.

***Types de documents* :** Curriculum vitæ et résumés non sollicités, modèles de questions et de réponses d'entrevue, affiches et annonces de concours, formulaires de demande d'emploi, outils d'évaluation et guides de notation des concours, procédures de vérification des références, listes de contrôle et lettres de recommandation, répertoires de candidats qualifiés (y compris les bassins de candidats préqualifiés), demandes de renseignements des candidats et réponses, copies des lettres d'offres, évaluations des comités de notation, renseignements inclus dans les outils automatisés ou les outils Web de demande d'emploi, résultats d'évaluation de la langue seconde, etc.

***Numéro de fichier :*** NDP 920

**Sécurité**

***Description :*** Comprend des documents concernant l'utilisation de mesures pour protéger les employés, préserver la confidentialité, l'intégrité, la disponibilité et la valeur des biens et assurer la prestation continue des services à la suite de dommages accidentels ou intentionnels ou d'un accès non autorisé. Les documents peuvent inclure des renseignements concernant la conception des installations, les mesures de protection matérielle, les dispositifs de surveillance, l'accès aux zones à accès restreint, l'entreposage, le transport et la transmission de renseignements et de biens, la violence en milieu de travail, les renseignements protégés et classifiés, les points d'entrée et de sortie, les services d'urgence, la signalisation, les cartes d'identité et/ou les laissez-passer, les enquêtes de sécurité sur les employés, la gestion continue des risques pour la sécurité, les codes du bâtiment et de prévention des incendies et la destruction de renseignements et de biens. Il peut également s'agir de documents concernant les liaisons avec d'autres institutions fédérales ayant des responsabilités en matière de sécurité (p. ex., le Service canadien du renseignement de sécurité, Sécurité publique Canada, la Gendarmerie royale du Canada et le Centre de la sécurité des télécommunications, etc.).

***Types de documents :*** Procédures et outils d'accès sécuritaire (laissez-passer, cartes d'identité), rapports d'enquêtes sur les incidents liés à la sécurité, formation sur la sécurité, exemplaires des évaluations de la menace et des risques, documents de sensibilisation et d'information, dossiers d'autorisations de sécurité, procédures d'intervention en cas d'incident, rapports de vérification du programme de sécurité, exigences sécuritaires de base, plans d'évacuation, normes opérationnelles et documents techniques, analyses des répercussions sur les activités et exemplaires des règlements et des codes pertinents en matière de travail, d'incendie, de bâtiment et d'électricité.

***Numéro de fichier :*** NDP 931

### 1.3 Fichiers de renseignements personnels ordinaires – Vérification de sécurité du personnel

Les articles 10 et 11 de la *Loi sur la protection des renseignements personnels* obligeNT les institutions gouvernementales à saisie dans des fichiers de renseignements personnels (FRP) tous les renseignements en leur possession et qu'elle publie un index de tous les fichiers de renseignements personnels qu'elle possède. Ces renseignements du SITR sont recueillis conformément aux FRP de Vérification de sécurité du personnel, POU 917 d'EACL.

