

February 2025

1243-1 (DGPCD)

DIRECTIVE FOR THE SEXUAL MISCONDUCT INCIDENT TRACKING SYSTEM (SMITS)

References: A. [CDS Directive for the Termination of Operation HONOUR, 9 May 2022](#)

B. [Directive on the Institutionalization of the Operation HONOUR Tracking and Analysis System \(OPHTAS\), 16 September 2019](#)

C. [CANFORGEN 089/24 CPCC 012/24 191450Z JUN 24](#)

D. DAOD 1002-3, Personal Information Management

E. DAOD 1002-6, Disclosure of Personal Information

F. DAOD 9005-1, Sexual Misconduct Response

SITUATION

1. **General.** In accordance with the CDS Directive for the Termination of Operation HONOUR (Ref A), the Operation HONOUR Tracking and Analysis System (OPHTAS) transitioned to the Sexual Misconduct Incident Tracking System (SMITS). This Directive supersedes Ref B and provides revised guidance. While SMITS is an updated version of OPHTAS, the intent of the system, its function and the data collected remain the same as OPHTAS. All data that was recorded in OPHTAS has been migrated into SMITS.

2. SMITS is a centralized system for units and organisations to record and track conduct deficiencies of a sexual nature, harassment of a sexual nature, and crimes of a sexual nature involving a CAF member as defined in Ref C, and formally reported to the chain of command (CoC). It serves as a central information source

février 2025

1243-1 (DGCDP)

DIRECTIVE SUR LE SYSTÈME DE SUIVI DES INCIDENTS D'INCONDUITE SEXUELLE (SSIIS)

Références : A. [Directive du CÉMD pour mettre fin à l'opération HONNEUR, 9 mai 2022](#)

B. [Directive sur l'institutionnalisation du système de suivi et d'analyse de l'opération HONNEUR \(SSAOPH\), 16 septembre 2019](#)

C. [CANFORGEN 089/24 CPCC 012/24 191450Z JUN 24](#)

D. DOAD 1002-3, Gestion des renseignements personnels

E. DOAD 1002-6, Divulgence de renseignements personnels

F. DOAD 9005-1, Intervention sur l'inconduite sexuelle

SITUATION

1. **Généralités.** Conformément à la Directive du CEMD pour mettre fin à l'opération HONOUR (réf. A), le Système de suivi et d'analyse de l'opération HONOUR (SSAOPH) passera au Système de suivi des incidents d'inconduite sexuelle (SSIIS). La présente directive remplace la réf. B et fournit des directives révisées. Malgré le fait que le SSIIS est une version améliorée du SSAOPH, l'intention du système, les fonctions de celui-ci et les données collectées restent les mêmes que dans le SSAOPH. Toutes les données conservées dans ce dernier seront déplacées vers le SSIIS.

2. Le SSIIS est un système centralisé permettant aux unités et organisations d'enregistrer et de suivre les écarts de conduite, le harcèlement et les infractions de nature sexuelle impliquant un membre des FAC tel que définis à la réf. C, et signalés officiellement à la chaîne de commandement (C de C). Il sert de

of conduct deficiencies of a sexual nature, harassment of a sexual nature, and crimes of a sexual nature in the CAF for the CoC. It also provides aggregated data reports to inform CAF and Department of National Defence (DND) leadership, the Government of Canada, and the public of the extent of sexual and gender-based violence in the CAF. This aggregated data for CAF and DND leadership will be used to affect systemic culture evolution to positively impact Defence Team members' job experience while improving the response for affected persons/victims.

3. **Problem Definition.** SMITS data must be accurate and up to date. All Level 1s (L1) must ensure that their subordinate L2/L3/L4 record all incidents formally reported to the unit/organisation's CoC within 48 hours (two working days) and update cases as new information becomes available up to and including case closure.

MISSION

4. All conduct deficiencies of a sexual nature, harassment of a sexual nature, and crimes of a sexual nature formally reported to the CoC involving a CAF member as an affected person or as a respondent will be recorded and updated in SMITS to ensure the DND/CAF leadership has access to decision making data IOT inform the development of effective policies and programs.

source d'information centrale sur les manquements à la conduite et les crimes de nature sexuelle dans les Forces armées canadiennes (FAC) pour la C de C. Il fournit des rapports de données regroupées pour informer les hauts dirigeants des FAC et du ministère de la Défense nationale (MDN), le gouvernement du Canada et le public de l'étendue de la violence sexuelle et fondée sur le genre au sein des FAC. Les données regroupées pour les hauts dirigeants des FAC et du MDN seront utilisées pour apporter des changements systémiques afin d'avoir une incidence positive sur l'expérience de travail des membres de l'Équipe de la Défense et d'améliorer l'intervention auprès des personnes affectées et des victimes.

