# Vérification des enquêtes de sécurité sur le personnel

## RAPPORT

**Division de la vérification et de l'évaluation**
**Juillet 2003**

Statistics Canada Statistique Canada

Canada

# Table des matières

## Énoncé du vérificateur

Je viens de terminer la vérification des enquêtes de sécurité sur le personnel, dont l'objectif consistait à examiner le niveau de conformité aux normes du *Manuel des pratiques de sécurité* de Statistique Canada concernant les enquêtes de sécurité sur le personnel et à une norme connexe concernant l'accès au réseau A de Statistique Canada, c'est-à-dire le contrôle de l'accès « logique » lié à la sécurité de la technologie de l'information. La vérification visait de plus à déterminer les raisons de la non-conformité, afin d'améliorer les procédures.

Cette vérification interne a été effectuée conformément aux Normes de vérification interne dans l'administration fédérale. Au cours de la période de vérification, l'équipe de vérification a examiné les dossiers de sécurité pour 493 cas, ainsi que les dossiers liés au contrôle de l'accès logique pour 35 % d'entre eux.

Dans le cas des employés nommés pour une période indéterminée, les procédures sont généralement conformes au chapitre 3 du *Manuel des pratiques de sécurité* de Statistique Canada, selon lequel une vérification de sécurité doit être effectuée avant l'entrée en fonction. Dans le cas des employés nommés pour une période déterminée et des intervieweurs, qui peuvent être nommés avant qu'une vérification approfondie de la fiabilité soit effectuée, afin de répondre aux besoins opérationnels, ainsi que des étudiants, qui peuvent être nommés avant qu'une vérification soit effectuée, nous concluons que le processus est conforme, même s'il pourrait être accéléré. Dans le cas des personnes réputées être employées visées par la vérification, nous n'avons pas pu déterminer le niveau de conformité en raison de considérations méthodologiques. L'accès aux comptes du système informatique est conforme à la norme relative à l'accès au réseau A (c'est-à-dire celle sur le contrôle de l'accès logique pour les comptes informatiques standard figurent dans le *Manuel des pratiques de sécurité*, chapitre 5).

Ces conclusions sont fondées sur l'évaluation des constatations par rapport à des critères préétablis et approuvés par le Comité de la vérification interne, en novembre 2002, et rendent compte des travaux de vérification qui se sont déroulés principalement entre mars et juin 2003.

À mon avis, les travaux de vérification ont été suffisants et appropriés, et des preuves ont été recueillies pour appuyer les conclusions comprises dans le présent rapport de vérification.

Beverly Prentice
Gestionnaire de la vérification

Décembre 2003

# I. Introduction

## Contexte

La gestion de la sécurité à Statistique Canada et dans l'administration fédérale englobe trois grands domaines : la sécurité matérielle et électronique de l'information, la sécurité des biens et la sécurité du personnel. En ce qui a trait à la sécurité du personnel, elle a essentiellement trait à des enquêtes appropriées de sécurité sur les employés, selon le niveau de sécurité correspondant à la classification de sécurité de l'information qu'ils utilisent dans leur travail.

La sécurité du personnel a récemment pris une importance considérable sur la scène mondiale, et elle est considérée comme un élément essentiel de la sécurité de l'information et des biens. L'absence d'enquêtes ou des enquêtes inappropriées sur les employés pourrait avoir des répercussions extrêmement dommageables sur notre réputation si une infraction grave à la sécurité était commise par un employé qui n'aurait pas fait l'objet d'une enquête. L'augmentation récente et rapide du nombre d'employés à Statistique Canada, ainsi que la nature délicate des données recueillies par le Bureau, ont motivé la vérification, étant donné qu'il a été déterminé que les risques sont réels et que les répercussions possibles sur notre réputation sont très grandes.

## Objectif

La vérification avait comme objectif de déterminer le niveau de conformité aux normes du *Manuel des pratiques de sécurité* de Statistique Canada concernant les enquêtes de sécurité sur le personnel et à une norme connexe concernant le contrôle de l'accès logique lié à la sécurité de la technologie de l'information. La vérification visait de plus à déterminer les raisons de la non-conformité, afin d'améliorer les procédures.

## Portée

La vérification a mis l'accent sur les normes relatives aux enquêtes de sécurité sur le personnel qui s'appliquent aux employés, aux intervieweurs et aux personnes réputées être employées de Statistique Canada, par exemple, les chercheurs sur place, les agents provinciaux, d'autres fonctionnaires fédéraux et les participants à des échanges.