**Vérification de sécurité du personnel**
**Numéro d'inscription SCT –** 7193
***Description :*** Ce fichier décrit les renseignements qui sont reliés aux évaluations des enquêtes de sécurité portant sur des personnes qui travaillent dans une institution gouvernementale ou qui y présentent une demande d'emploi. Les renseignements personnels peuvent comprendre les noms, les coordonnées, les données biographiques, les renseignements biométriques (p. ex. empreintes digitales, photos numériques, etc.), les évaluations de la personnalité (p. ex. loyauté, fidélité, etc.), le statut de citoyen, les renseignements de solvabilité, les vérifications et les antécédents judiciaires, la date de naissance, les renseignements sur les études, le numéro d'identification d'employé, les renseignements personnels d'employés, l'information financière, d'autres numéros d'identification, des opinions ou des points de vue de personnes ou sur des personnes, les signes distinctifs, le lieu de naissance, la signature et les renseignements sur le service militaire. Le fichier peut également décrire des renseignements personnels sur des membres de la famille immédiate, y compris le nom, les coordonnées, la date de naissance et la date de décès, ainsi que le lien avec le demandeur.
***Nota*** : Le ministère de la Défense nationale (MDN), la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS) ont établi les fichiers de renseignements personnels spécifiques aux institutions suivants afin de rendre compte des renseignements utilisés lors des contrôles de sécurité et de fiabilité de leurs propres employés : MDN, « Dossier d'enquête sur la sécurité et vérification relative à la fiabilité » - MDN PPE-834; GRC, « Dossiers de l'habilitation sécuritaire et relative à la fiabilité » - GRC P-PU-065; SCRS, « Cotes de sécurité » - SISP P-PE 815. En outre, Travaux publics et Services gouvernementaux Canada (TPSGC) a établi le fichier de renseignements personnels spécifique aux institutions suivant afin de rendre compte des renseignements utilisés lors des contrôles de sécurité et de fiabilité du personnel du secteur privé : « Autorisations de sécurité et dossiers de fiabilité pour le personnel de l'industrie privée » - TPSGC P-PU-015.
***Catégories de personnes*** : Le grand public, notamment les bénévoles, tous les employés, actuels et anciens, les entrepreneurs, les parents immédiats, les époux ou conjoints de fait actuels et anciens, les organismes, les employés occasionnels et les étudiants, les personnes qui donnent des références morales (notamment des voisins), les employés, anciens et actuels.
***But*** : Les renseignements personnels sont utilisés pour étayer la décision d'accorder la cote de fiabilité, le niveau d'autorisation de sécurité ou l'accès aux lieux, ou d'examiner les causes justifiant leur attribution, relativement aux personnes qui travaillent ou qui souhaitent travailler, dans des situations de nomination, d'affectation ou de contrat. Un examen des causes justifiant l'attribution peut donner lieu à la révocation de la cote de fiabilité, de l'autorisation de sécurité ou de l'accès aux lieux de la personne. Pour de nombreuses institutions, les renseignements personnels sont recueillis conformément au paragraphe 7(1) de la *Loi sur la gestion des finances publiques* (LGFP) et, au besoin, en vertu de la Politique du gouvernement sur la sécurité. Dans le cas des institutions qui ne sont pas assujetties à la LGFP ou à la Politique du gouvernement sur la sécurité, consulter le Coordonnateur de l'accès à l'information de l'institution pour déterminer l'autorité responsable de la collecte
***Usages compatibles*** : Le cas échéant, les renseignements, y compris les empreintes digitales, peuvent être communiqués à la GRC et au SCRS afin d'effectuer les vérifications et/ou les enquêtes requises conformément à la Politique du gouvernement sur la sécurité (veuillez consulter les fichiers de renseignements personnels spécifiques aux institutions suivants : pour la GRC, « Services des sciences judiciaires et de l'identité et les Services canadiens d'identification criminelle en temps réel » - GRC PPU 030, et pour le SCRS, « Évaluations de sécurité/avis » - SRS PPU 005. La cote de sécurité peut être communiquée aux représentants des ressources humaines afin de mettre à jour le dossier personnel d'une personne (veuillez consulter le ficher de renseignements personnels « Dossier personnel d'un employé » - POE 901). Les renseignements peuvent être communiqués à des organismes extérieurs à l'administration fédérale, notamment aux agences de notation du crédit. Certains renseignements peuvent être utilisés ou divulgués aux fins d'évaluation des programmes.
***Normes de conservation et de destruction*** : Pour des renseignements sur la durée de conservation d'un type précis de dossiers administratifs communs par une institution du gouvernement, y compris sur la suppression de ces dossiers, veuillez communiquer avec le coordonnateur de l'accès à l'information et de la protection des renseignements personnels de l'institution.
***Numéro ADD :*** 98/001
***Catégories apparentée du dossier:*** NDP 920 et NDP 931
***Numéro de fichier :*** POU 917 d'EACL

### 1.4 Responsable juridique pour l'activité de programme :

Énergie atomique du Canada limitée a été constituée en société en 1952 en vertu de la *Loi sur les corporations canadiennes* (et a continué en 1977 selon les dispositions de la *Loi canadienne sur les sociétés par action*), aux termes de l'autorité et des pouvoirs conférés au ministre des Ressources naturelles par la *Loi sur l'énergie nucléaire*. Le 1er septembre 2007, la *Loi fédérale sur la responsabilité* a modifié la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels* afin d'inclure EACL.

La société est une société d'État visée par la partie I de l'annexe III de la *Loi sur la gestion des finances publiques* et est un mandataire de Sa Majesté la Reine du chef du Canada. EACL a le pouvoir de recueillir des renseignements personnels dans le but d'établir des autorisations de sécurité en vertu des paragraphes 7(1) et 11.1(1) de la *Loi sur la gestion des finances publiques.*

Les Services de sécurité du personnel d'EACL sont également responsables de procéder à des enquêtes sur le personnel conformément à la Politique du gouvernement sur la sécurité du Secrétariat du Conseil du Trésor du Canada, réf. 2-4 – Norme sur la sécurité du personnel et à l'article 18.1 du *Règlement sur la sécurité nucléaire*.

### 1.5 Sommaire du projet / de l'initiative / du changement

#### Objectifs d'affaire d'EACL

EACL est alignée sur un Résultat stratégique unique : Faire en sorte que les Canadiens et le monde entier bénéficient des retombées positives de la science et de la technologie nucléaires sur le plan de l'énergie, de la santé, de l'environnement et de l'économie, tout en ayant la certitude que la sûreté et la sécurité nucléaires sont garanties.