3. **Définition du problème.** Les données du SSIIS doivent être exactes et à jour. Toutes les organisations de niveau 1 (N1) doivent s'assurer que leurs N2/N3/N4 subordonnées consignent tous les incidents signalés officiellement à la C de C de l'unité/organisation dans un délai de 48 heures (deux journées de travail) et qu'elles mettent à jour les dossiers dès que de nouveaux renseignements sont disponibles.

MISSION

4. Tous les manquements à la conduite, tous les cas de harcèlement et tous les crimes de nature sexuelle signalés officiellement à la C de C qui impliquent un membre des FAC en tant que personne affectée ou en tant qu'intimé seront consignés et mis à jour dans le SSIIS afin de garantir que les dirigeants du MDN/FAC aient accès aux données nécessaires à la prise de décision dans le but d'informer les décisions pour le développement de politiques et programmes efficaces.

EXECUTION

5. **Intent.** To ensure SMITS is the primary reliable source of information on sexual misconduct incidents formally reported to the CAF CoC.

6. **Responsibilities:**

a. CPCC:

- (1) CPCC is the overall administrator of SMITS;
- (2) CPCC has designated DGPCD as the SMITS Manager and assigned the overall responsibility for the system;
- (3) CPCC is the final vetting authority to grant access to the SMITS based on L1 recommendation;
- (4) CPCC, in cooperation with implicated L1s, will investigate any potential breaches of privacy or misuse of information; and
- (5) CPCC, as the L0 SMITS administrator, is the sole release authority for SMITS data. Any access to information or privacy requests received should be forwarded to CPCC for consideration.

EXÉCUTION

5. **Intention.** Faire en sorte que le SSIS soit la principale source d'information fiable sur les cas d'inconduite sexuelle signalés officiellement à la C de C des FAC.

6. **Tâches :**

a. CCPC :

- (1) le Chef – Conduite professionnelle et culture a la responsabilité générale du SSIS;
- (2) Le CCPC a nommé le DGCPD gestionnaire du SSIS et responsable de l'ensemble du système;
- (3) Le CCPC est l'autorité de vérification finale pour accorder l'accès au SSIS en fonction de la recommandation du N1;
- (4) Le CCPC, en collaboration avec les N1 en cause, enquêtera sur toute atteinte potentielle à la vie privée ou à l'utilisation abusive de renseignements; et
- (5) Le CCPC, en tant qu'administrateur du SSIS L0, est la seule autorité de diffusion des données du SMITS. Toute demande d'accès à l'information ou de protection des renseignements personnels reçue devrait être transmise au CCPC aux fins d'examen.

- b. All L1s: L1s are required through their L1 representatives and SMITS users to facilitate the use of the SMITS in accordance with Annexes A and B.

- b. Tous les N1 : Les N1 sont requis, par l'intermédiaire de leurs représentants de N1 et des utilisateurs SSIS de faciliter l'utilisation du SSIS conformément aux Annexes A et B.

7. Coordinating Instructions:

- a. SMITS Guidelines. Detailed instructions on the operation of SMITS are available in the [SMITS online user training](#);
- b. A [SMITS administration guide](#) is also available to assist users.
- c. SMITS is intended to maintain accurate awareness of instances of conduct deficiencies of a sexual nature, harassment of a sexual nature, and crimes of a sexual nature and their outcomes for the purposes of aggregate reporting and analysis. Tracking is to be done at an aggregate level and not at the individual level;
- d. The [SMITS Field Form](#) is available when connectivity to SMITS is not available;
- e. In cases where a single respondent is involved with multiple incidents on separate occasions, each incident will be recorded separately in SMITS. Incidents in which a single respondent is involved in a single incident that affects more than one person will be recorded as a single case in SMITS;

