NRC·CNRC

Addendum / Addenda

No./No
1

Project Description / Description de projet		
Smart Building Monitoring and On-Going Commissioning - Borden		
Solicitation No./N° de solicitation 17-22058	Project No./N° de projet	W.O. No./N° d'ordre de travail
Departmental Representative / représentant ministériel Scott Shillinglaw		Date October 23, 2017

Notice:	**Nota**:
This addendum shall form part of the tender documents and all conditions shall apply and be read in conjunction with the original plans and specifications.	Cet addenda fait partie intégrale des dossiers d'appel; toutes les conditions énoncées doivent être lues et appliquées en conjonction avec les plans et les devis originaux.

1 Questions and Answers
2 Summary Table with available building data
3 Appendix C: Mandatory Requirement Checklist for SoR – add01
4 Memorandum
5 SRCL
6 National Defence Security Orders & Directives Chapter 8: Industrial and Contract Security

17-22058 – Smart Building Monitoring and On-going Commissioning – Borden

Question and Answer

1. Can NRC/DND provide the annual Energy use (MJ) for each Primary Building?

Answer: See attached revised summary table with available building data.

2. Can NRC/DND provide the annual Energy Costs ($) for each Primary Building?

Answer: See attached revised summary table with available building data.

3. Will NRC award all three solicitations 17-22057, 17-22058 and 17-22059 to a single successful bidder?

Answer: These RFPs are all individual open processes and will be conducted as such.

4. NRC Requests Section 1.0 PRESENTATIONS OF PROPOSALS four copies of Techincal Proposals and two copies of Financial Proposals and in "APPENDIX A" Statement of Requirements NRC requests one(1) Original Submission, One(1) electronic submission and six(6) hard copies in organized in three ring binder. Can NRC confirm how many copies and what format is required of each Technical and Financial Proposals.

Answer: The information in Section 1.0 PRESENTATION OF PROPOSALS is the appropriate format for this RFP. We require four (4) copies of a Technical Proposal and two (2) copies of the Financial Proposal in two (2) separate envelopes. One envelope must be clearly marked "Technical Proposal" and the other envelope must be marked "Financial Proposal".

5. Will NRC be awarding contract to single successful bidder for each proposal?

Answer: NRC will award a contract to the successful bidder.

6. Can NRC verify and confirm which measurement intervals are required as Mandatory for BAS Data Collection and Energy Meter Data Collection. In section 2.3 and 2.4 of "Appendix A" NRC request is 15 minutes or less and 60 minutes of less respectively. In "Appendix C" Mandatory Requirements and Checklist NRC request for the same section 2.3 and 2.4 one (1) minute interval and fifteen (15) respectively.

Answer: The attached document entitled "Appendix C: Mandatory Requirement Checklist for SoR – add01" replaces the document in the RFP entitled "Appendix C: Mandatory Requirement Checklist for SoR". Refer to Appendix C: Mandatory Requirement Checklist for SoR – add01.

7. The Mandatory Requirement Checklist has a column titled "Reference to Statement of Work". Is this different from the Statement of Requirements?

Answer: The attached document entitled “Appendix C: Mandatory Requirement Checklist for SoR – add01” replaces the document in the RFP entitled “Appendix C: Mandatory Requirement Checklist for SoR”. Refer to Appendix C: Mandatory Requirement Checklist for SoR – add01.

8. The Mandatory Requirement Checklist has a mandatory requirement for “Work orders generated based on outputs of the FDD system”. Please clarify if this is a requirement for the specified system to generate work orders from the recommendations, or a requirement to export recommendations to an existing third party work order system. Please specify which 3rd party work order system if applicable.

Answer: The attached document entitled “Appendix C: Mandatory Requirement Checklist for SoR – add01” replaces the document in the RFP entitled “Appendix C: Mandatory Requirement Checklist for SoR”. Refer to Appendix C: Mandatory Requirement Checklist for SoR – add01. Also refer to SoR, Item 4.G. Yes, the solution must export anomaly corrections to a third party system using open source protocols and formats.

9. Can NRC confirm work begin date. In Section 3.0 PERIOD OF CONTRACT the begin date is November 6, 2017 completed March 31, 2018 and in “Appendix C” Mandatory Requirements Checklist award date is January 8, 2018

Answer: The date of November 6th, 2017 was an estimated date for contract award. Contract award will be complete by November 10, 2017. This should be sufficient time to evaluate and score the bids. The attached document entitled “Appendix C: Mandatory Requirement Checklist for SoR – add01” replaces the document in the RFP entitled “Appendix C: Mandatory Requirement Checklist for SoR”. Refer to Appendix C: Mandatory Requirement Checklist for SoR – add01.

10. Can NRC confirm the duration of the contract award regardless of the starting date confirmation request

Answer: Contract award is dependent on how long it takes to review, score and determine the successful candidate. We are setting November 10, 2017 as our date for contract award. Proposals submitted must be valid for not less than sixty (60) calendar days from the closing date of the RFP. System installation and implementation must be completed by March 2nd, 2018

11. Can you please provide BAS as-built drawings for all buildings to help us determine the size and scope of the BAS?

Answer: Not available.

12. Does the Johnson Controls BAS in B605- TEME currently communicate between control panels using BACnet Protocol? Do all devices have unique IDs?

Answer: Not applicable.

13. Can the Crown clarify that in Appendix C "Mandatory and Rated Requirements, within the Mandatory Requirement Checklist table, that Bidder's Mandatory response only needs to address for Section 2 "Mandatory Requirements – Scope of Work", the items in the column under Mandatory Requirements, instated of all the items within Section 2?

Answer: The attached document entitled "Appendix C: Mandatory Requirement Checklist for SoR – add01" replaces the document in the RFP entitled "Appendix C: Mandatory Requirement Checklist for SoR". Refer to Appendix C: Mandatory Requirement Checklist for SoR – add01.

14. Appendix C "Mandatory and Rated Requirements", Mandatory Requirements Checklist table item 1.17 – 2.12 States: "Minimum system availability: 99% during operating hours and". Please clarify if additional wording is required after the word "and" or should the word "and" be removed?

Answer: The attached document entitled "Appendix C: Mandatory Requirement Checklist for SoR – add01" replaces the document in the RFP entitled "Appendix C: Mandatory Requirement Checklist for SoR". Refer to Appendix C: Mandatory Requirement Checklist for SoR – add01.

15. Could we respectfully request a three week extension for this submission?

Answer: No.

16. What are the DND Security and privacy policies?

Answer: Refer to the attached SRCL, Memorandum, National Defence Security Orders & Directives Chapter 8: Industrial and Contract Security, and all other documents referenced in the above noted documentation.

Contractors will be forbidden to engage or enter secret zones. Everything under the Assistant Deputy Minister, Infrastructure and Environment, is to be considered confidential unless it is cleared to be shared. All Bases, Wings, Detachments and Stations are military establishments and are defined under the Defence Act and under the jurisdiction of the Base Commander and the Military Police. Any individual who does not comply with security requests can be arrested and held.

These National Defence Security Orders and Directives (NDSODs) are issued under the authority of the Director General Defence Security (DGDS) for the Department of National Defence (DND) and the Canadian Armed Forces (CAF). These NDSODs are intended for use only by the DND and the CAF and are not for distribution to the public. The NDSODs can be, on a required basis, shared with contractors who have entered into an active contract (or future contract) with the DND or the CAF. Only the relevant portions of the NDSODs are to be disclosed. Any inquiries concerning the security and proper handling of these NDSODs are to be sent to Director Defence Security Policy, Training and Awareness at DND.DGDSPolicies-DGSDPolitiques.MDN@forces.gc.ca<mailto:DND.DGDSPolicies-DGSDPolitiques.MDN@forces.gc.ca>

Upon award of the contract, the successful Bidder's appointed CSO (Company Security Officer) and possibly an approved alternate (ACSO) shall immediately contact the appropriate authorities at PSPC(PWGSC)/DND and follow the PWGSC/PSPC ISM (Industrial Security Manual) to complete and submit the required site access documentation for their staff.

If the successful Bidder chooses to hire sub-contractors (SRCL 10(b) says any contractor used requires Reliability), the CSO must complete a sub-SRCL for each sub-contracted company and submit to PSPC(PWGSC)/DND. Once the SCRL is awarded, the CSO for each of the sub-contractors shall immediately contact the appropriate authorities at PSPC(PWGSC)/DND and follow the PWGSC/PSPC ISM (Industrial Security Manual) to complete and submit the required site access documentation for their staff.

Item No. 1.26 of the Mandatory Requirements Checklist: In the schedule submitted with the bid, the prime Bidder shall account for one month to submit and finalize the SRCL and Request for Visit (RFV), and receive a valid Visit Clearance Request (VCR) for their staff. The schedule submitted with the bid shall also account for two months for any sub-contractors to receive a valid VCR for staff (including one month for the SRCL and one month for the RFV/VCR).

17. What are the DND approved network connectivity methods?

Answer: Cellular communication with VPN setup.

18. In Appendix C: Mandatory and Rated Requirements Check List: in the matrix, there is no reference to section 2.17. Please confirm if this was intentional

Answer: Yes

19. For Appendix A, Section 2.18: Do we need to provide security clearance information of our sub-contractors when submitting the RFP?