Fidèle à la stratégique fédérale sur les sciences et la technologie (S et T), EACL contribue à l'avantage du savoir du Canada en travaillant à l'atteinte de ce résultat stratégique. L'avantage du savoir met l'accent sur la recherche dans des domaines qui revêtent une importance stratégique pour l'avenir des Canadiens. Il met également l'accent sur la recherche dans des domaines où le Canada a établi sa force. Sur ces deux aspects, les S et T nucléaires sont bien placées pour améliorer la qualité de vie des Canadiens.

#### Objectifs de l'EFVP

Le présent rapport est une évaluation des facteurs relatifs à la vie privée effectuée pour le système d'identification en temps réel (SITR) acheté par EACL, et qui doit être installé aux Laboratoires de Chalk River et de Whiteshell. L'EFVP garantira que la vie privée est prise en compte tout au long du processus d'achat et de mise en œuvre du SITR. Il s'agit de l'assurance documentée du fait que les questions relatives à la vie privée ont été relevées et résolues de manière adéquate.

Les objectifs de l'EFVP sont les suivants :

- Examiner les processus opérationnels afin d'identifier le flux de données de renseignements personnels;

- Analyser la collecte, l'utilisation, la divulgation et la conservation des renseignements personnels :
- Déterminer s'il y a des enjeux ou des risques en matière d'atteinte à la vie privée associés à la mise en œuvre du SITR;
- Recommander des mesures visant à éviter, contrôler et atténuer tout enjeu ou risque en matière d'atteinte à la vie privée.

L'information présentée dans ce rapport est conforme au format de la Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor, et du document d'orientation du CPVP : « *Nos attentes : un guide pour la présentation d'évaluations des facteurs relatifs à la vie privée au Commissariat à la protection de la vie privée du Canada* ».

La Directive sur l'évaluation des facteurs relatifs à la vie privée du SCT est entrée en vigueur le 1er avril 2010. Elle s'applique aux institutions gouvernementales définies à l'article 3 de la *Loi sur la protection de la vie privée*, notamment les sociétés d'État mère.

## Portée du projet

La portée des travaux que représente l'EFVP est la mise en œuvre du SITR. Le système est limité, dans sa portée, à la réception et au traitement de diverses identifications et de demandes connexes. En particulier, il permettra à la Sécurité d'EACL de traiter les transactions civiles d'autorisation de sécurité pour le personnel existant et les candidats à un poste au sein d'EACL. La portée de la présente EFVP est limitée à la collecte de renseignements personnels dans le SITR et à l'analyse de leur utilisation, protection, conservation et divulgation.

Il serait avantageux pour EACL de prendre les empreintes digitales d'employés potentiels pendant qu'ils sont sur place pour leur entrevue en ayant recours à un formulaire de consentement écrit (Appendice A) à la saisie de leurs empreintes. Les données de sécurité du personnel seront transmises électroniquement à la GRC aux fins de vérification. Le SITR permettra d'accélérer le processus, grâce à l'application des normes du National Institute of Standards in Technology (NIST).

Les postulants pris en compte pour un emploi au sein d'EACL doivent obtenir une autorisation de sécurité avant de commencer leur emploi. Pour le moment, pour obtenir des renseignements sur le casier judiciaire, EACL utilise actuellement le système 400X de la Gendarmerie royale du Canada (GRC) et du Centre d'information de la police canadienne (CIPC)

EACL a entrepris d'acheter un appareil dactyloscopieur LiveScan qui permettra aux Services de vérification de sécurité du personnel d'envoyer les empreintes par voie électronique et de recevoir une réponse dans les 48 à 72 heures au lieu d'envoyer des copies papiers pour lesquelles on ne recevait la réponse que 8 à 12 semaines plus tard. Dans le passé (avant les événements du 11 septembre), notre processus ordinaire était d'envoyer des empreintes pour tous les employés et tous les entrepreneurs. EACL utilisera la technologie du SITR aux Laboratoires de Chalk River et de Whiteshell. Les systèmes ont obtenu l'accréditation de la GRC et satisfont aux exigences DCI NIST des SNP (voir l'Appendice E). La certification garantit que les transactions sont correctement formatées et possèdent tout le contenu requis.

## Initiative du projet

En 1968, les Services nationaux de police (SNP) ont installé le premier Système automatisé d'identification dactyloscopique au monde (SAID). Depuis, les SNP ont utilisé plusieurs générations de SAID ainsi que d'autres technologies pour effectuer des recherches électroniques de jeux complets

d'empreintes entrantes[1] et d'empreintes digitales latentes[2] et les comparer avec celles contenues dans les bases de données dactylaires criminelles. D'autres systèmes, comme le Fichier judiciaire nominatif (FJN), le système sur les antécédents criminels (Criminal History System (CHS), le système d'inscription, de mise à jour et de contrôle des casiers judiciaires (SIMCCJ) et le SIMCCJDED (une ancienne version du SIMCCJC) ont aidé à accélérer le traitement électronique[3]. Bien qu'efficients, ces systèmes ne sont pas reliés par une interface et ont été mis au point séparément d'autres systèmes d'application de la loi. Le traitement des soumissions exige aussi un fort taux de duplication des entrées de données. Les processus sont complexes, demandent beaucoup de main-d'œuvre et ne peuvent produire des résultats dans les délais requis par les clients. Le rapport de 2000 du vérificateur général du Canada soulignait ces lacunes (Section 3.3 de ce document). La haute direction de la GRC travaille à résoudre ces questions depuis 2000, et a fourni des ressources importantes pour définir les exigences opérationnelles d'un système électronique; elle a présenté quatre options dans une analyse de cas.