Au départ, les entrepreneurs faisaient partie du champ de la vérification. Par la suite, nous les avons exclus pour les raisons suivantes :

- les résultats positifs récents de la vérification interne des services de sous-traitance;
- notre évaluation selon laquelle leur risque pour la sécurité est faible;
- le fardeau de réponse imposé aux employés des Services du matériel et des contrats.

Nous avons conclu que les agents provinciaux, les autres fonctionnaires fédéraux et les bénévoles sont peu nombreux et présentent un faible risque, et nous n'avons pas examiné leurs dossiers.

Même s'il était prévu dans le mandat d'examiner la façon dont les gestionnaires contrôlent l'accès à l'information matérielle désignée, lorsqu'une enquête de sécurité est en cours, nous avons exclu cet élément pour les raisons suivantes :

- risque plus faible;
- difficultés liées à la mesure;
- échéancier.

## Critères

Nous nous attendions à constater ce qui suit :

- les employés font l'objet d'une enquête de sécurité et obtiennent une cote de sécurité conformément au *Manuel des pratiques de sécurité*, chapitre 3, en raison de l'information et des biens auxquels ils ont accès.

| **Type** | **Chapitre 3 – Éléments clés** |
|---|---|
| Employés nommés pour une période indéterminée | La cote de fiabilité approfondie doit avoir été accordée avant qu'une nomination à un poste d'une durée indéterminée soit faite. |
| Employés nommés pour une période déterminée | Les personnes embauchées pour une durée de moins de six mois peuvent être nommées avant que la vérification approfondie de la fiabilité soit terminée si, de l'avis du gestionnaire intéressé, les besoins du service le nécessitent. Il est toutefois essentiel que les références personnelles soient vérifiées et que les résultats soient satisfaisants. Les nominations pour une période déterminée ne doivent pas s'étendre au-delà de la durée prévue sans que la cote de fiabilité approfondie n'ait été accordée. |
| Étudiants | Les nominations aux postes prévus pour les étudiants peuvent être faites avant que la vérification approfondie de la fiabilité soit menée. La vérification doit être commencée dès qu'une décision d'embauchage est rendue. Lorsque c'est possible, les références devraient être vérifiées avant la nomination et les résultats obtenus doivent être satisfaisants. |
| Intervieweurs | En raison du caractère délicat du rôle des intervieweurs, ceux-ci devraient normalement avoir la cote de fiabilité approfondie avant d'entreprendre effectivement la collecte des données. Toutefois, les nominations aux postes d'intervieweurs peuvent être confirmées avant que la cote de fiabilité approfondie ait été accordée si, de l'avis du gestionnaire intéressé, les besoins du service le nécessitent. La vérification approfondie de la fiabilité doit être entreprise dès qu'une décision d'embauchage est prise et la nomination devrait être |

retardée jusqu'à ce que la vérification complète des références personnelles soit terminée et que les résultats obtenus soient satisfaisants.

Nous nous attendions à constater ce qui suit :

- l'accès aux comptes du système informatique et l'information matérielle désignée, lorsqu'une enquête de sécurité est en cours, est conforme au *Manuel des pratiques de sécurité*, chapitre 5.

Les personnes réputées être employées sont considérées comme des employés aux fins de la *Loi sur la statistique*. La *Politique sur l'utilisation de personnes réputées être employées* de Statistique Canada, datée de juillet 2002, comporte des renseignements additionnels à ce sujet.

**Processus d'enquête de sécurité sur le personnel pour les nouveaux employés**

Les enquêtes de sécurité sur le personnel, en vue de l'obtention d'une cote de fiabilité approfondie, comportent plusieurs étapes, qui sont documentées dans le formulaire d'enquête de sécurité, de consentement et d'autorisation :

- obtenir le consentement du postulant, pour que soit effectuée une enquête à son sujet, et une déclaration concernant l'existence d'un casier judiciaire;
- vérifier la date de naissance, l'adresse, les études, les compétences professionnelles, les antécédents professionnels et les références morales;
- faire effectuer une vérification nominale de casier judiciaire par la GRC;
- au besoin, obtenir des empreintes digitales, afin que la GRC puisse procéder à une vérification;
- recevoir les résultats;
- prendre une décision.

L'accès au réseau est autorisé une fois que la Sécurité du Bureau a signé le formulaire de demande.