Answer: Yes

20. May we have additional detail on what is required for API export to third party system (Section 2.2B)

Answer: Energy meter data and anomaly correction data.

17-22059 – Surveillance de bâtiments intelligents et mise en service continue – Borden

Questions et réponses

1. Le CNRC/MDN fournissent-ils la consommation d'énergie (MJ) annuelle pour chaque bâtiment principal ?

Réponse : Voir le tableau récapitulatif révisé annexé avec les données disponibles sur le bâtiment.

2. Le CNRC/MDN peuvent-ils fournir les coûts énergétiques annuels ($) pour chaque bâtiment principal ?

Réponse : Voir le tableau récapitulatif révisé annexé avec les données disponibles sur le bâtiment.

3. Le CNRC octroiera-t-il les trois demandes 17-22057, 17-22058 et 17-22059 à un seul soumissionnaire ?

Réponse : Ces DP sont des processus individuels et seront traitées en tant que tels.

4. Le CNRC demande dans la Section 1.0 PRÉSENTATIONS DES PROPOSITIONS quatre copies des propositions techniques et deux copies des propositions financières, puis dans l'ANNEXE A Enoncé des exigences , le CNRC demande une (1) soumission originale, une (1) soumission électronique et (6) copies papier reliées dans un classeur à trois anneaux. Le CNRC peut-il confirmer le nombre de copies nécessaires et le format requis pour les propositions techniques et financières.

Réponse : L'information correcte est celle de la Section 1.0 PRÉSENTATIONS DES PROPOSITIONS : nous demandons quatre copies (4) d'une proposition technique et deux (2) copies des propositions financières dans deux (2) enveloppes séparées. Inscrire clairement « Proposition technique » sur l'enveloppe et « Proposition financière » sur l'autre.

5. Le CNRC attribuera-t-il le contrat à un seul soumissionnaire pour chaque proposition ?

Réponse : Le CNRC attribuera le contrat au soumissionnaire retenu.

6. Le CNRC vérifie et confirme les intervalles de mesure requis dans Collecte de données de SAB et Collecte de données du compteur énergétique. Dans les sections 2.3 et 2.4 de l'Annexe A, la demande du CNRC est de 15 minutes ou moins et 60 minutes ou moins, respectivement. Dans l'Annexe C, Exigences obligatoires et liste de contrôle, pour les mêmes sections 2.3 et 2.4 la demande du CNRC est un intervalle de une (1) minute et quinze (15), respectivement.

Réponse : le document annexé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01* remplace le document de la DP intitulé *Annexe C : Liste de contrôle des exigences obligatoires pour*

SoR. Référez-vous au document *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01*.

7. La liste de contrôle des exigences obligatoires contient une colonne intitulée Référence à l'énoncé des travaux. Est-ce différent de l'Enoncé des exigences ?

Réponse : le document annexé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01* remplace le document de la DP intitulé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR*. Référez-vous au document *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01.*

8. La liste de contrôle des exigences obligatoires contient une exigence obligatoire pour les « Ordres de travaux générés en fonction des résultats du système FDD ». Veuillez clarifier si cela est une exigence pour le système spécifié de générer des ordres de travaux à partir des recommandations ou une exigence pour exporter des recommandations à un système d'ordre de travaux d'une tierce partie existante. Veuillez spécifier quel système d'ordre de travaux d'une tierce partie est applicable.

Réponse : le document annexé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01* remplace le document de la DP intitulé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR*. Référez-vous au document *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01.* Référez-vous également au SoR, article 4.G. Oui, la solution doit exporter les corrections d'anomalies à un système de tierce partie en utilisant les protocoles et formats source ouverts.

9. Le CNRC peut-il confirmer la date de début des travaux. Dans la section Section 3.0 PERIODE DU CONTRAT la date de début est le 6 novembre 2017 jusqu'au 31 mars 2018 et dans l'Annexe C, la date de vérification des exigences obligatoires est le 8 janvier 2018.

   Réponse : La date du 31 octobre 2017 est une date d'estimation de l'attribution du contrat. L'attribution du contrat sera complète d'ici le 10 novembre 2017. Cela devrait être suffisant pour évaluer et noter les soumissions. Le document annexé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01* remplace le document de la DP intitulé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR*. Référez-vous au document *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01*.

10. Le CNRC peut-il confirmer la durée de l'attribution du contrat indépendamment de la demande de confirmation de la date de début.

    Réponse : L'attribution du contrat dépend du temps qu'il faudra pour revoir, noter et déterminer le candidat retenu. Nous fixons au 10 novembre 2017 la date de l'attribution du contrat. Les propositions soumises doivent être valides pendant au moins soixante (60) jours civils à partir de la date de fermeture de la DP. L'installation et la mise en œuvre du système doivent être complétées d'ici au 2 mars 2018.

11. Pouvez-vous fournir les dessins des ouvrages finis du SAB pour tous les bâtiments afin de nous aider à déterminer la taille et la portée du SAB ?

Réponse : Non disponible.

12. Le SAB de Johnson Controls dans B605- TEME communique-t-il actuellement entre les panneaux de contrôle à l'aide du protocole BACnet ? Chaque dispositif a-t-il un ID distinct ?

Réponse : n'est pas applicable

13. La couronne peut-elle clarifier que dans l'Annexe C Exigences cotées et obligatoires, dans le tableau Liste de contrôle des exigences obligatoires, la réponse obligatoire du soumissionnaire ne doit répondre pour la section 2 « Exigences obligatoires – Portée des travaux », qu'aux articles de la colonne Exigences obligatoires et non à tous les articles de la section 2 ?

Réponse : le document annexé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01* remplace le document de la DP intitulé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR*. Référez-vous au document *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01*.

14. Annexe C Exigences obligatoires et cotées, article 1.17 – 2.12 du tableau Liste de contrôle des exigences obligatoires indique : « Disponibilité système minimum : 99 % pendant les heures de fonctionnement et ». Veuillez clarifier s'il doit y avoir un ajout après le mot « et » ou si le mot « et » doit être enlevé ?

Réponse : le document annexé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01* remplace le document de la DP intitulé *Annexe C : Liste de contrôle des exigences obligatoires pour SoR*. Référez-vous au document *Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01*.

15. Pouvons-nous demander 3 semaines de plus pour cette soumission ?

Réponse : Non.

16. Quelles sont les politiques du MDN en matière de sécurité et de confidentialité ?

Réponse : Veuillez vous référer au document annexé *SRCL, Memorandum, National Defence Security Orders & Directives Chapter 8: Industrial and Contract Security*, et à tous les autres documents référencés dans la documentation susmentionnée.

Les entrepreneurs n'auront pas le droit d'entrer dans certaines zones confidentielles. Tout ce qui dépend du sous-ministre adjoint, Infrastructure et environnement, doit être considéré comme confidentiel sauf suppression du caractère confidentiel. Toutes les bases, ailes, détachements et stations sont des établissements militaires définis dans le cadre de la loi sur la défense et sous la

juridiction du commandant de la base et de la police militaire. Tout individu qui ne répondrait pas aux exigences de sécurité pourrait être arrêté et détenu.

Ces *Ordonnances et directives de sécurité de la Défense nationale* (ODSDN) sont publiées sous l'égide du directeur général – Sécurité de la défense (DGSD) pour le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC). Ces ODSDN visent à être utilisées par le MDN et les FAC uniquement et ne doivent pas être diffusées au public. Les ODSDN peuvent être, sur une base régulière, partagées avec les entrepreneurs qui ont un contrat actif (ou auront) avec le MDN ou les FAC. Seules les parties pertinentes des ODSDN peuvent être divulguées. Toutes questions au sujet de la sécurité et de la bonne gestion des ces ODSDN doivent être adressées au Directeur – Politique, instruction et sensibilisation (Sécurité de la défense) à l'adresse DND.DGDSPolicies-DGSDPolitiques.MDN@forces.gc.ca<mailto:DND.DGDSPolicies-DGSDPolitiques.MDN@forces.gc.ca>

Une fois le contrat attribué, l'agent de sûreté de la compagnie (CSO) du soumissionnaire choisi ainsi qu'un agent subalterne éventuel (ACSO) contacteront immédiatement les autorités concernées au SPAC (TPSGC)/MDN et suivront le MSI (manuel de la sécurité industrielle) du TPSGC/SPAC afin de remplir et soumettre les documents requis pour l'accès au site de leurs employés.

Si le soumissionnaire retenu décide d'employer des entrepreneurs sous-traitants (LVERS 10(b) stipule que tout entrepreneur utilisé requiert une cote de fiabilité), le CSO doit remplir une sous-LVERS pour chaque entreprise sous-contractée et la soumettre au SPAC (TPSGC)/MDN. Une fois la LVERS accordée, le CSO pour chaque sous-traitant devra immédiatement contacter les autorités appropriées au SPAC (TPSGC)/MDN et suivre le MSI (manuel de la sécurité industrielle) du TPSGC/SPAC afin de remplir et soumettre les documents requis pour l'accès au site de leurs employés.