Le SITR, quand il atteindra ses objectifs, réduira de manière significative le temps requis pour vérifier et mettre à jour les renseignements. Les exemples suivants illustrent le type d'amélioration de service que fournira le SITR à EACL. De nos jours, EACL réalise une transaction civile d'autorisation de sécurité de la manière suivante :

a) Le Bureau de vérification de sécurité du personnel reçoit la trousse de vérification du personnel des RH;
b) Le Formulaire d'autorisation, de consentement et de vérification du personnel TBS/SCT 330-23F est rempli; on s'assure que le document et les vérifications des références ont été signés par les RH et le postulant;
c) Si le formulaire n'est pas signé, l'agent de sécurité du personnel (ASP) obtiendra un consentement oral ou écrit de la part du postulant;
d) Les renseignements sur les postulants sont saisis dans le système d'alerte de sécurité par l'ASP:
e) On effectue une vérification nominale du casier judiciaire (VNCJ) certifiée auprès de la GRC, au moyen du système 400X;
f) Si la réponse de la GRC est incomplète, une demande de VNCJ est transmise au DPRS;
g) Si les résultats indiquent une condamnation au criminel autre qu'une condamnation signalée par le postulant, des empreintes digitales sont requises :
h) Si des empreintes sont requises, l'ASP contacte le postulant et l'informe qu'il doit faire faire une dactyloscopie au poste de police le plus près de chez lui;
i) Les services de police locaux remplissent un formulaire de dactyloscopie de la GRC (C-216C (88-12) 7540-21-862-7891) et l'envoient à la GRC aux fins de vérification des antécédents criminels (Voir le diagramme 1 pour l'acheminement manuel/automatisé sur copie papier contre l'acheminement automatisé du SITR en ce qui a trait aux transactions civiles de demandes d'autorisation de sécurité);
j) Il incombe au postulant de transmettre les résultats de la vérification de ses antécédents criminels aux Services de sécurité du personnel;
k) Si les résultats de la GRC sont défavorables, le dossier est transmis au coordinateur du programme de sécurité du personnel pour qu'il arrange une entrevue avec le sujet et fasse une évaluation de la gestion des risques;
l) Si les résultats de la GRC ne sont pas défavorables, l'autorisation de sécurité est accordée;

1 Il s'agit d'un ensemble complet d'empreintes digitales roulées, typiquement reçu lorsqu'il y a condamnation au criminel, dans un formulaire C-216.
2 Les empreintes latentes sont les empreintes relevées sur le lieu d'un crime.
3 Voir l'Appendice A pour plus de détails sur les systèmes actuels.

m) Un Certificat d'enquête de sécurité (TBS/SCT 330-47) est rempli et signé par l'agent de sécurité du personnel ou le coordinateur du programme de sécurité du personnel;
n) Un avis est envoyé par courriel aux RH et aux TI pour les informer que la personne a une autorisation de sécurité valide;
o) Afin que la personne puisse recevoir une autorisation d'accès au niveau 1, 2 ou 3, toutes les exigences de la vérification de fiabilité doivent être satisfaites.

Outre les étapes A à K de la vérification de la fiabilité décrites ci-dessus, les étapes suivantes sont respectées pour les autorisations de niveau 2 et de niveau 3 et/ou les accès au site, à l'exception des étapes F à I, qui ne s'appliquent pas pour le niveau 3 car les SSP utilisent actuellement le SITR pour les autorisations de niveau 3 seulement, puisque le Conseil du Trésor exige que des empreintes digitales soient présentées pour ce niveau.