7. Instructions de coordination:

- a. Lignes directrices du SSIS. Des instructions détaillées sur le fonctionnement du SSIS sont disponibles dans la [formation de l'utilisateur SSIS en ligne](#),
- b. Un [guide d'administration SSIS](#) est également disponible pour aider les utilisateurs.
- c. Le SSIS a pour objet de tenir des dossiers exacts sur les cas de manquement à la conduite de nature sexuelle, de harcèlement de nature sexuelle et de crimes de nature sexuelle et sur leurs résultats, aux fins de rapports globaux et d'analyse. Les rapports sont établis à un niveau global et non à un niveau individuel,
- d. Le [formulaire de rapport du SSIS](#) est disponible lorsque la connexion au système n'est pas possible,
- e. Dans les cas où un seul intimé est concerné dans plusieurs incidents à des occasions distinctes, chaque incident doit être consigné séparément dans le SSIS. Les incidents qui concernent un seul intimé et un seul incident, et qui affectent plusieurs personnes seront consignés en un seul dossier dans le système,

- | | |
|---|---|
| <p>f. Incidents where the formally delegated CoC designates (i.e., that have formal powers to order an investigation) do not order an investigation to be conducted, or where the affected person does not want an investigation conducted, will still be required to be included in SMITS. These types of incidents are important for aggregate level reporting and program and policy development and review. Once a case is closed in SMITS, no personal information (affected person or respondent) will be available or searchable to users. L0 system administrators will be the only users able to see this information.</p> <p>g. Cases that ultimately prove to be unfounded are to be entered and updated in SMITS. These types of cases are important for aggregate level reporting and for policies and programs development and review. Individual SMITS case information shall not be used for any purpose other than recording, tracking, and updating for statistical purposes;</p> <p>h. The start date for the SMITS database is for incidents that occurred and were formally reported to the CoC starting on 1 April 2016. Incidents formally reported to the CoC on and after 1 April 2016 are to be included in</p> | <p>f. Les incidents pour lesquels les autorités officielles (p.ex. pouvoirs délégués formellement) de la C de C n'autorisent pas qu'une enquête soit menée ou pour lesquels la personne affectée ne désire pas qu'une enquête soit menée doivent tout de même être inscrits dans le SSIS. Ces types d'incident sont importants pour les rapports qui sont établis au niveau global et pour le développement et révision de programmes et politiques. Une fois qu'un cas est fermé à l'intérieur du SSIS, aucun renseignement personnel (personne affectée ou répondant) ne sera disponible ou consultable pour les utilisateurs. Les administrateurs du système au N0 seront les seuls utilisateurs capables de voir ces informations.</p> <p>g. Les cas qui s'avèrent, en fin de compte, à être non fondés doivent être consignés et mis à jour dans le SSIS. Ces types d'incident sont importants pour les rapports qui sont établis au niveau global et pour le développement et révision de programmes et politiques. Les informations relatives aux dossiers individuels dans SSIS doivent être utilisées exclusivement à des fins d'enregistrement, de suivi et de mise à jour à des fins statistiques,</p> <p>h. La base de données du SSIS sert à saisir tous les incidents qui ont eu lieu et ont été signalés officiellement à la C de C depuis le 1 avril 2016. Les incidents qui ont été signalés officiellement à la C de C le 1 avril 2016, ainsi qu'après cette date, doivent être consignés</p> |
|---|---|

SMITS, regardless of when the incident occurred;

dans le SSIS, peu importe la date à laquelle ils ont eu lieu,

- i. In accordance with ref D, the only personnel with access to SMITS cases are the SMITS users, designated CoC personnel, L1 OPIs, the DG PCD personnel responsible for SMITS operations, and the Director of Application Product Support and Delivery (DAPSD) personnel tasked with SMITS program development. SMITS uses a tiered access system: unit/organisation users can only see cases in their unit/organisation; L1 OPIs can only see cases in their L1; only DG PCD and DAPSD have access to the entire system. No other parties will be granted access to SMITS. All users with access to SMITS will sign a non-disclosure agreement to ensure adherence to the privacy safeguards in place;

- i. Conformément à la réf D, les seules personnes qui ont accès aux dossiers consignés dans le SSIS sont les utilisateurs de ce dernier, le personnel désigné de la C de C, les BPR de N1, le personnel du DGCPD qui s'occupe des opérations du système et le personnel du Directeur de support de la livraison des produits d'application (DSLPA) qui s'occupe de l'élaboration du programme du SSIS. Ce système repose sur un régime d'accès à paliers : l'utilisateur d'une unité/organisation ne peut accéder que les cas qui concernent cette dernière, les BPR de N1 ne peuvent lire que les cas de leur N1. Seuls le DGCDP et le DSLPA peuvent accéder tout le système. Aucun autre individu n'aura accès au SSIS. Tous les utilisateurs ayant accès au SSIS signeront une entente de non-divulgaration pour assurer le respect des mesures de protection de la vie privée en place,