Article n° 1.26 de la liste de contrôle des exigences obligatoires : dans le calendrier soumis avec la soumission, le premier soumissionnaire devra compter un mois pour soumettre et finaliser la LVERS et la demande de visite (RFV), et recevoir une Demande de permis de visite (VCR) valide pour ses employés. Le calendrier soumis avec la soumission devra aussi compter deux mois afin que toute entreprise sous-traitante reçoive un VCR valide pour ses employés (dont un mois pour la LVERS et un mois pour le RFV/VCR).

17. Quelles sont les méthodes de connexion au réseau approuvées par le MDN ?

Réponse : Communication cellulaire avec VPN.

18. À l'annexe C: Liste de vérification des exigences obligatoires et cotées: dans la matrice, il n'y a pas de référence à l'article 2.17. S'il vous plaît confirmer si c'était intentionnel.

Réponse : Oui.

19. Pour l'annexe A, section 2.18: Devons-nous fournir des renseignements sur l'habilitation de sécurité de nos sous-traitants lors de la soumission?

Réponse : Oui.

20. Peut-on avoir plus de détails sur les exigences pour exporter via API vers une tierce partie (Section 2.2B)

Réponse : données compteur énergétique et données correction anomalies

National Defence / Défense nationale

DND Smart Building Pilot 2017/18 - add01

Base	Building	Type	Built (approximate)	Clearance	Gross Floor Area (m2)	Estimated Electricity		Estimated Heating energy				Vendor/MFG	BAS			Environmental Cert.
						kWh	Costs	Type	Volume	Unit	Costs		Estimated Number of Points	Remotely Monitored	On Other Network	
CFB Borden	S-164	Curtiss Mess Hall	5 yrs ago	Reliable	5,003	2,364,806	$276,682	Steam	NA	NA	NA	JCI (BACNET)	1,200	No	No	Designed LEED Silver
CFB Borden	S-165	School/ Administrative	1 yr ago	Reliable	12,800	NA	NA	Gas	NA	NA	NA	JCI (BACNET)	3,200	No	No	Designed LEED Silver
CFB Borden	T-169	Vickers Mess Hall	4 yrs ago	Reliable	5,161	5,157,108	$603,381	Steam	NA	NA	NA	JCI (BACNET)	1,200	No	No	Designed LEED Silver

Appendix C: Mandatory Requirement Checklist for SoR – add01

1. Mandatory Requirement Checklist

In order to receive consideration by NRC and DND, all proposals must respond to the following mandatory requirements and must include the referenced Section/Page in Bidder's proposal. Any proposal that fails to indicate clearly that all mandatory requirements have been met will receive no further consideration.

The following table must be completed and included with the offer.

Item No.	Reference to Statement of Requirements	Mandatory Requirements	Compliant (Yes/No)	Referenced Section/ Page in Bidder's Proposal
1.1		Access through Web services for 3rd party applications to retrieve energy data and anomaly correction data		
1.2	2.1	All requirements in section 2.1 General		
1.3	2.2	All requirements in section 2.2 Components and services		
1.4	2.3	All requirements in section 2.3 Building Automation System (BAS) Data Collection		
1.5	2.4	All requirements in section 2.4 Energy Meter Data Collection		
1.6	2.5	All requirements in section 2.5 Building Data Analytics and Fault Detection and Diagnostics		
1.7	2.5	The Subject Matter Expert must review anomaly corrections before they are issued to DND. The subject matter expert must be a Professional Engineer licensed in the Province that the site work is being conducted.		
1.8	2.5	Fault detection & diagnostics (FDD) as defined in Section 2.5 Building Data Analytics and Fault Detection and Diagnostics		
1.9	2.6	All requirements in section 2.6 Continuous Commissioning and Building Optimization		
1.10	2.6	Capability of continuous commissioning		
1.11	2.7	All requirements in section 2.7 User Interface		
1.12	2.8	All requirements in section 2.8 Demonstration of Targeted Savings		
1.13	2.9	All requirements in section 2.9 Data Visualisation		
1.14	2.9	Anomaly corrections prioritized according to their impacts		

1.15	2.10	All requirements in section 2.10 Building Maintenance Service Performance Monitoring		
1.16	2.11	All requirements in section 2.11 Reporting		
1.17	2.12	All requirements in section 2.12 System Availability, Scalability, and Interoperability		
1.18	2.12	Scalability to additional buildings		
1.19	2.13	All requirements in section 2.13 System Security, Privacy, and Data Sovereignty		
1.20	2.14	All requirements in section 2.14 Ownership and Retention of Collected Data		
1.21	2.15	All requirements in section 2.15 Turnkey solution		
1.22	2.15	FDD system configured and updated, as required, by the vendor, without support from DND		
1.23	2.16	All requirements in section 2.16 System Maintenance. Hardware and software updates covered under the annual fee		
1.24	2.18	All requirements in section 2.18 Security Clearance		
1.25	2.19	All requirements in section 2.19 Health and Safety		
1.26	2.20	All requirements in section 2.20 Coordination and Schedule Selected Bidder shall be ready to provide the services as required (i.e. facilities and personnel already in place). The Bidder shall confirm that they have adequate staff available for the duration of the contract to ensure all work is complete and issues resolved in such a way that the installations are complete and data is being received by March 2nd, 2018. Assume that site access will commence by January 8th, 2018. The Bidder shall submit a proposed schedule with their bid. The Bidder shall confirm that they are capable of conducting site visits for troubling shooting and repair within 24 hours of learning that the data acquisition system is malfunctioning.		
1.27	RFP Section 7.0	A fixed price including a full cost breakdown and hourly rates of all staff categories		

2. Rated Requirements

Offers that meet all the mandatory technical criteria will be evaluated and scored as specified in the tables inserted below.

Proposals achieving 85 or higher technical points and the minimum points for each individual technical requirement will then be evaluated on financial information and price.

Each point rated technical criterion shall be addressed separately.

In order to qualify for the rating process, proposals must respond to the following rated requirements and must include the referenced Section/Page in the Bidder's proposal.

The following table must be completed and included with the offer.

	Rated Technical Requirements	**Points**		**Referenced Section/ Page in Bidder's Proposal**
		Max.	**Min.**	
2.1	Data collection including BAS data and energy data, and data sovereignty	15	10	
2.2	Building data analytics, fault detection and diagnosis	20	12	
2.3	Dashboards / user interfaces	15	8	
2.4	System installation, integration, and connectivity	15	8	
2.5	System scalability, interoperability, and APIs	10	5	
2.6	Monitoring of maintenance service providers' performance	10	5	
2.7	Continuous commissioning and building optimization	5	3	
2.8	Savings calculation capability	5	3	
2.9	Content and quality of reporting	5	3	
2.10	Corporate expertise & experience	10	5	
2.11	Implementation schedule and milestones	5	3	
2.12	Service levels and KPIs as proposed by the Bidder	5	3	
2.13	Customer service	5	3	
	TOTAL TECHNICAL POINTS:	**125**	**85**	

Annexe C : Liste de contrôle des exigences obligatoires pour SoR – ajout 01

1. Liste de contrôle des exigences obligatoires

Afin d'être prises en compte par le CNRC et le MDN, toutes les propositions doivent répondre aux exigences obligatoires suivantes et doivent contenir la section/page référencée dans la proposition du soumissionnaire. Toute proposition qui n'indiquera pas clairement que toutes les exigences obligatoires ont été respectées sera écartée.

Le tableau suivant doit être rempli et annexé à l'offre.

Article n°	Référence à l'énoncé des travaux	Exigences obligatoires	Conforme (Oui/Non)	Section/Page référencée dans la proposition du soumissionnaire
1.1		Accès via le Web aux applications tierces afin d'extraire les données énergétiques et celles des corrections d'anomalies		
1.2	2.1	Toutes les exigences de la section 2.1 Général		
1.3	2.2	Toutes les exigences de la section 2.2 Composants et services		
1.4	2.3	Toutes les exigences de la section 2.3 Collecte de données par le système d'automatisation du bâtiment (SAB)		
1.5	2.4	Toutes les exigences de la section 2.4 Collecte de données des compteurs énergétiques		
1.6	2.5	Toutes les exigences de la section 2.5 Analyse des données du bâtiment et Détection des défauts et diagnostics (BDA/FDD)		
1.7	2.5	Examen des corrections d'anomalies par l'expert en la matière avant qu'elles ne soient transmises au MDN. L'expert en la matière doit être un ingénieur professionnel agréé dans la province où sera effectué le travail.		
1.8	2.5	Détection des défauts et diagnostics (FDD) tel que défini dans la section 2.5, Analyse des données du bâtiment et Détection des défauts et diagnostics		
1.9	2.6	Toutes les exigences de la section 2.6 Mise en service continue et optimisation du bâtiment		
1.10	2.6	Capacité de mise en service continue		
1.11	2.7	Toutes les exigences de la section 2.7 Interface utilisateur		
1.12	2.8	Toutes les exigences de la section 2.8 Démonstration des économies ciblées		
1.13	2.9	Toutes les exigences de la section 2.9 Visualisation des données		
1.14	2.9	Corrections des anomalies hiérarchisées en fonction de leurs impacts		