## II. Méthodologie

Avec l'aide d'un méthodologiste, l'équipe de vérification a :

- identifié les nouveaux employés devant faire l'objet d'une enquête de sécurité sur le personnel, à partir de la base de données du Système de paye des opérations des enquêtes statistiques (SPOES), dans le cas des intervieweurs, et de Global, une autre base de données des ressources humaines, dans le cas des autres employés. La liste de Global couvre la période du 1er février 2002 au 31 janvier 2003, tandis que celle du SPOES porte sur une période légèrement antérieure, soit du 1er décembre 2001 au 30 novembre 2002.

- tiré des échantillons représentatifs, vérifié les données requises dans les dossiers de la Sécurité du Bureau et de la Division des services de technologie informatique

(DSTI), afin de déterminer quand les employés ont obtenu leurs codes d'utilisateurs pour accéder au réseau. Nous avons examiné les dossiers de la Sécurité du Bureau pour 493 cas, et ceux de la DSTI pour 35 % d'entre eux. Dans le cas des dossiers de la DSTI où figuraient les deux dates, nous avons vérifié si la Sécurité du Bureau avait signé le formulaire le jour ou avant le jour de l'octroi de l'accès par la DSTI.

- identifié les postes nécessitant une cote de sécurité au niveau secret et identifié les employés les occupant, ainsi que les cas où les cotes de fiabilité approfondie devaient être mises à jour parce qu'elles dataient de plus de dix ans, sur la base des employés figurant à l'effectif en date du 31 mai 2003, selon Global.

- dans le cas des personnes réputées être employées, examiné 78 cas de la base de données du Programme des centres de données de recherche.

- effectué des entrevues auprès des employés de la Sécurité du Bureau, de la Division des opérations des ressources humaines, de la Direction des opérations régionales, y compris les gestionnaires et les employés des Services de gestion et informatique dans les bureaux régionaux, de la Division des services de technologie informatique et du gestionnaire du Programme des centres de données de recherche.

## III. Constatations et recommandations

### *Principaux résultats*

- Les procédures sont conformes de façon générale aux exigences en matière d'enquêtes de sécurité sur le personnel du *Manuel des pratiques de sécurité*, chapitre 3, même si, dans le cas des employés nommés pour une période déterminée, des intervieweurs et des étudiants, ce processus pourrait être accéléré.
- La Division des services de technologie informatique ne délivre pas de code d'utilisateur du réseau sans avoir reçu l'approbation de la Sécurité du Bureau.

### *Détails*
### *Évaluation du niveau de conformité*

Tous les employés et les personnes réputées être employées de Statistique Canada doivent faire l'objet d'une vérification approfondie de la fiabilité. Une minorité d'entre eux, y compris ceux de la catégorie des cadres supérieurs, doivent obtenir une cote de sécurité au niveau secret.

## Dans le cas des employés

**Nouveaux employés**
Dans le cas des employés nommés pour une période indéterminée, les résultats montrent que les procédures sont généralement conformes aux exigences du *Manuel des pratiques de sécurité* interne, selon lesquelles aucun employé nommé pour une période

indéterminée ne doit commencer à travailler avant d'avoir obtenu une cote de fiabilité approfondie. Près de 90 %[1] répondaient à ce critère, et 95 % ont reçu une cote deux semaines après avoir commencé à travailler.

Les normes sont moins rigoureuses et plus variées dans le cas des autres employés, comme il est indiqué précédemment. Lorsque les besoins du service le nécessite, les employés nommés pour une période déterminée et les intervieweurs peuvent commencer à travailler avant que l'enquête soit terminée. Moins de la moitié des employés nommés pour une période déterminée et des étudiants avaient reçu leur cote de sécurité avant de commencer à travailler, mais 86 %[2] et 92 %[3] d'entre eux, respectivement, l'ont obtenue dans un délai de deux semaines. Dans le cas des intervieweurs, 50 %[4] avaient reçu leur cote de sécurité avant de commencer à travailler. Deux semaines plus tard, cette proportion était de 89 %[5]. À Sturgeon Falls, dans le cas de l'échantillon d'intervieweurs, la conformité était complète au moment de l'entrée en fonction.