- j. The proper use and storage of personal information recorded in SMITS is governed by the Privacy Act, DAOD 1002-6 and DAOD 6500-1. Any potential breaches of the Privacy Act will be referred to the appropriate authorities for investigation; and

- j. L'utilisation et l'entreposage appropriés des renseignements personnels consignés dans le SSIS sont régis par la Loi sur la protection des renseignements personnels, la DOAD 1002-6 et la DOAD 6500-1. Toute violation éventuelle de la Loi susmentionnée doit être signalée aux autorités compétentes aux fins d'enquête, et

k. Under the Privacy Act, SMITS data can be used for research purposes. Researchers will not be authorized to have direct access to SMITS. Research requests to be directed in writing to the SMITS Manager and will be considered on a case-by-case basis.

k. En vertu de la *Loi sur la protection des renseignements personnels*, les données du SSIS peuvent être utilisées à des fins de recherche. Les chercheurs ne pourront pas avoir un accès direct au système. Les demandes de recherche seront envoyées par écrit au gestionnaire du SSIS et seront examinées au cas par cas.

8. **CPCC POCs:**

- a. DG PCD, Marc Parent, Brigadier-General;
- b. DG PCD COS, Nick Torrington-Smith, Colonel;
- c. DG PCD PCDS Section Head, Rodney Dietzmann, Lieutenant-Colonel; and
- d. DG PCD PCDS Senior Staff Officer, Gregory Sabine-Pasley, Lieutenant-Commander.

8. **Personnes-ressources du CCPC :**

- a. DGCDP, Marc Parent, brigadier-général;
- b. CEM du DGCDP, Nick Torrington-Smith, colonel;
- c. Chef de section de la DCP du DGDCP, Rodney Dietzmann, lieutenant-colonel; et
- d. OSEM de la DCP du DGDCP, Gregory Sabine-Pasley, capitaine de corvette.

Chef de conduite professionnelle et culture

PREVOST, PAUL 284 Digitally signed by
PREVOST, PAUL 284
Date: 2025.02.04
17:28:56 -05'00'

J.P.R. Prévost
Lieutenant-General / lieutenant-général
Chief Professional Conduct and Culture

Annexes (next page)

Annexes (page suivante)

Annexes:

Annex A – Administration Guidelines for L1 Organizations and L2/L3/L4 Chains of Command

Annex B – Information Management and Storage

Distribution List

VCDS
CDRNORAD/DCDRNORAD
SJS DOS
Comd RCN
Comd CA
Comd RCAF
Comd MILPERSCOM
Comd CJOC
Comd CFINTCOM
Comd CANSOFCOM
Comd CPCC
JAG
CANMILREP NATO
DComd JFC Naples
ADM(DS)
ADM(Pol)
ADM(Mat)
ADM(Fin)/CFO
ADM(IE)
ADM(HR-Civ)
ADM(DRDC)
ADM(RS)
ADM(PA)
DND/CFLA
Corp Sec

Annexes:

Annexe A – Lignes directrices administratives pour les organisations de niveau 1 et les chaînes de commandement des N2/N3/N4

Annexe B – Gestion et stockage des informations

Liste de distribution

VCESD
Cmdt NORAD/CmdtA NORAD
DEM EMIS
Cmdt MRC
Cmdt AC
Cmdt ARC
Cmdt COMPERSMIL
Cmdt COIC
Cmdt COMRENSFC
Cmdt COMFOSCAN
Cmdt CCPC
JAG
CANMILREP NATO
CmdtA JFC Naples
SMA(SN)
SMA(Pol)
SMA(Mat)
SMA(Fin)/DPF
SMA(IE)
SMA(RH-Civ)
SMA(RDDC)
SMA(SE)
SMA(AP)
MDN/CJFC
Sec Gén

Annex A
1243-1 (DGPCD)
January 2025

**ADMINISTRATION GUIDELINES FOR L1S
AND L2/L3/L4 CHAINS OF COMMAND**

- A. [Privacy Act, R.S.C., 1985, c.P-21](#)
- B. Privacy Impact Assessment (PIA); Operation HONOUR Tracking & Analysis System (OPHTAS), 8 September 2020 (NOTAL)
- C. [Canadian Victims Bill of Rights \(S.C. 2015, c.13, s.2\)](#)
- D. DAOD 2008-3, Issue and Crisis Management