1.15	2.10	Toutes les exigences de la section 2.10 Surveillance de la performance des services de maintenance		
1.16	2.11	Toutes les exigences de la section 2.11 Rapports		
1.17	2.12	Toutes les exigences de la section 2.12 Disponibilité, adaptabilité et interopérabilité du système		
1.18	2.12	Adaptabilité à d'autres bâtiments		
1.19	2.13	Toutes les exigences de la section 2.13 Sécurité du système, confidentialité et souveraineté des données		
1.20	2.14	Toutes les exigences de la section 2.14 Propriété et rétention des données collectées		
1.21	2.15	Toutes les exigences de la section 2.15 Solution clé en main		
1.22	2.15	Système FDD configuré et mis à jour, tel que requis par le vendeur, sans soutien du MDN		
1.23	2.16	Toutes les exigences de la section 2.16 Maintenance du système. Mises à jour matériel et logiciel comprises dans les frais annuels		
1.24	2.18	Toutes les exigences de la section 2.18 Habilitation de sécurité		
1.25	2.19	Toutes les exigences de la section 2.19 Santé et sécurité		
1.26	2.20	Toutes les exigences de la section 2.20 Coordination et calendrier Le soumissionnaire sélectionné doit être prêt à fournir les services tels que requis (c.-à-d. installations et personnel déjà en place). Le soumissionnaire doit confirmer que le personnel adéquat est disponible pour la durée du contrat afin d'assurer que tous les travaux sont exécutés et les problèmes résolus de manière à ce que les installations soient complétées et les données reçues d'ici au 2 mars 2018. En supposant que le contrat soit octroyé d'ici au 8 janvier 2018. Le soumissionnaire doit soumettre avec sa soumission une proposition de calendrier. Le soumissionnaire doit confirmer sa capacité à visiter le site pour détection de pannes et réparation dans les 24 heures après avoir été informé d'un dysfonctionnement du système d'acquisition de données.		
1.27	RFP Section 7.0	Un prix fixe comprenant une ventilation complète des coûts et les taux horaires de toutes les catégories de personnel.		

2. Exigences cotées

Les offres qui répondent à tous les critères techniques obligatoires seront évaluées et notées conformément aux tableaux ci-dessous

Les propositions atteignant au moins 85 points techniques ainsi que le nombre de points minimum pour chaque exigence technique individuelle seront ensuite évaluées en fonction des informations financières et du prix.

Chaque critère technique coté par point sera traité séparément.

Afin de se qualifier pour le processus de cotation, les propositions doivent répondre aux exigences cotées suivantes et doivent contenir la section/page référencée dans la proposition du soumissionnaire

Vous devez compléter le tableau suivant et l'inclure dans votre offre.

	Exigences techniques cotées	**Points**		**Section/page référencée dans la proposition**
		Max.	**Min.**	
2.1	Collecte de données y compris données SAB et données énergétiques, et souveraineté des données	15	10	
2.2	Analyse des données du bâtiment, détection de	20	12	
2.3	Tableaux de bord/interfaces utilisateurs	15	8	
2.4	Installation, intégration, et connectivité des systèmes	15	8	
2.5	Adaptabilité, interopérabilité, et API des systèmes	10	5	
2.6	Contrôle de la performance des fournisseurs des services de maintenance	10	5	
2.7	Mise en service continue et optimisation du bâtiment	5	3	
2.8	Capacité de calcul des économies	5	3	
2.9	Contenu et qualité des rapports	5	3	
2.10	Expertise et expérience de l'entreprise	10	5	
2.11	Calendrier de mise en œuvre et échéances	5	3	
2.12	Niveaux de services et ICP (KPI) tels que proposés par le	5	3	
2.13	Service à la clientèle	5	3	
	TOTAL POINTS TECHNIQUES :	**125**	**85**	

Government of Canada | Gouvernement du Canada

MEMORANDUM **NOTE DE SERVICE**

Security Classification - Classification de sécurité	
Our File - Notre référence	
Your File - Votre référence	
Date	23 October 2017

To / À

Sasa Medjovic
Security Analyst
DND

From / De

Contract Security Officer
Contract Security Division,
Canadian Industrial Security Directorate (CISD)
Public Works and Government Services Canada (PWGSC)
2745 Iris Street, 6th Floor

Subject / Objet

SRCL: 2017-56-A1-012196

The attached Security Requirements Check List (SRCL) and security clauses are approved by CISD for use and incorporation into your pre-contractual/contractual documents. Please ensure that both are included in the resulting contract.

Should you wish to ensure that bidders direct all enquiries to you, page 4 of the SRCL which contains the authorization signatures may be removed from the bidding document. Should the lower portion of page 4 contain additional instructions, the signatures may be blanked out.

The complete SRCL (including page 4) shall be used in the contract document.

CISD is obliged under various international security agreements, arrangements and protocols to insert special security clauses into contracts for award outside of Canada. The appropriate clauses vary from country to country, and therefore must be provided by CISD on a case-by-case basis.

Should foreign suppliers be bidding on this procurement please contact me for an international security clause.

A "Security Requirement clause" is attached. Should the client department raise any objections to the wording of the clause, kindly contact the undersigned **PRIOR TO** finalizing the contractual documentation. **No changes** to the clause wording are permitted without prior consultation with CISD. A copy of this memo and attachments has been forwarded to the client department's Security Office.

Is this a renewal of a current contract? If so, please provide the current PWGSC file number.

Information on the security status of prospective suppliers may be obtained from the Contract Section of CISD.

Should it be necessary to initiate security screening action on the chosen supplier, the CISD will require written notification from your Directorate's Sponsorship Coordinator. The request shall include the name of the supplier, complete address, the name and telephone number of the President and the level of Facility Security Clearance required (see your Security Coordinator for details).

Please advise CISD if you are aware of any work to be assigned to a third party in relation to this requirement under a subcontract or service agreement arrangement or any other business arrangement that will entail the release and/or access to the government's sensitive information and/or assets.

Kindly ensure that:

1. the cover page of the contractual documents include the following statement in bold/block type:

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT / DOCUMENT CONTIENT DES EXIGENCES RELATIVES À LA SÉCURITÉ

2. the document index shall identify the block statement entitled "Security Requirements".

3. the block statement entitled "Security Requirements" shall appear very early in the line up of contractual conditions.

4. IT IS MANDATORY THAT A COMPLETE COPY OF THE CONTRACTUAL DOCUMENTATION (LOI, RFP, CONTRACT, RFSO or SO) BE PROVIDED UPON RELEASE TO CISD AT SSICONTRATS.ISSCONTRACTS@PWGSC-TPSGC.GC.CA

Linda Daly
Contract Security Officer
613-957-9337

Attachments

c.c.: Luc Boulanger
Collin Long

NOTES:

1. **A CONTRACT/SUB-CONTRACT/STANDING OFFER/SUPPLY ARRANGEMENT CONTAINING A SECURITY REQUIREMENT CLAUSE WHEREBY VENDOR PERSONNEL MUST BE RELIABILITY SCREENED/SECURITY CLEARED, MUST NOT BE AWARDED WITHOUT FIRST VERIFYING THROUGH THE CANADIAN INDUSTRIAL SECURITY DIRECTORATE (CISD) THAT THE VENDOR HOLDS THE APPROPRIATE LEVEL OF FACILITY SECURITY CLEARANCE AND (IF REQUIRED) DOCUMENT SAFEGUARDING CAPABILITY.**

2. **A COPY OF THE CONTRACTUAL DOCUMENTATION MUST BE PROVIDED TO THE COMPANY SECURITY OFFICER AND THE CISD AT SSICONTRATS.ISSCONTRACTS@PWGSC-TPSGC.GC.CA CISD WILL REQUIRE THREE COPIES IF THE CONTRACT IS AWARDED TO A FOREIGN SUPPLIER.**

3. **BEFORE FORWARDING ANY PROTECTED OR CLASSIFIED INFORMATION/ASSETS TO AN ORGANIZATION, GOVERNMENT OFFICIALS SHALL FIRST ENSURE THROUGH THE CANADIAN INDUSTRIAL SECURITY DIRECTORATE THAT THE INTENDED SUPPLIER AND SELECTED SITE HOLDS THE APPROPRIATE LEVEL OF DOCUMENT SAFEGUARDING CAPABILITY.**

4. **WITHIN CANADA, ALL PROTECTED AND CLASSIFIED INFORMATION/ASSETS MUST BE FORWARDED TO THE COMPANY SECURITY OFFICER (CSO). HOWEVER, THE CSO *MUST* FORWARD A COPY OF THE DOCUMENT TRANSMITTAL FORM TO THE CANADIAN INDUSTRIAL SECURITY DIRECTORATE (CISD)/DOCUMENT CONTROL UNIT.**

5. **PROTECTED AND CLASSIFIED INFORMATION/ASSETS INTENDED FOR FOREIGN SUPPLIERS MUST BE TRANSMITTED ON A GOVERNMENT-TO-GOVERNMENT BASIS VIA THE CANADIAN INDUSTRIAL SECURITY DIRECTORATE (CISD)/DOCUMENT CONTROL UNIT.**

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER:
PWGSC FILE 2017-56-A1-012196

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS), issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).

2. The Contractor/Offeror personnel requiring access to sensitive work site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by CISD/PWGSC.

3. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.

4. The Contractor/Offeror must comply with the provisions of the:

   a.Security Requirements Check List and security guide (if applicable), attached at Annex _____;
   b.Industrial Security Manual (Latest Edition).

EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN:
DOSSIER TPSGC No 2017-56-A1-012196

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, délivrée par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

2. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des établissements de travail dont l'accès est réglementé doivent TOUS détenir une cote de FIABILITÉ en vigueur, délivrée ou approuvée par la DSIC de TPSGC.

3. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE DOIVENT PAS être attribués sans l'autorisation écrite préalable de la DSIC de TPSGC.

4. L'entrepreneur ou l'offrant doit respecter les dispositions :

   a.de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe _____;
   b.du Manuel de la sécurité industrielle (dernière édition).

Government of Canada / Gouvernement du Canada

SEP - 6 2017

Contract Number / Numéro du contrat
'2017-56 (A1-012196)

Security Classification / Classification de sécurité
Unclassified

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organizati Ministère ou organisme gouvernemental d'origine NRC / DND	2. Branch or Directorate / Direction générale ou Direction Construction
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Pilot project to install smart building technology in parallel with the building automation system, on military bases in Canada.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	✓ No Non ☐ Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	✓ No Non ☐ Yes Oui
6. Indicate the type of access required / Indiquer le type d'accès requis	
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	✓ No Non ☐ Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☐ No Non ✓ Yes Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?	✓ No Non ☐ Yes Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada SIM	NATO / OTAN	Foreign / Étranger
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions Aucune restriction relative à la diffusion Not releasable À ne pas diffuser Restricted to: / Limité à : Specify country(ies): / Préciser le(s) pays :	All NATO countries Tous les pays de l'OTAN Restricted to: / Limité à : Specify country(ies): / Préciser le(s) pays :	No release restrictions Aucune restriction relative à la diffusion Restricted to: / Limité à : Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A —	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	PROTECTED A / PROTÉGÉ A
PROTECTED B / PROTÉGÉ B	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C —	NATO CONFIDENTIAL / NATO CONFIDENTIEL	PROTECTED C / PROTÉGÉ C —
CONFIDENTIAL / CONFIDENTIEL	NATO SECRET / NATO SECRET	CONFIDENTIAL / CONFIDENTIEL —
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET		TOP SECRET / TRÈS SECRET
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) —		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) —

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — No ✓ / Non — Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — No ✓ / Non — Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

✓ RELIABILITY STATUS / COTE DE FIABILITÉ	CONFIDENTIAL / CONFIDENTIEL	SECRET / SECRET	TOP SECRET / TRÈS SECRET
TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET / NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET
SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux :

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No ✓ / Non — Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted? — No ✓ / Non — Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No ✓ / Non — Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — No ✓ / Non — Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No ✓ / Non — Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No ✓ / Non — Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — No ✓ / Non — Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC				
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRES SECRET
Information / Assets / Renseignements / Biens															
Production															
IT Media / Support TI															
IT Link / Lien électronique															

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

13. Organization Project Authority / Chargé de [illegible]t de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Luc Boulanger	Mechanical Engineer	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-922-8778		luc.boulanger3@forces.gc.ca	2017-08-31

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Sasa Medjovic - DDSO - Industrial Security		
[illegible]	Senior Security Analyst [illegible]	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
Tel: 613-996-0286		E-mail: sasa.medjovic@forces.gc.ca	2017-Sept 06

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

No / Non ☐ Yes / Oui ☑

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Collin Long	Procurement Officer	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-993-0431		Collin.Long@nrc-cnrc.gc.ca	Oct. 23, 2017

[illegible]e sécurité

[illegible]re		Signature
		Linda Daly
[illegible]r	E-mail address - Adresse courriel	Date
		Sept 14 17

Linda Daly
Agente à la Sécurité des contrats | Contract Security Officer
Programme de la Sécurité industrielle | Industrial Security Program
Linda.Daly@tpsgc-pwgsc.gc.ca
Téléphone : 613 957-9337

Security Classification / Classification de sécurité
Unclassified

Canada

National Défense
Defence nationale

National Defence Security Orders and Directives

Chapter 8: Industrial and Contract Security

Department of National Defence and Canadian Armed Forces

Version 2.0 This document contains 31 pages Status: Final

Date of Issue: 2015-06-08

Supersession:

- National Defence Security Policy
- National Defence Security Instructions
- Defence Security Manual

DND and CAF policies, directives and standards relevant to this chapter of the NDSODs:

- DAOD 2006-0 Defence Security

Date of Last Update and Section(s) Updated:

2016-05-03 – Major amendments

- Annexes D to G added. They were moved out of Chapter 4: Personnel Security

2016-06-06 – Minor amendment

- Update to Caveat

2017-09-11, Consequential Changes

- Added to SDA in a non DND establishment (para 8.20)
- Addition to Table 1: Commander Canadian Forces Intelligence Command and Chief of Defence Intelligence;
- Update to Table 2: Security Process for Contracts, Step 4, fixed contradiction between French and English versions
- Update to Table 3: Access Requirements for High Security Zones and SCIFs
- Update hyperlink for SRCL checklist (para 8.36)
- Revisions to Annex E, para. 8.99.b, Access to DND and CAF property re one time visits
- Clarified Annex C, para 8.61, re foreign information
- Implementation of new Navigation System affecting headers, footers and all para numbers

Table of Contents

This page intentionally left blank

Section 1: General

These National Defence Security Orders and Directives (NDSOD) are issued under the authority of the Director General Defence Security (DGDS) for the Department of National Defence (DND) and the Canadian Armed Forces (CAF). The NDSOD are intended for use only by DND and the CAF and are not for distribution to the public. The NDSOD can be, on an as required basis, shared with contractors who have entered into a contract with DND or the CAF and require access at any point in the contracting process. Only the relevant portions of the NDSOD are to be disclosed.

Any inquiries concerning the security and proper handling of the NDSOD are to be sent to Director Defence Security Policy, Training and Awareness at DND.DGDSPolicies-DGSDPolitiques.MDN@forces.gc.ca.

Application

8.1 The National Defence Security Orders and Directives (NDSOD) apply to the conduct of the activities and operations of both DND and the CAF. They are directives that apply to the employees of the Department of National Defence (DND employees) and orders that apply to officers and non-commissioned members of the Canadian Armed Forces (CAF members).

Context

8.2 The Department of National Defence enters into contracts with industry for both DND and the CAF, for the acquisition of goods, services, construction, and leases. For the purposes of this chapter, a contract is an agreement (from definition of requirements to closure) between a procurement authority and a contracting authority, and a person or firm, to provide a good, perform a service, construct a work, or to lease real property for appropriate consideration.

8.3 In many cases a single organization will be both the procurement and the contracting authority. The Director General Defence Security (DGDS) is required to ensure that security requirements are appropriately identified, implemented, and monitored for DND contracts with industry. This chapter focuses on what must be in place in order to ensure security is incorporated into all industrial contracts.

Note: Industrial and contract security is the application of protective measures and procedures to prevent, detect and recover from the loss or compromise of sensitive information handled by industry in contracts.

Objectives, Requirements and Expected Results

Objectives

8.4 The objectives of this chapter are to ensure that:

- **a.** DND contracts are provided with the appropriate level of protection through the integration of security measures during all phases of their life cycles;
- **b.** security requirements are consistently and accurately identified, formally documented, addressed and monitored for all contracts for goods, services, construction and leases;

c. all persons who will have access to sensitive DND or CAF information, assets or resources must be security screened at the appropriate level before the commencement of their duties;

d. protected and classified information, assets and resources entrusted to, or developed by contractors and organizations under contract to DND or the CAF, are safeguarded in accordance with applicable legislations, regulations and policies;

e. the end state of the overall security of a contract is clearly identified; and

f. the residual risk is formally accepted by the appropriate authority (see Chapter: 3 Security Risk Management).

Requirements

8.5 Security requirements must form part of the contract between DND and the contractor for all contracts for goods, services, construction, and leases. These security requirements apply but are not limited to construction and materiel projects, professional services contracts, and facility maintenance contracts.

8.6 All DND employees and CAF members must identify and apply security measures to contracts during all phases of their implementation to ensure that DND and CAF information, assets and resources entrusted to, or developed by contractors or organizations, are safeguarded according to DND and the CAF standards.

8.7 Changes to the minimum baseline security measures prescribed in these Security Orders and Directives must be implemented using a formal security risk management process (see Chapter: 3 Security Risk Management). In instances where an organization is unable to comply with the baseline standards, written authorization (a waiver) for any deviation must be obtained from DGDS.

Expected Results

8.8 The expected results of this chapter are that:

a. DND and the CAF implement security within all phases of applicable contracts for goods, services, construction, and leases;

b. the established DND and CAF security risk management process is consistently and correctly applied and followed in DND contracts as prescribed in these Security Orders and Directives;

c. DND or CAF protected or classified information, assets and resources held or accessed by contractors or other organizations are safeguarded in accordance with these Security Orders and Directives; and

d. the residual risk, if present, is accepted by the appropriate authorities.