Cette vérification a été axée sur des normes internes qui sont en place depuis 1991. Toutefois, la dernière *Politique sur la sécurité du gouvernement du Canada*, qui a été révisée le 1er février 2002, stipule que « les ministères doivent s'assurer qu'avant leur entrée en fonction, les personnes qui ont besoin d'avoir : a) accès aux biens du gouvernement (y compris l'information) font l'objet d'une vérification de la fiabilité et obtiennent une cote de fiabilité ». Le Bureau doit réviser ses normes en conséquence.

**Mise à jour des cotes de fiabilité approfondie des employés**

Les cotes de fiabilité approfondie sont valides pour une période de dix ans, après quoi elles doivent être mises à jour. Les résultats fondés sur Global montrent que la cote de sécurité de 11 % des 6 352 employés faisant partie de l'effectif en date du 31 mai 2003 était expirée. En mai 2003, la Sécurité du Bureau a entrepris de déterminer les cas de cotes expirées et de demander des mises à jour. L'élimination de cet arriéré et l'établissement d'un processus de mise à jour avant la date d'expiration permettraient de résoudre le problème.

La vérification des dates d'expiration, au moment des mesures de dotation, et le lancement d'un processus de mise à jour, au besoin, constitueraient une autre façon d'assurer le contrôle. À l'heure actuelle, nous avons déterminé que parmi les 705 cas de cotes expirées, 45 % ont fait l'objet de mesures de dotation après la date d'expiration.

**Cote de sécurité au niveau secret et mises à jour**

Les résultats de Global montrent que, de façon générale, les employés qui ont besoin d'une cote de sécurité au niveau secret en possèdent une. Il existe quelques exceptions, 5 des 193 postes nécessitant une cote au niveau secret sont occupés par des employés qui

[1] L'intervalle de confiance à 95 % est de +/- 15 %. Le coefficient de variation est de 9 %.
[2] L'intervalle de confiance à 95 % est de +/- 12 %. Le coefficient de variation est de 8 %.
[3] L'intervalle de confiance à 95 % est de +/- 19 %. Le coefficient de variation est de 11 %.
[4] L'intervalle de confiance à 95 % est de +/- 5 %. Le coefficient de variation est de 5 %.
[5] L'intervalle de confiance à 95 % est de +/- 3 %. Le coefficient de variation est de 2 %.

n'ont pas la cote de sécurité appropriée. Des mesures ont déjà été prises pour résoudre ce problème.

**Code d'utilisateur du réseau : mesure de contrôle efficace**
Les résultats de la vérification montrent que la Division des services de technologie informatique ne délivre pas de code d'utilisateur du réseau sans avoir obtenu l'approbation de la Sécurité du Bureau.

## Dans le cas des personnes réputées être employées

La *Loi sur la statistique* permet à des personnes autres que des employés de fournir des services et de travailler à titre de personne réputée être employée. Il peut s'agir d'autres fonctionnaires fédéraux, d'agents provinciaux, d'entrepreneurs, de personnel temporaire, de personnel participant à des échanges canadiens et internationaux, d'étudiants non rémunérés et de bénévoles, ainsi que de responsables de projets de recherche approuvés.

Les directeurs doivent s'assurer que les procédures appropriées sont suivies, y compris la vérification approfondie de la fiabilité, avant de donner accès à des données statistiques de nature délicate aux personnes réputées être employées dans leur division. Le gestionnaire du Programme des centres de données de recherche (CDR) a des responsabilités similaires pour les chercheurs des CDR. C'est donc dire que la responsabilité est partagée par de nombreuses personnes.

**Chercheurs du Programme des centres de données de recherche**
Il existe une base de données dans laquelle des employés qui n'appartiennent pas à la Sécurité inscrivent des renseignements au sujet des chercheurs et de leurs projets, y compris la date d'obtention de leur cote de sécurité. Il n'existe pas d'exigence opérationnelle prévoyant l'inscription de la date à partir de laquelle les chercheurs ont accès à des données confidentielles dans le cadre du Programme des centres de données de recherche (PCDR), qui pourrait servir à une vérification par rapport à la date d'octroi de la cote de sécurité. Nous n'avons pas été en mesure de déterminer le niveau de conformité, la méthodologie utilisée devant être modifiée de façon significative pour que l'on puisse tirer des conclusions.

## *Amélioration du traitement*

La présente section résume les principales pratiques exemplaires. Les gestionnaires ont reçu des renseignements plus détaillés.

**Approche de partenariat**
Les enquêtes de sécurité sur le personnel font intervenir diverses personnes — gestionnaires, spécialistes des ressources humaines et spécialistes de la sécurité. L'établissement de rapports de travail plus étroits, afin que les responsabilités de ces personnes se complètent, et que les rôles et les responsabilités puissent être compris, contribueraient à un effort intégré et amélioreraient les résultats.