a) L'ASP passe en revue le questionnaire sur l'accès au site ou le formulaire d'autorisation de sécurité (TBS/SCT 330-60F) pour vérifier qu'il est dûment rempli et qu'il contient toute l'information demandée et toutes les signatures requises;
b) Outre la VNCJ, l'ASP effectuera un dossier de crédit pout les autorisations de niveau 2 et 3;
c) Les renseignements sur les postulants sont saisis dans le système d'alerte de sécurité par l'ASP;
d) L'ASP saisit les renseignements sur le postulant dans le système d'information sur les vérifications de sécurité (SIVS) qui sont propres au niveau d'autorisation demandé;
e) L'ASP exporte les renseignements sur les postulants du SIVS et les transmet au Service canadien du renseignement de sécurité (SCRS)
f) Les résultats du SCRS peuvent prendre jusqu'à 10 jours ouvrables, ou plus, selon les renseignements soumis.
g) L'ASP importera les résultats du SCRS dès la réception du dossier chiffré;
h) Si les résultats du SCRS sont « incomplet », le dossier est transmis au coordinateur du programme de sécurité pour qu'il arrange une entrevue avec le sujet et fasse une évaluation de la gestion des risques;
i) Si les résultats du SCRS sont « rien à signaler », l'autorisation est accordée;
j) Un Certificat d'enquête de sécurité (TBS/SCT 330-47) est rempli et signé par l'agent de sécurité du personnel ou le coordinateur du programme de sécurité du personnel;
k) Un avis est envoyé par courriel aux RH et aux TI pour les informer que la personne a une autorisation de sécurité valide;
l) La personne doit prendre part à une séance d'information sur les cotes de sécurité et reçoit une carte d'accès d'EACL après avoir suivi la formation applicable d'EACL.

Étape pour le processus d'autorisation au moyen du SITR :

a) Le postulant assiste à un processus d'entrevue avec les RH et/ou un jury d'entrevue;
b) Le postulant est amené aux Services de vérification de sécurité du personnel pour une séance d'information sur le formulaire de consentement à la dactyloscopie. Les conditions lui sont expliquées, comme il est décrit dans l'Appendice A. Le Formulaire est signé par le postulant et l'ASP;
c) L'agent de sécurité du personnel se sert du scanner du SITR pour faire la dactyloscopie du postulant. Le dossier est sauvegardé dans le journal des entrées du SITR;
d) Lorsque EACL/les RH reçoivent la lettre d'offre signée du postulant, l'ASP accède au journal des entrées du SITR et soumet électroniquement les empreintes du postulant à la GRC, au moyen du serveur des commissionnaires;
e) Les dossiers des postulants non-retenus sont supprimés du journal des entrées du SITR;
f) La trousse de vérification du personnel du postulant retenu est reçue des RH;
g) On vérifie que le formulaire de vérification de la sécurité, de consentement et d'autorisation du personnel (TBS/SCT 330-23F) est dûment rempli et que les documents et les vérifications des

références ont été signés par les RH et le postulant;

h) Les renseignements sur le postulant sont saisis dans le système d'alerte de sécurité par l'ASP;
i) L'Agent de sécurité du personnel extrait les résultats du SITR;
   I. Avis « Aucuns renseignements défavorables » reçu dans les 24 à 48 heures
   II. Avis « Renseignements défavorables » reçu dans les 48 à 72 heures, à moins que le postulant ne soit devant les tribunaux, auquel cas il pourrait y avoir des retards.
j) Les résultats de la dactyloscopie et du casier judiciaire sont imprimés et placés dans le dossier de sécurité du personnel de la personne, puis supprimés du SITR;
k) Si les résultats montrent des renseignements défavorables, le dossier est transmis au coordinateur du programme de sécurité pour qu'il arrange une entrevue avec le sujet et fasse une évaluation de la gestion des risques;
l) Si les résultats n'indiquent aucuns renseignements défavorables, la vérification de fiabilité est accordée;
m) Un Certificat d'enquête de sécurité (TBS/SCT 330-47) est rempli et signé par l'agent de sécurité du personnel ou le coordinateur du programme de sécurité du personnel;
n) Un avis est envoyé par courriel aux RH et aux TI pour les informer que la personne a une autorisation de sécurité valide;
o) Afin qu'une personne puisse recevoir une autorisation d'accès au niveau 1, 2 ou 3, toutes les exigences de la vérification de fiabilité doivent être satisfaites. Outre les étapes suivies pour une autorisation au moyen du SITR, les étapes énumérées ci-dessus pour les niveaux 2 et 3 et l'accès au site doivent aussi être suivies.

Le SITR intégrera le traitement électronique des empreintes digitales et du casier judiciaire. Aujourd'hui, ces deux activités sont traitées comme des fonctions séparées. Le SITR intégrera l'ensemble actuel de systèmes « en tuyau de poêle » (systèmes séparés qui n'échangent pas de données au moyen d'une base de données commune) utilisé pour appuyer les renseignements sur les antécédents criminels et les empreintes digitales.