Contract Security Process

8.9 It is critical that security requirements are determined and assessed at the beginning, during the identification phase and reassessed throughout all phases of the contract. Failure to do so often results in increased security risks and costs, wasted resources and incurred delays. It is imperative that local security advisors (e.g. the Information Systems Security Officer (ISSO), the Unit Security Supervisor (USS), the Military Police (MP), etc.) are consulted in order to

ensure that security requirements are well defined. If further clarification and direction is required, the Regional Departmental Security Officers (RDSOs) or as applicable, Director Information Management Security (DIM Secur), the National Special Centre (NSC), the Controlled Technology Access and Transfer (CTAT) Office, or DGDS may be consulted. To manage the security process applicable to all projects and all such resulting contracts, one should follow the steps identified in Annex A, Table 2: Security Process for Contracts.

8.10 The security process for contracts sets out the major activities that are essential for contract security. These are the completion of a Security Identification Document (SID), a project Threat and Risk Assessment (TRA), a Security Requirement Check List (SRCL) and a Visit Clearance Request (VCR). To assist with the security screening requirements, Annex A, Table 3: Minimum Security Levels for Contract Activities contains the minimum security levels for various activities relating to contracting.

8.11 The Requirement Owner is the administrative body responsible to identify contract requirements including security requirements. The Requirement Owner is also responsible for ensuring that all contracts have a current and detailed TRA. The format and scope of the TRA are not strictly defined. This is to allow for flexibility so that the TRA may meet the needs of each contract. In general, TRA producers should consider the security risks throughout the life of the contract starting from the identification of a deliverable, following through the life of the deliverable and, when applicable, including the destruction of the material or information produced by the contract.

> Note: The Requirement Owner in contracting security is the person or organization that owns the requirements.

8.12 A local baseline TRA may be used in place of a contract specific TRA in situations where the scope of the contract risks are covered by the baseline TRA. When the baseline TRA is used it is recommended that the local RDSO be consulted. More detail on TRAs can be found in Chapter 3: Security Risk Management of these Security Orders and Directives.

Security Identification Document (SID)

8.13 The SID is a DGDS template that will assist contract authorities and project managers in the completion of the TRAs and Security Requirement Check Lists (SRCLs) and inform DGDS on security requirements for contracts. Part A of the SID is to be completed for contracts that involve contractor access to special rooms in a security zone, a high security zone or secret and higher classified information or assets. Part B of the SID is to be completed for contracts that will require contractor access to DND and CAF Information System (IS) or where contractor facilities will be processing electronic data or sending data to DND or CAF electronically. In addition, Part B of the SID is to be completed for each contractor's facility and for each contractor involved in a contract. On completion, the SID is to be sent to DGDS Industrial Security. Industrial Security staff will review the SID and determine the extent of their involvement in the contract. The SID template is found at Annex B: Security Identification Document (SID).

> Note: For more information on contracting of Controlled Goods, DND employees and CAF members should consult DAOD 3003-1, Management, Security and Access Requirements Relating to Controlled Goods, Protective Measures Table for Unclassified Controlled Goods.

Security Requirement Check List (SRCL)

8.14 The SRCL is a Treasury Board (TB) form that is used to define the security requirements associated with **all** contracts. The SRCL ensures that the appropriate security clauses are identified by the Contracting Authority (CA) so they may be incorporated into the contract, thereby legally binding the contractor to meet the contract's security requirements. The SRCL must accompany all contractual documents, including subcontracts that contain security requirements. Guidance on completion of the SRCL is contained in Annex C: Security Requirements Check List Instructions.

8.15 For contracts where there are Information Technology (IT) dependencies or implications, the IT security requirement document is to be completed. This document outlines specific IT security requirements that the contractor will need to satisfy in order to be able to process DND and CAF protected, classified or sensitive electronic information. Guidance on the completion of the IT security requirement document is available on the DIM Secur website.

8.16 The SRCL is to be completed and signed by the Requirement Owner. The SRCL must be forwarded with applicable contractual documentation to the Organization Security Authority DGDS SRCL Section (+SRCL@VCDS DGDS@Ottawa-Hull). Once verified, DGDS sends the SRCL to the Contracting Security Authority (Public Services and Procurement Canada (PSPC) Canadian Industrial Security Directorate (CISD) for verification and to define the appropriate security clauses that must be included in any subsequent contract.

8.17 If it is determined that there are no security requirements involved with a contract, the Requirement Owner is to sign the SRCL. In this case, there is no requirement to send the SRCL to DGDS for signature; however, a signed copy of the SRCL must be retained on the contract file.

Contractor Security Screening

8.18 Contractors who will need access to or who will retain controlled goods, protected or classified information, assets or resources, must be cleared as follows:

- **a.** contractors must be screened to safeguard the highest level of information and asset to be retained, meaning:
  - **i.** Designated Organization Screening (DOS) for contracts at the protected level only; and
  - **ii.** Facility Security Clearance (FSC) for contracts at the protected or classified levels;
- **b.** contractors who will electronically process protected or classified information must have an approved IT processing capability commensurate with the security classification level of the information to be processed, and must be cleared to the level commensurate with the information or asset to be accessed; and
- **c.** contractors accessing controlled goods must be registered with the PSPC Controlled Goods Program or exempt from such registration.

8.19 In order to ensure that the contractors and their personnel have the appropriate security screening level in time for the commencement of work or services, time must be built into the contract to allow for the screening process to be completed.

Note: Registration with the PSPC Controlled Goods Program is legally required for any person examining, possessing or transferring controlled goods. For more information, DND employees and CAF members should consult DAOD 3003-1, Management, Security and Access Requirements Relating to Controlled Goods, Protective Measures Table for Unclassified Controlled Goods.

Sensitive Discussion Area in a non-DND Establishment.

8.20 When a Sensitive Discussion Area (SDA) is located in a contractor's facility, Public Services and Procurement Canada (PSPC) is responsible for its accreditation. When this SDA is used to safeguard Government of Canada information, the design, construction and contractor clearance requirements are to be in accordance with these Security Orders and Directives. The local Military Police security section can provide assistance in an advisory capacity; however, a contractor's SDA does not fall within their core mandate.

Inability to Meet Security Requirements

8.21 In instances where contracted personnel do not meet the personnel screening level to enter an operations zone but their security clearance is in the pending state with PSPC, the CO, or senior manager may accept the risk and allow the contractors access, under positive control, to the operations zone. The state of the clearance may be obtained by contacting PSPC - Contract Security Program. Instances of risk mitigation must be coordinated with the RDSO and recorded in a local security risk register for audit and trend analysis purposes. The register must include the date that the contractor's clearance was finally issued.

8.22 For all other instances not covered, the Requirement Owner must not assume risk when that decision reduces the security posture below the minimum security standard as defined in these Security Orders and Directives. In these instances, the Requirement Owner will prepare the Risk Mitigation Plan Template (see the Risk Mitigation Plan Template). This is a strategic form and must include the situation, the security requirements that cannot be met, the operational impact, and the mitigating measures to minimize risk. The risk mitigation plan form and the associated SRCL must be sent to the appropriate RDSO to initiate the approval process.

Use of Escorts

8.23 Escorts for contractors who do not meet the required security screening level for site access may be approved by DGDS for special circumstances, but not as a recurring security mitigation strategy. In the use of escorts, it is important to note that:

a. escorts are not to be used for work on the inside of a Sensitive Compartmented Information Facility (SCIF) without obtaining approval from the National Special Centre (NSC) and DGDS;

b. escorts are not to be used to allow non-screened contractors access to security or high security zones, including SCIFs and SDAs. However, escorts can be used to enhance the security for work being completed by screened contractors;

c. for the occasions where contractors are required to do work in an operational zone where they do not have the appropriate security screening, the use of escorts may be requested following the process identified above in 8.22. However, to do so the contractor must have started the security screening process with the PSPC Contract Security Program and must continue to complete the process;

d. for emergency repairs, meaning unplanned repairs generally lasting less than one week, escorts may be authorized by the organization construction engineering officer or equivalent authority with coordination with local military police and RDSOs; and

e. persons requiring access to an operation zone in support of a future contract with DND who are not screened to the appropriate level may be granted access, under positive control, for the required pre-contract visits.

Verifications

8.24 DGDS may conduct compliance visits to verify that the approved risk mitigation measures are being implemented as specified and actual practice complies with these Security Orders and Directives. For further details on compliance, refer to Chapter 2: Oversight and Compliance (Framework on Security Compliance).

Visit Clearance Requests (VCR)

8.25 The proper staffing of the VCR will ensure compliance and reduce the risk of non-legitimate individuals or organizations having access to Defence sensitive organizations and assets. For details on the VCR refer to Annex E: Canadian Industry Visits to Defence Establishments.

8.26 It is the responsibility of the DND OPI (e.g. the Requirement Owner or the project authority) and the appropriate Unit Security Supervisor (USS) to manage the security aspects associated with the contract as well as the visit requirements for contractor personnel to a DND facility. Therefore, the DND OPI is to ensure that access to information, assets and resources, as well as secure areas and sites, is restricted to those individuals who have a need-to-know or a need-to-access. The DND OPI must also ensure such access corresponds to the security level indicated for each individual listed on the visit approval. The DND OPI is responsible for arranging the required access and passes and to advise all visit points (must include the appropriate USS) of the details of the visit (date, time, location, etc.).

Obtaining Security Services

8.27 Refer to Annex D: Obtaining Security Services from other Organizations for information on contracting civilian security services that perform a direct security function, such as access control, traffic control, visitors' escort, security patrols, etc.