**Obtention d'une signature au tout début du processus**
L'obtention de la signature des postulants sur les formulaires de consentement et d'autorisation, tôt au début du processus d'embauchage, par exemple, au moment où ils sont invités à participer à un examen écrit ou à une entrevue, permettrait aux gestionnaires d'assurer un plus grand niveau de conformité. Des procédures écrites uniformes, grâce auxquelles cet élément serait intégré au processus d'embauchage et serait appliqué par toutes les équipes de dotation, tant les gestionnaires que les professionnels des ressources humaines, augmenteraient la probabilité que les personnes reçoivent leur cote de sécurité avant d'entrer en fonction.

**Meilleures gestion des cas et documentation**
Un contrôle plus efficace du fichier des cas en suspens de la Sécurité du Bureau pour les cas nécessitant des empreintes digitales réduirait la taille et permettrait d'éliminer les cas en suspens pendant de longues périodes. Selon les bonnes pratiques de gestion, la responsabilité revient à la Sécurité du Bureau dans ce cas, et il existe une possibilité que cette dernière assume un rôle de leadership, ce qui aiderait les gestionnaires à faire de même. Des formulaires de consentement et d'autorisation bien remplis facilitent les étapes ultérieures du processus des enquêtes de sécurité, y compris la tenue des dossiers et le classement.

**Recommandations**

1. Que la Division des services d'accès et de contrôle des données révise le chapitre 3 du *Manuel des pratiques de sécurité* de Statistique Canada, conformément à la *Politique sur la sécurité du gouvernement du Canada* révisée, le fasse approuver par le Comité des politiques et diffuse largement les changements. Parmi les éléments clés figure l'examen de l'échéancier prévu pour les cotes de fiabilité, en vue d'améliorer les pratiques actuelles.

2. Que la Division des services d'accès et de contrôle des données, la Division des opérations des ressources humaines et la Direction des opérations régionales mettent leurs efforts en commun, en vue d'améliorer le contrôle et la gestion des enquêtes de sécurité sur le personnel, et rendent compte des résultats de façon périodique au Comité de la confidentialité et des mesures législatives.

3. Que les données sur la cote de sécurité et sa date d'expiration, dans le cas des employés et des personnes réputées être employées, soient entrées dans la base de données pertinente du Bureau par le personnel de la Sécurité seulement, conformément à la pratique exemplaire en place pour la base de données Global. Les bases de données auxquelles ces pratiques devraient être appliquées sont les suivantes : Système de paye des opérations des enquêtes statistiques pour les intervieweurs et base de données du Système de gestion de projets des centres de données de recherche, dont la mise à jour est assurée par le gestionnaire du Programme des centres de données de recherche et qui devrait inclure tous les chercheurs réputés être employés.

## IV. Conclusion

Dans le cas des employés nommés pour une période indéterminée, les procédures sont généralement conformes au chapitre 3 du *Manuel des pratiques de sécurité* de Statistique Canada, selon lequel une vérification de sécurité doit être effectuée avant l'entrée en fonction. Dans le cas des employés nommés pour une période déterminée et des intervieweurs, qui peuvent être nommés avant qu'une vérification approfondie de la fiabilité soit effectuée, afin de répondre aux besoins opérationnels, ainsi que des étudiants, qui peuvent être nommés avant qu'une vérification soit effectuée, nous concluons que le processus est conforme, même s'il pourrait être accéléré. Dans le cas des personnes réputées être employées visées par la vérification, nous n'avons pas pu déterminer le niveau de conformité en raison de considérations méthodologiques. L'accès aux comptes du système informatique est conforme à la norme relative à l'accès au réseau A (c'est-à-dire celle sur le contrôle de l'accès logique pour les comptes informatiques standard figurent dans le *Manuel des pratiques de sécurité*, chapitre 5).