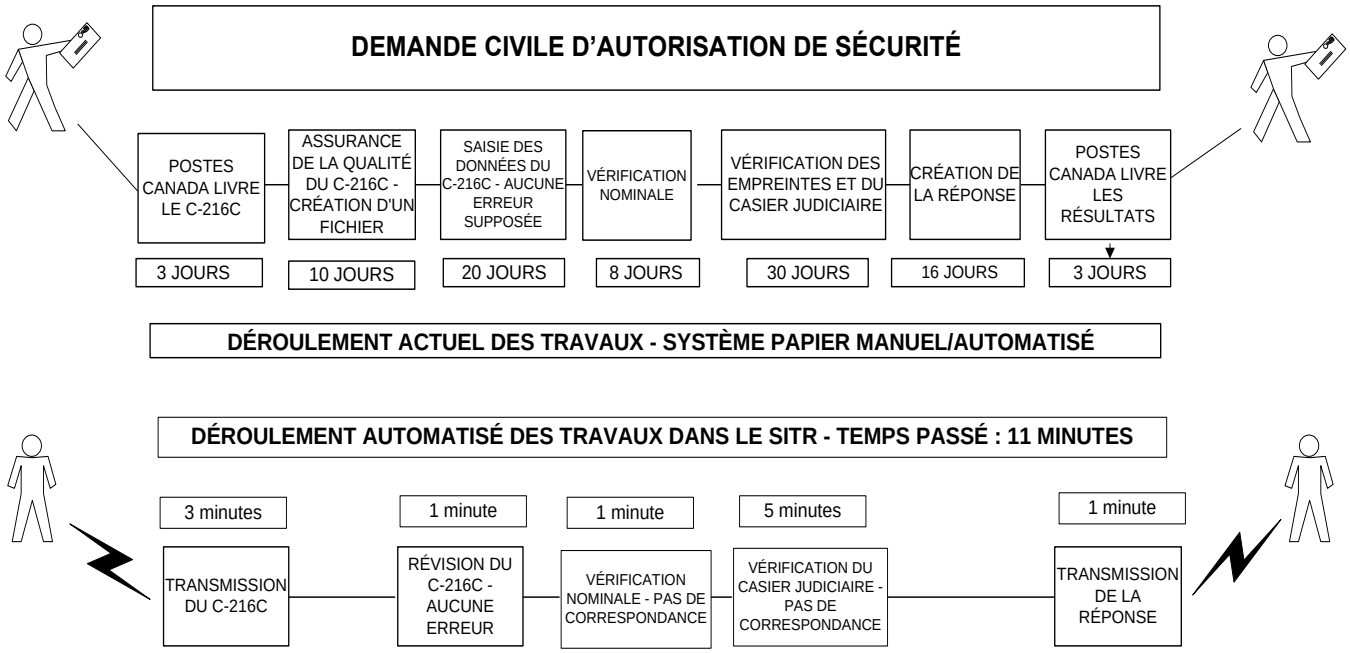


***Schéma 1 – Déroulement des transactions civiles de demandes d'autorisation de sécurité de la GRC***

## Avantages du SITR

- Résout les risques à la population et aux systèmes judiciaires et d'application de la loi du Canada causés par l'obsolescence des dossiers criminels au CIPS;
- Résout l'incapacité de la GRC à traiter les transactions civiles d'autorisation de sécurité dans des délais acceptables; l'initiative sur la frontière intelligente dirigée par l'Agence des services frontaliers du Canada (ASFC) et d'autres initiatives de sécurité civiles ont imposé des demandes et des attentes en matière de temps de réponse auxquelles la GRC n'est pas en mesure de répondre. En ce moment, il faut trois mois pour traiter une demande civile. Les renseignements pour la vérification nominale du casier judiciaire sont toujours reçus en temps opportuns. S'il y a des renseignements défavorables, et qu'une copie papier des empreintes est nécessaire, les retards peuvent s'étendre jusqu'à huit ou douze semaines.
- Répondre aux exigences en matière de sécurité : le processus actuel (sur papier) ne peut fonctionner dans un milieu « Protégé B ». Le SITR sera un milieu « Protégé B ».
- Fournit une capacité de reprise des activités/reprise après sinistre pour l'identification dactylaire. Comme le système actuel repose sur des dossiers papier, il serait très difficile, voire impossible de les récupérer après un sinistre.
- Envoie des transactions chiffrées. Tous les renseignements personnels transmis à la GRC au moyen du SITR seront chiffrés.