Roles and Responsibilities

Table 1: Roles and Responsibilities

The…	is or are responsible for…
Director General Defence Security	▪ providing security advice on contracts and contractural arrangments for goods, services, construction, and leases; ▪ providing security oversight and compliance for contracts for goods, services, construction, and leases; ▪ reporting to VCDS on any significant security risk associated with any contract; ▪ signing as the Organizational Security Authority for the SRCL; and ▪ coordinating the VCR program for contracts.
Assistant Deputy Minister (Infrastructure and Environment)	▪ ensuring that these Security Orders and Directives are followed in all Real Property (RP) contracts; and ▪ implementing policy and procedures outlining how security will be addressed in RP contracting activities performed in DND.
Assistant Deputy Minister (Materiel)	▪ procurement and contracting for the Department of National Defence; and ▪ supporting compliance with defence trade controls (International Traffic in Arms Regulation (ITAR)) and the PSPC administered controlled goods program for DND.
Assistant Deputy Minister (Information Management)	▪ reviewing and recommending the approval of SRCLs with IT security requirements; and ▪ outlining IT security policy and procedures for all IT acquisitions and contracting activities.
Commander Canadian Forces Intelligence Command and Chief of Defence Intelligence	▪ ensuring the application of secure access control and handling systems of sensitive compartmented information (SCI) and materials within DND (such as Talent Keyhole and Special Intelligence); ▪ overseeing the proper use of sensitive compartmented information facilities (SCIFs); and ▪ enforcing, on behalf of the Canadian Security Establishment (CSE), the Canadian SIGINT Security Standards within DND.
Canadian Forces Military Police Group	▪ supporting DND and CAF security in the provision of security advice on contracts for goods, services, construction, and leases; and ▪ providing advice on the use of contracted security services to the contracting authority.
Level 1s	▪ advising DGDS of new project ideas by submitting SID documents to DGDS; ▪ identifying Organizational Authorities and ensuring that they are aware of the contract security process and the responsible organizations; ▪ ensuring that the identified security risk mitigation procedures are enforced, managing the implementation of the security measures identified within the Security Guide that is attached to the contract; ▪ submitting an SRCL when a contractor will have access to controlled goods, protected or classified information, assets, resources or facilities in the performance of their work; ▪ ensuring that VCRs are submitted as required; ▪ ensuring that security requirements have been identified throughout the contract process; and

The…	is or are responsible for…
	▪ ensuring that the security risk mitigation procedures identified within the Security Guide attached to the contract are implemented and enforced.
Commanding Officers, Managers and Supervisors at all levels	▪ identifying security requirements for information, assets and resources with respect to contracts for goods, services, construction, and leases.
Procurement and Contracting Authority	▪ ensuring that the necessary security requirements to safeguard government information, assets, resources and information systems are addressed in the terms and conditions of a contract; ▪ ensuring that contractors and their personnel requiring access to protected and classified information, assets, and resources have the required security screening or clearance; and ▪ ensuring that DGDS is advised when contractors have to be removed from a contract for any security related reasons or issues. This is to be done via an email sent to DGDS Industrial Security Staff: +Industrial Security@VCDS DGDS@Ottawa-Hull. Note: Depending on the level of the delegation, the appropriate Contracting Authority (CA) could be DND or PSPC.

Note: Public Services and Procurement Canada (PSPC) administers the Contract Security Program and manages the Controlled Goods Program for the Government of Canada. As such, PSPC is responsible for screening industry organizations and their employees (e.g. Designated Organization Security, Facility Security Clearance and Document Safeguarding), providing contractual clauses through the Security Requirements Check List (SRCL) process and providing verification of Security Screening levels and the need to know via the VCR process. In some DND contracts, PSPC will serve as the contracting authority in which case the Assistant Deputy Minister (Materiel) (ADM (Mat)) would serve as the procurement authority. This will occur, for example, when the contract is above a certain dollar value.

References

External References

Policy on Government Security

Project Complexity and Risk Assessment Tool

PSPC, Industrial Security Manual

PSPC, Contract Security Program

Security and Contracting Management Standard

Security Requirements Check List

Internal References

DAOD 3003-0, Controlled Goods

DAOD 3003-1, Management, Security, and Access Requirements Relating to Controlled Goods

DAOD 3016-0, National Security Exception Under Trade Agreements

DAOD 6003-0, Information Technology Security

DAOD 6003-2, Information Technology Security Risk Management

Procurement Administration Manual

Project Approval Directive

Enquiries

8.28 Any enquiries on this chapter are to be addressed to the Director General Defence Security Policy Section at DND.DGDSPolicies-DGSDPolitiques.MDN@forces.gc.ca.

Definitions

8.29 All definitions can be found in the glossary to the NDSOD Glossary.

Annex A: Contract Security Process Aids

Introduction

8.30 The steps outlined in the table below provide guidance during the process of implementing security in contracts. Due to the diversity of contract requirements, not all steps may apply to each case. Specific inquiries on this process can be directed to DGDS Industrial Security Staff (+Industrial Security@VCDS DGDS@Ottawa-Hull).

Table 2: Security Process for Contracts

Step	Action	Schedule	Responsibilities
1	Development of a Security Identification Document (SID) is required if the contract deals with controlled goods, sensitive information and any activities that are within, or will be functioning within, a security zone or a high security zone	▪ The completion of the SID should assist with the definition of contract requirements and with the completion of other contract and project documents such as the Project Brief (ID) ▪ Must be revised prior to any major change to the Statement of Requirements (SOR)	▪ Security Identification Document (Annex B: Security Identification Document (SID))
2	Determine relevant security authority for the contract, and conduct a Threat and Risk Assessment (TRA)	▪ Determined during identification	▪ Local TRA authority
3	Assess whether to establish a Project Security Working Group (SWG)	▪ Dependent on contract activities ▪ Early assessment of security issues will benefit the contract	▪ DGDS
4	Determine the Information System security requirements	▪ Determined during identification of contract or project requirements or as required	▪ DIM Secur and regional or local Information System Security Officer (ISSO)
5	Assess the need for secure contract communications	▪ Determined when identifying contract or project requirements ▪ Requirement will need to be reconsidered as contract participants and activities change	▪ DGDS ▪ DIM Secur
6	Assess the requirement for any contractors to obtain security clearances or sponsorship with Public Services and Procurement Canada (PSPC) if the company is not already registered	▪ Assessed well in advance of the tendering process	▪ DGDS

Step	Action	Schedule	Responsibilities
7	Assess PSPC Controlled Goods Program's registration requirements for firms and contractors if controlled goods are involved	▪ Assessed well in advance of the release of any controlled goods to contractors	▪ CTAT Office
8	Assess foreign authorization requirements such as International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR)	▪ Assessed well in advance to permit sufficient time to receive foreign authorizations prior to industry briefings and RFPs (Request for Proposals)	▪ CTAT Office
9	Develop a Security Requirements Check List (SRCL) and IT Security Requirement Document (when applicable)	▪ Assessed well in advance of the tendering process	▪ DGDS ▪ DIM Secur ▪ PSPC
10	Develop a Contract Security Requirements Document utilizing information from the TRA in order to deliver to the contractor as part of the SOW	▪ Contract Security Requirements Document is created following identification ▪ This will be delivered once the bidding process is completed and the contract has been signed	▪ Defence Risk Management Framework for Security Aide-Memoire
11	Assess security requirements to be included in any Invitation to Register interest	▪ Assessed well in advance of the release of the invitation ▪ Assess whether to issue an Advanced Procurement Notice (APN) with SRCL to allow contractors to begin security clearance process	▪ DGDS ▪ Contracting Authority ▪ Procurement Authority
12	Assess security requirements for any Industry Briefing	▪ Assessed well in advance of the conduct of an Industry Briefing	▪ DGDS ▪ Contracting Authority
13	Assess security requirements to be included in any request documentation (RFP), Request for Quotation, Request for Tender, etc.	▪ Assessed well in advance of the release of any request documentation	▪ DGDS ▪ Contracting Authority ▪ Procurement Authority ▪ ADM(Mat) ▪ DND Contract Officer

Step	Action	Schedule	Responsibilities
14	Assess security requirements to be included in any contract documents	▪ Assessed prior to contract signature	▪ Contracting Authority ▪ DND Procurement Officer
15	Review contractors' Security Implementation Plan	▪ The contractor will produce their own Security Implementation Plan as a result of the Contract Security Requirements Document	▪ DGDS

8.31 The table below identifies the minimum acceptable level for security screening of contractors. When granting access to enter areas, it is important to restrict the access to the information contained within, in accordance with Chapter 6: Security of Information and the Security of Information Standards. The access to sensitive information must always be limited to individuals holding the appropriate security screening level and who have demonstrated the need-to-know.