# Annexe A – Plan d'action de la direction

| Recommandations | Plan d'action de la direction | Responsable | Date de réalisation prévue | Situation |
|---|---|---|---|---|
| 1. Que la Division des services d'accès et de contrôle des données révise le chapitre 3 du *Manuel des pratiques de sécurité* de Statistique Canada, conformément à la *Politique sur la sécurité du gouvernement du Canada* révisée, le fasse approuver par le Comité des politiques et diffuse largement les changements. Parmi les éléments clés figure l'examen de l'échéancier prévu pour les cotes de fiabilité, en vue d'améliorer les pratiques actuelles. | Les responsables de la SACD ont rencontré ceux des RH et ont reçu les commentaires des bureaux régionaux concernant les changements qui doivent être apportés à la Politique sur les enquêtes de sécurité. | SACD/RH | Octobre 2003 | Terminé |
| | Les responsables des RH effectuent une analyse approfondie des étapes du recrutement et entreprendront l'intégration dans les étapes remaniées de l'obligation de procéder à une enquête de sécurité pour tous les employés nommés pour une période indéterminée, les employés nommés pour une période déterminée, les employés occasionnels et les étudiants, avant leur entrée en fonction. | RH | Novembre 2003 | Continu |
| | Il faudra communiquer avec les cadres supérieurs, les professionnels des RH, les administrateurs et la sécurité de la SACD, afin que les changements nécessaires soient mis en œuvre. | RH/SACD | Mai 2004 | Planification de la stratégie de communication : janvier 2004 |
| | Des discussions devront se tenir avec l'équipe du Recensement de 2006 concernant les exigences en matière de cotes de sécurité pour les recenseurs de 2006. | RH/SACD/ Recensement | Mai 2004 | Déjà entrepris |

| Recommandations | Plan d'action de la direction | Responsable | Date de réalisation prévue | Situation |
|---|---|---|---|---|
| | La SACD proposera les changements qui doivent être apportés au *Manuel des pratiques de sécurité*. | SACD | Mai 2004 | Déjà entrepris |
| 2. Que la Division des services d'accès et de contrôle des données, la Division des opérations des ressources humaines et la Direction des opérations régionales mettent leurs efforts en commun, en vue d'améliorer le contrôle et la gestion des enquêtes de sécurité sur le personnel, et rendent compte des résultats de façon périodique au Comité de la confidentialité et des mesures législatives. | Élimination des cotes expirées dans le système GLOBAL. | Sécurité de la SACD | Novembre 2003 | L'arriéré a été éliminé en date de novembre 2003. Un examen doit être effectué sur une base mensuelle, et toutes les cotes qui doivent venir à expiration sous peu doivent faire l'objet de mesures deux mois avant la date d'expiration prévue. |
| | Élimination des cotes expirées dans le SPOES. | SACD/DOR | Août 2004 | Les travaux en vue d'éliminer l'arriéré doivent commencer en mars 2004. Un examen doit être effectué sur une base mensuelle, et toutes les cotes qui doivent venir à expiration sous peu doivent faire l'objet de mesures deux mois avant la date d'expiration prévue. |
| | Pratiques exemplaires | RH/SACD/DOR | Continu | Continu |

| Recommandations | Plan d'action de la direction | Responsable | Date de réalisation prévue | Situation |
|---|---|---|---|---|
| | Amélioration de la gestion par l'entremise des projets à venir de remaniement des systèmes administratifs. | RH/SACD | 2005 | Les RH/la SACD ont déterminé les besoins et les ont communiqués à l'équipe chargée du projet de remaniement. (Ils seront intégrés dans la proposition d'IRS des administrateurs.) |
| | Contrôle de la conformité | SACD | En cours | Mise à jour hebdomadaire et rapports mensuels, à partir d'octobre 2003<br><br>Rapport au comité approprié sur une base annuelle |
| 3. Que les données sur la cote de sécurité et sa date d'expiration, dans le cas des employés et des personnes réputées être employées, soient entrées dans la base de données pertinente du Bureau par le personnel de la Sécurité seulement, conformément à la pratique exemplaire en place pour la base de données Global. Les bases de données auxquelles ces pratiques devraient être appliquées sont les suivantes : Système de paye des opérations des enquêtes statistiques pour les intervieweurs et base de données du Système de gestion de projets des centres de données de recherche, dont la mise à jour est assurée par le gestionnaire du Programme des centres de données de recherche et qui devrait inclure tous les chercheurs réputés être employés. | SPOES<br><br>Base de données du système de gestion de projets des CDR | DOR/SACD<br><br>CDR/SACD | Août 2004<br><br>À déterminer | La SACD doit accéder au SPOES d'ici mars 2004, afin de commencer l'entrée de nouvelles données et de mettre à jour les données sur la sécurité.<br><br>Discussions en cours avec les gestionnaires des CDR. |