1. Tasks

a. All L1s:

- (1) All L1s are responsible for ensuring the proper administration of SMITS in all their subordinate organizations;
- (2) L1s shall appoint a SMITS OPI to administer the program and designate L2 and lower SMITS OPIs as required;
- (3) The minimum rank for SMITS OPIs is WO/PO1 for NCMs and Capt/Lt(N) for officers. Unit Human Resources Managers at the rank of Sgt/PO2 may also be appointed SMITS users. Civilian SMITS OPIs will be at an equivalent classification level; and

Annexe A
1243-1 (DGCDP)
janvier 2025

**LIGNES DIRECTRICES ADMINISTRATIVES
POUR LES ORGANISATIONS DE NIVEAU 1
ET LES CHAÎNES DE COMMANDEMENT DES
N2/N3/N4**

- A. [Loi sur la protection des renseignements personnels, L.R.C., 1985, ch. P-21](#)
- B. Évaluation des facteurs relatifs à la vie privée (EFVP), Système de suivi et d'analyse de l'opération HONOUR (SSAOPH), 8 septembre 2020 (non diffusé à tous)
- C. [Charte canadienne des droits des victimes \(L.C. 2015, ch. 13, art. 2\)](#)
- D. DOAD 2008-3, Gestion des problèmes et des crises

1. Tâches

a. Tous les N1:

- (1) Tous les N1 sont responsables de la bonne administration du SSIS dans toutes les organisations qui leur sont subordonnées,
- (2) Les N1 doivent nommer un bureau de première responsabilité (BPR) SSIS pour administrer le programme et désigner des BPR SSIS de N2 et inférieurs selon les besoins,
- (3) Le grade minimum pour les BPR SSIS est adjudant/maître de première classe pour les MR et capitaine/lieutenant de vaisseau pour les officiers. Les gestionnaires des ressources humaines d'unité au grade de sergent/maître de 2e classe peuvent également être désignés comme utilisateurs du SSIS. Les BPR civils du SSIS seront d'un niveau de classification équivalent, et

- (4) All L1s, through their appointed SMITS OPIs, shall record in SMITS all incidents of conduct deficiencies of a sexual nature, harassment of a sexual nature, and crimes of a sexual nature involving a CAF member formally reported to the CoC within 48 hours (two working days) of an incident being reported.

b. L2/L3/L4 CoC:

- (1) The CoC will inform their designated unit/organisation SMITS OPI whenever a conduct deficiency of a sexual nature, harassment of a sexual nature, or crime of a sexual nature is formally reported to them and provide the information required to record the case in SMITS;
- (2) All information concerning CAF members involved in conduct deficiencies of a sexual nature, harassment of a sexual nature, and crimes of a sexual nature must be documented in the SMITS as information becomes available;
- (3) IAW the Privacy Act (Ref A), the Privacy Impact Assessment (PIA) (Ref B) for the system, and the Canadian Victims Bill of Rights (Ref C), no personal information from SMITS shall be provided to anyone who does not have authority to have access to that SMITS case;

- (4) Tous les N1, par l'intermédiaire de leurs BPR SSIIS, doivent enregistrer dans SSIIS tous les incidents de manquements de conduite de nature sexuelle, de harcèlement de nature sexuelle et de crimes de nature sexuelle impliquant un membre des FAC, signalés officiellement à la chaîne de commandement, dans les 48 heures (deux jours ouvrables) suivant le signalement de l'incident.

b. C de C de N2/N3/N4:

- (1) La C de C informera le BPR SSIIS de leur unité/organisation chaque fois qu'un manquement de conduite de nature sexuelle, un harcèlement de nature sexuelle ou un crime de nature sexuelle leur est officiellement signalé et fournira les informations nécessaires pour enregistrer le cas dans le SSIIS,
- (2) Toutes les informations concernant les membres des FAC impliqués dans des manquements de conduite de nature sexuelle, du harcèlement de nature sexuelle et des crimes de nature sexuelle doivent être documentées dans le SSIIS au fur et à mesure que les informations deviennent disponibles,
- (3) Conformément à la Loi sur la protection des renseignements personnels (réf. A), à l'évaluation des facteurs relatifs à la vie privée (EFVP) (réf. B) pour le système, et la Charte canadienne des droits des victimes (réf.C), aucune information personnelle provenant du SSIIS ne doit être fournie à

quiconque n'ayant pas l'autorité d'accéder à ce dossier SSIIS,

- | | |
|---|---|
| <ul style="list-style-type: none">(4) CoCs should seek legal advice prior to including case information involving CAF members who are minors;(5) Access to SMITS data is intended to protect the privacy of all individuals whose data is entered in SMITS; and(6) SMITS cases shall be updated by the SMITS OPIs as new information becomes available. CoC shall ensure all available information is entered into the case until the case is closed. <p>c. The responsibilities of the L1 SMITS OPIs:</p> <ul style="list-style-type: none">(1) Complete SMITS training;(2) Ensure each subordinate L2/L3/L4 have sufficient designated SMITS OPIs;(3) Conduct regular audits of L1 SMITS accounts;(4) Request removal of SMITS access for OPIs who no longer need access to SMITS, or request creation of new SMITS accounts to CPCC DGPCD SMITS Manager;(5) Investigate issues of noncompliance with SMITS guidelines and directions and | <ul style="list-style-type: none">(4) La C de C devraient demander un avis juridique avant d'inclure des informations sur les cas impliquant des membres des FAC qui sont mineurs,(5) L'accès aux données du SSIIS vise à protéger la vie privée de toutes les personnes dont les données sont saisies dans le SSIIS, et(6) Les BPR SSIIS doivent mettre à jour les cas dans le SSIIS au fur et à mesure que de nouvelles informations deviennent disponibles. La C de C doit s'assurer que toutes les informations disponibles sont saisies dans le dossier jusqu'à ce que celui-ci soit fermé. <p>c. Les responsabilités des BPR SSIIS de N1:</p> <ul style="list-style-type: none">(1) Compléter la formation SSIIS;(2) S'assurer que chaque N2/N3/N4 subordonnée disposent d'un nombre suffisant de BPR SSIIS;(3) Effectuer des audits réguliers des comptes SSIIS du N1;(4) Demander que soit supprimer les comptes SSIIS pour les BPR qui n'ont plus besoin d'accéder à SSIIS, ou demander la création de nouveaux comptes SSIIS au gestionnaire SSIIS à l'intérieur de CCPC/DGCDP;(5) Enquêter les problèmes de non-conformité par rapport aux lignes directrices et aux directives du |
|---|---|

taking actions to correct those issues;	SSIIS et prendre des mesures correctrices appropriées pour ces problèmes;
(6) Conduct regular audits to ensure SMITS entries are completed correctly and are being updated in a timely manner;	(6) Effectuer des vérifications régulières pour s'assurer que les entrées à l'intérieur du SSIIS sont remplies correctement et qu'elles sont mises à jour en temps opportun;
(7) Remain current on SMITS changes and communicate this information to subordinate SMITS OPIs;	(7) Se tenir au courant des changements apportés au SSIIS et communiquer ces derniers aux BPR SSIIS subordonnés;
(8) Report SMITS issues to SMITS Manager (DGPCD);	(8) Signaler les problèmes SSIIS au gestionnaire SMITS (DGCDP) ;
(9) Complete SMITS statistical reports as requested by the L1; and	(9) Remplir les rapports statistiques du SSIIS à la demande du N1; et
(10) Represent the L1 at SMITS working groups and meetings.	(10) Représenter le N1 aux réunions et du groupes de travail du SSIIS.
d. The duties of L2 and below SMITS OPIs:	d. Les tâches des BPR SSIIS de N2 et subordonnés:
(1) Complete SMITS training;	(1) Compléter la formation SSIIS;
(2) Enter all available case information into SMITS within 48 hours (two working days) of the case being formally reported to the CoC. Complete information does not have to be available before creating a case;	(2) Saisir toutes les informations disponibles sur le cas dans le SSIIS dans les 48 heures (deux jours ouvrables) suivant la déclaration officielle du cas à la C de C. Les informations complètes n'ont pas besoin d'être disponibles avant de créer un cas;
(3) For incidents in which a significant incident report (SIR) or a commander's critical information requirement (CCIR) is created; refer to Reference D and include the SIR or CCIR as an attachment in the SMITS case;	(3) Pour les incidents pour lesquels un Rapport d'incident d'importance (RII) ou un besoin essentiel du commandant en information (BECI) est créé, se reporter à la référence D et inclure le RII ou le BECI en tant que pièce jointe dans le dossier SSIIS;