# 2 SECTION II - DÉTERMINATION ET CATÉGORISATION DES FACTEURS DE RISQUE

| A: Type de programme ou d'activité | Niveau de risque pour la vie privée |
|---|---|
| Le programme ou l'activité ne comporte PAS de décision visant un individu identifiable.<br>Les renseignements personnels servent uniquement aux fins de travaux de recherche ou de statistique ou à des évaluations, y compris une liste d'envois où aucune des décisions prises a un effet direct sur un individu identifiable. La Directive sur l'EFVP s'applique à l'utilisation administrative de renseignements personnels. En vertu de la Politique sur la protection de la vie privée, les institutions fédérales sont tenues d'établir un protocole ministériel/organisationnel de protection des renseignements personnels pour traiter des utilisations non administratives de renseignements personnels. | ☐ 1 |
| Administration de programmes/activités et de services<br>Les renseignements personnels sont utilisés pour prendre des décisions qui touchent directement l'intéressé (p. ex., déterminer l'admissibilité à des programmes, y compris procéder à l'authentification pour permettre l'accès à des programmes ou services, administrer les paiements de programme, les trop-payés ou le soutien à la clientèle, délivrer ou refuser des permis ou des licences, traiter des appels, etc.). | ☐ 2 |
| Exécution/Enquêtes d'observation ou réglementaires<br>Les renseignements personnels sont utilisés pour détecter des fraudes ou enquêter sur d'éventuels abus dans les programmes lorsque les conséquences sont de nature administrative (p. ex. imposition d'une amende, interruption du versement de prestations, vérification de la déclaration de revenu d'un particulier ou déportation d'une personne pour des motifs non liés à la sécurité national ni à un acte criminel). | ☒ 3 |
| Enquête criminelle et exécution/sécurité nationale<br>Les renseignements personnels sont utilisés à des fins d'enquête et d'application des lois en matière criminelle (p. ex. décisions pouvant mener à des accusations ou à des peines au criminel ou à la déportation pour des motifs liés à la sécurité nationale ou à un acte criminel). | ☐ 4 |

| B: Type de renseignements personnels en cause, et contexte | Niveau de risque pour la vie privée |
|---|---|
| Uniquement des renseignements personnels fournis par l'intéressé — au moment de leur collecte — concernant un programme autorisé et recueillis auprès de l'individu lui-même ou avec son consentement quant à leur communication, en l'absence d'éléments contextuels sensibles.<br>Le contexte dans lequel les renseignements personnels sont recueillis n'est pas particulièrement sensible; par exemple, la délivrance d'un permis ou le renouvellement de documents de voyage ou de pièces d'identité. | ☐ 1 |
| Renseignements personnels fournis par l'intéressé avec consentement d'utiliser aussi les renseignements personnels détenus par une autre source/en l'absence d'éléments contextuels sensibles, après leur collecte. | ☐ 2 |
| Numéro d'assurance sociale, renseignements médicaux ou financiers ou autres renseignements personnels sensibles et/ou éléments contextuels sensibles entourant les renseignements personnels. Renseignements personnels sur des mineurs ou des incapables ou encore concernant une personne ayant qualité pour agir au nom de l'intéressé. | ☐ 3 |

| | |
|---|---|
| Par exemple, les renseignements personnels par association révèlent indirectement de l'information sur l'état de santé, la situation financière, la religion ou le style de vie de l'intéressé. | |
| Renseignements personnels sensibles, y compris des profils détaillés, des allégations ou soupçons, des échantillons de substances corporelles et/ou éléments contextuels particulièrement sensibles entourant les renseignements personnels.<br>Par exemple, les renseignements personnels par association révèlent indirectement des détails intimes sur l'état de santé, la situation financière, la religion ou le style de vie de l'intéressé ou d'autres personnes, comme des parents de l'intéressé. | ☒ 4 |

| **C: Partenaires du programme ou de l'activité et participation du secteur privé** | **Niveau de risque pour la vie privée** |
|---|---|
| Au sein de l'institution (parmi un ou plusieurs programmes de la même institution) | ☐ 1 |
| Avec d'autres institutions fédérales | ☒ 2 |
| Avec une autre institution ou une combinaison d'institutions du gouvernement fédéral, des gouvernementaux provinciaux et des municipalités | ☐ 3 |
| Organisations du secteur privé ou organisations internationales ou gouvernements étrangers | ☐ 4 |

| **D: Durée du programme ou de l'activité** | **Niveau de risque pour la vie privée** |
|---|---|
| Activité ou programme ponctuel<br>Il s'agit généralement d'une mesure de soutien ponctuel prenant la forme d'une subvention versée dans le cadre d'un mécanisme de soutien social. | ☐ 1 |
| Programme à court terme<br>Programme ou activité qui vise un objectif à court terme et dont la date limite est fixée. | ☐ 2 |
| Programme à long terme<br>Programme existant qui a été modifié ou dont la date limite n'est pas clairement établie. | ☒ 3 |

| **E: Population du programme** | **Niveau de risque pour la vie privée** |
|---|---|
| Le programme touche certains employés à des fins administratives internes. | ☐ 1 |
| Le programme touche tous les employés à des fins administratives internes. | ☐ 2 |
| Le programme touche certains individus à des fins administratives externes. | ☒ 3 |
| Le programme touche tous les individus à des fins administratives externes. | ☐ 4 |

| **F: Technologie et vie privée** | **Niveau de risque pour la vie privée** |
|---|---|
| 1. L'activité ou le programme (nouveau ou modifié) comporte-il l'implantation d'un nouveau système électronique, logiciel ou programme d'application, y compris un | ☒ OUI<br>☐ NON |