- | | |
|---|--|
| (4) Liaise with the reporting unit/organisation CoC to update missing case information; | (4) Collaborer avec la C de C de l'unité/organisation rapportrice afin de mettre à jour les informations manquantes du dossier; |
| (5) Update SMITS cases as soon as information is received; | (5) Mettre à jour les dossiers SSIS dès que d'autres informations sont reçues; |
| (6) Follow up on cases to ensure that information is complete and that fields are populated before requesting case closure; | (6) Faire un suivi des dossiers pour s'assurer que les informations sont complètes et que les champs sont remplis avant de demander la clôture du dossier; |
| (7) Inform the L1 SMITS OPI of any problems or issues with SMITS; and | (7) Informer le BPR SSIS de N1 de tout problème ou de toute question concernant le SSIS; et |
| (8) Direct any ATIP requests or requests for personal information to the L0 SMITS Administrator through the L1 OPI. | (8) Diriger toute demande d'AIPRP ou demande de renseignements personnels vers l'administrateur L0 SSIS par l'entremise du BPR de N1. |

Annex B
1243-1 (DGPCD)
January 2025

INFORMATION MANAGEMENT AND STORAGE

- A. [Privacy Act, R.S.C., 1985, c.P-21](#)
- B. Privacy Impact Assessment (PIA); Operation HONOUR Tracking & Analysis System (OPHTAS), 8 September 2020 (NOTAL)
- C. [Canadian Victims Bill of Rights \(S.C. 2015, c.13, s.2\)](#)

1. Restraints:

- a. L1 or subordinate L2/L3/L4s are not authorized to opt out of using SMITS to record an incident of conduct deficiencies of a sexual nature, harassment of sexual nature, and crimes of a sexual nature formally reported to the CoC. Every incident formally reported to the CoC shall be recorded, updated and closed based on CoC actions;
- b. Individual SMITS case information shall not be used for any purpose other than incident recording, tracking, and updating for statistical purposes only;
- c. IAW the Privacy Act (Ref A), the Privacy Impact Assessment (PIA) (Ref B) for the system, and the Canadian Victims Bill of Rights (Ref C), no personal information from SMITS shall be provided to anyone who does not have authority to have access to that SMITS case; and

Annexe B
1243-1 (DGPCD)
janvier 2025

GESTION ET STOKAGE DE L'INFORMATION

- A. [Loi sur la protection des renseignements personnels, L.R.C., 1985, ch. P-21](#)
- B. Évaluation des facteurs relatifs à la vie privée (EFVP), Système de suivi et d'analyse de l'opération HONOUR (SSAOPH), 8 septembre 2020 (non diffusé à tous)
- C. [Charte canadienne des droits des victimes \(L.C. 2015, ch. 13, art. 2\)](#)

1. Contraintes:

- a. Les N1 ou les N2/N3/N4 subordonnées ne sont pas autorisés à se soustraire à l'utilisation du SSIIS pour enregistrer un incident de manquement à la conduite de nature sexuelle, de harcèlement de nature sexuelle et de crimes de nature sexuelle signalés officiellement à la C de C. Chaque incident signalé officiellement à la C de C doit être enregistré, mis à jour et clôturé en fonction des actions de la C de C;
- b. Les informations individuelles des dossiers SSIIS ne doivent être utilisées qu'à des fins d'enregistrement, de suivi et de mise à jour des incidents à des fins statistiques uniquement;
- c. Conformément à la Loi sur la protection des renseignements personnels (réf. A), à l'Évaluation des facteurs relatifs à la vie privée (EFVP) (réf. B) pour le système, et à la Charte canadienne des droits des victimes (réf. C), aucune information personnelle provenant du SSIIS ne doit être fournie à quiconque n'a pas l'autorité d'accéder à ce dossier SSIIS; et

- | | |
|---|--|
| <p>d. SMITS users who generate aggregate reports using SMITS data shall not produce reports which allow individuals to be identified through the information in the report.</p> | <p>d. Les utilisateurs du SSIS qui génèrent des rapports agrégés à partir des données du SSIS ne doivent pas produire de rapports permettant d'identifier des individus à partir des informations contenues dans le rapport.</p> |
|---|--|