| | |
|---|---|
| collecticiel (ou logiciel de groupe) qui est implanté pour soutenir le programme ou l'activité eu égard à la création, la collecte ou la manipulation de renseignements personnels? | |
| 2. L'activité ou le programme nouveau ou modifié exige-t-il une modification de systèmes ou services existants de TI? | ☐ OUI<br>☒ NON |
| 3. L'activité ou le programme nouveau ou modifié implique-t-il l'implantation d'une ou plusieurs des technologies suivantes : | |
| 3.1 Méthodes d'identification améliorées<br>Cela comprend la technologie biométrique (comme la reconnaissance faciale, l'analyse de la démarche, la lecture ou le balayage de l'iris, l'analyse des empreintes digitales, la signature ou empreinte vocale, l'identification par radiofréquence (IRF) etc.) ainsi que la technologie des laissez-passer facilités (Easy pass), les nouvelles cartes d'identification comportant des bandes magnétiques, comme les « cartes intelligentes » (c.-à-d. des cartes d'identité sur lesquelles est gravée soit une antenne soit une plage de contact connectée à un microprocesseur et une puce mémoire ou uniquement à une puce mémoire avec matrice logique non programmable).<br>Précisez la ou les catégories applicables : | ☒OUI<br>☐ NON |
| 3.2 Recours à la surveillance :<br>Cela comprend les technologies de surveillance tels que les appareils d'enregistrement audio/vidéo, l'imagerie thermique, les appareils de reconnaissances, l'IRF, la surveillance/interception clandestine, le contrôle assisté par ordinateur, y compris les pistes de vérification, la surveillance par satellite, etc.<br>Précisez la ou les catégories applicables : | ☐OUI<br>☒ NON |
| 3.3 Utilisation de l'analyse automatisée des renseignements personnels, du couplage de renseignements personnels et des techniques de découverte/acquisition de connaissances<br>Aux fins de la directive sur l'EFVP, les institutions fédérales doivent préciser quelles activités comportent le recours à des technologies d'analyse, de création, de comparaison, de tri, d'identification ou d'extraction automatiques, d'éléments de renseignements personnels. Ces activités comprendraient le couplage (ou appariement) de renseignements personnels, le couplage de dossiers, l'exploration de renseignements personnels, la comparaison de renseignements personnels, la découverte de connaissances et le filtrage ou l'analyse d'informations. De telles activités comportent une forme ou une autre d'intelligence artificielle et/ou d'apprentissage machine pour découvrir des connaissances (renseignements), des tendances ou des modèles, ou encore pour prédire des comportements.<br>Précisez la ou les catégorie(s) applicable(s) : | ☐OUI<br>☒ NON |
| Une réponse **AFFIRMATIVE** à l'une ou l'autre des rubriques qui précèdent signale la possibilité de préoccupations liées à la vie privée et de risques sur lesquels il faudra se pencher et qui devront être atténués au besoin. | |

| G: **Transmission des renseignements personnels** | **Niveau de risque pour la vie privée** |
|---|---|
| Les renseignements personnels sont utilisés à l'intérieur d'un système fermé. | ☒ 1 |

| | |
|---|---|
| Aucune connexion à l'Internet, l'intranet ou tout autre système. La circulation des documents sur support papier est contrôlée. | |
| Les renseignements personnels sont utilisés dans un système qui comporte des connexions à au moins un autre système. | ☐ 2 |
| Les renseignements personnels sont transférés à un appareil portable ou sont imprimés.<br>Clé USB, disquette, ordinateur portatif, tout transfert des renseignements personnels à un différent médium. | ☐ 3 |
| Les renseignements personnels sont transmis au moyen de technologies sans fil. | ☐ 4 |

| H: **Incidences des risques pour l'institution** | **Niveau de risque pour la vie privée** |
|---|---|
| Répercussions négatives au niveau de la direction/gestion<br>Les procédures/processus doivent être revus, les outils doivent être changés, il faut changer de fournisseur/partenaire. | ☐ 1 |
| Répercussions négatives au niveau organisationnel<br>Changements à la structure organisationnelle, modification de la structure décisionnelle de l'organisation, changement de la distribution/répartition des responsabilités, changement de l'architecture d'activités de programme, départ d'employés, réaffectation de ressources de RH. | ☒ 2 |
| Préjudice financier<br>Poursuites, montants supplémentaires requis, réaffectation de ressources financières. | ☐ 3 |
| Atteinte à la réputation, embarras, perte de crédibilité<br>Diminution de la confiance du public, élus placés sous les projecteurs, résultats stratégiques de l'institution compromis, priorité gouvernementale compromise, répercussions sur les secteurs de résultats du gouvernement du Canada. | ☐ 4 |

| **I: Incidences des risques sur l'individu ou l'employé** | **Niveau de risque pour la vie privée** |
|---|---|
| Inconvénient | ☐ 1 |
| Atteinte à la réputation, embarras | ☒ 2 |
| Préjudice financier | ☐ 3 |
| Préjudice physique | ☐ 4 |