Table 3: Minimum Security Levels for Contract Activities

Task/Requirement		Security Screening Level
Access Operations Zone	Logistics activities (shipping, receiving, waste removal, etc.)	Nil with positive control
	Transit through (no work)	Nil with positive control
	Pre-contract visits	Nil with positive control
	All other contract activities	Reliability
Access to Security Zones		Secret
Access to High Security Zones		Secret with a TS cleared escort
Access to a Sensitive Compartmented Information Facility (SCIF)		Secret with a TS SCI cleared escort
Embedded contractors accessing controlled goods at a DND or CAF facility		Secret
Construction of a facility where the end use will be an Operations Zone		Reliability
Construction of a facility where the end use will be a Security Zone with no Special Rooms		Reliability
Design and construction of a facility where the end use will be a Security Zone with a Secure Discussion Area (SDA)		Secret
Design of an Arms Storage Room, Secure Communication Room or a Secure Storage Room including the electronic security systems		Secret

Task/Requirement	Security Screening Level
Design and construction of an Arms Storage Room, Secure Communication Room or a Secure Storage Room less the electronic security systems	Reliability
Design and construction of a facility where the end use will include a high security zone or a Sensitive Compartmented Information Facility (SCIF)	Secret
Handling or shipment of small arms, explosive or classified equipment	Secret
Involvement with the design and installation of any element of a RED Distribution System (RDS)	Secret
Design and installation of an electronic security system, which includes the intrusion alarm, access control and surveillance systems (Protected Systems)	Reliability
Design and installation of an electronic security system, which includes the intrusion alarm, access control and surveillance systems (Classified Systems)	Secret
Design and installation of an electronic security system, which includes the intrusion alarm, access control and surveillance systems (Arms Storage)	Secret

Annex B: Security Identification Document (SID)

Security Identification Document Form

8.32 Parts A and B of the Security Identification Document Form can be found in the Defence Forms Catalogue: Part A DND 4133-E and Part B DND 4134-E.

Part A

8.33 Part A of the SID is to be completed for projects or contracts that involve contractor access to special rooms in a security zone; a high security zone; or secret and higher classified information, assets and resources. The SID is a living document and should be updated as more information becomes available. The SID (Part A) is to be submitted by the Project Manager or Contracting Authority to DGDS – Industrial Security (+Industrial Security@VCDS DGDS@Ottawa-Hull).

Part B

8.34 Part B of the SID is to be completed for projects or contracts that will require contractor access to the DND or the CAF Information System (IS) or where contractor facilities will be processing electronic data or sending data to DND or the CAF via electronic means. In addition, Part B of the SID is to be completed for each contractor's facility and for each contractor involved in a contract.

8.35 The Information Systems Supplement to the SID (Part B) is to be submitted by the Project Manager or Contracting Authority to Director General Defensive Security – Industrial Security (+Industrial Security@VCDS DGDS@Ottawa-Hull).

Annex C: Security Requirements Check List Instructions

Introduction

8.36 The Security Requirements Check List (SRCL) is a Treasury Board (TB) form that must be used to define the security requirements associated with a contract.

8.37 The SRCL must accompany all contracts and subcontracts. The SRCL also applies to call-ups against standing offers and supply arrangements.

8.38 The SRCL and IT security requirement document (when applicable) ensures the appropriate security clauses are incorporated in a contract by the PSPC, Canadian Industrial Security Directorate (CISD), thereby legally binding the contractor to ensure the security requirements are met. If these are not included, the contractor may have no legal obligation to safeguard the DND or CAF information, assets and resources entrusted to them.

8.39 An SRCL is required for all contracts. In addition to the SRCL, an IT security requirement document may be required when applicable.

Process

8.40 The SRCL and IT security requirement document (when applicable) is to be completed and signed by the Requirement Owner. Refer to Appendix 1: Aide Memoire to SRCL Completion below for completion details concerning the SRCL. For completion details for the IT Security Document refer to the DIM Secur website.

> Note: The SRCL is to be forwarded with applicable contractual documentation to DGDS Industrial Security Section for approval to the positional mailbox +SRCL@VCDS DGDS@Ottawa-Hull.

8.41 DGDS Industrial Security Section will staff the SRCL to PSPC CISD for verification of document completion and drafting of the security clauses to be included in the contract. The SRCL and associated security clauses identify to the contractor what security requirements are associated with the bid solicitation and subsequent contract, and form part of a legally binding obligation under the contract.

8.42 An SRCL is always required and must be documented in the contract file. When there are no security requirements involved with the contract, a copy of the completed SRCL must still be retained in the contract file.

Inability to Meet Security Requirements

8.43 In the event that the identified security requirements cannot be met, the Requirement Owner must not assume risk when that decision reduces the security posture below the minimum security standard as defined in these Orders and Directives. In these instances, the Requirement Owner will prepare a Risk Mitigation Plan form at Annex C, Risk Mitigation Plan Template.

8.44 The risk mitigation process is discussed in Chapter 3: Security Risk Management. This plan must include the situation, the security requirements that cannot be met, the operational impact, and the mitigating measures to maintain a LOW risk. The risk mitigation plan form must be sent to the Regional Departmental Security Officer (RDSO) to initiate the approval process.

Verifications

8.45 DGDS may conduct visits to verify that the approved risk mitigation measures are being implemented as specified and actual practice complies with security policy.

Risk Mitigation Plan Template

8.46 This form and associated SRCL (if available) are to be sent to the appropriate RDSO.

a. A template of the Risk Mitigation Plan is available in the Defence Forms Catalogue, Form DND 4135.

Aide Memoire to SRCL Completion

8.47 See Appendix 1: Aide Memoire to SRCL Completion.

Appendix 1: Aide Memoire to SRCL Completion

Introduction

The following aide memoire will assist in the completion of the SRCL (TBS/SCT 350-103). Although there are a variety of possible scenarios that may be encountered, a basic definition of each block appears below.

> Note: Questions or concerns relating to this process may be directed to +SRCL@VCDS DGDS@Ottawa-Hull.

Part A

8.48 BLOCK 1: DND

8.49 BLOCK 2: Directorate (e.g. VCDS/DGDS/DDSO)

8.50 BLOCK 3(a): Ignore – only for use by Prime for sub contracts

8.51 BLOCK 3(b): Ignore – only for use by Prime for sub contracts

8.52 BLOCK 4: Brief summary of work to be performed

8.53 BLOCK 5(a): The Controlled Goods Program managed by PSPC ensures the safeguarding of information, assets and resources (controlled goods) that have been modified for military use. Some controlled goods are classified while others are unclassified. For the purpose of this document the following applies primarily to unclassified controlled goods, in accordance with the requirements of DAOD 3003-1.

a. If the contracted individuals will be embedded, block **5(a)** must be checked "YES". The company **must** be registered in the PSPC Controlled Goods Program and the contracted individuals must hold a Secret security clearance.

> Note: An embedded contractor is an individual whose organization is under contract with the Department of National Defence (DND), has a need to access controlled goods and performs the totality of their contracted work within a DND establishment (a facility under the control of DND and where DND has authority and responsibility for security), whether on a full-time or part-time basis (i.e. no contracted work is performed off-site). The term "embedded contractor" refers to the individual physically working in a DND facility; not the organization employing or contracting the services of that individual. An embedded contractor can not discuss their work with their employer and must sign an embedded contractor acknowledgement letter to that effect.

b. If the contracted individuals will perform 100% of their work at DND but will not require access to controlled goods, they are not embedded and **Block 5(a**) will be checked "NO".

> Note: If the contracted individual(s) performs the work at their own facility and require access to unclassified controlled goods (no access to protected/classified information), NO SRCL is required **but** they **must** be registered in PSPC's Controlled Goods Program. For further information on controlled goods or for questions regarding what information/assets are controlled, please consult the Controlled Technology Access and Transfer (CTAT) website.

8.54 BLOCK 5(b): Unclassified Military Data differs somewhat from the Controlled Goods programme. Contractors must be registered in the Joint Certification Program. Questions regarding this program should be directed to the DGIIP website.

8.55 BLOCK 6(a): If the contractor will require access to information that is Protected or Classified, this block must be checked "YES".

8.56 BLOCK 6(b): This block must be marked "YES" if the contractor will be required to work in areas that may have access restrictions (require a clearance for access) but will **not** require access to any Protected or Classified information (e.g. Tarmac areas of airfields, Restricted rooms or areas at an organization).

> Note: Access to DND organizations requires as a minimum that the contractor holds the appropriate Security Clearance and that the DND establishment or facility has appropriate positive control measures in place for said contractor, such as identification or access badges, etc. In all instances, the minimum security requirements as detailed in this chapter must be met; however, more stringent requirements can be put in place.

8.57 BLOCK 6(c): This block refers to in-town couriers (e.g. bike couriers, hand messengers). These companies are not cleared to safeguard Protected or Classified information therefore overnight storage is not permitted. The package must be returned to the originator if it is undeliverable.

8.58 BLOCK 7(a): All types of information to which contractors will have access must be listed here (Canadian, NATO, Foreign).

8.59 BLOCK 7(b): This block refers to the citizenship of the personnel performing the work on the contract. See Note 1 at the end of this aide memoire if the contract is restricted to Canadian citizens only. The sharing of some information is outlined in specific MOU between countries. The PA must verify what restrictions apply.

a. "No release restrictions" – citizenship does not matter provided personnel hold the requisite clearance;

b. "Not releasable" – only Canadian citizens may perform the work; and

c. "Restricted to" – list the countries whose citizens may perform the work.

NATO Information

8.60 Not all NATO information is releasable to every NATO country therefore restrictions with regard to citizenship of contractor personnel performing the work would be indicated under "Restricted to". See Chapter 6: Security of Information for more details.

Foreign Information

8.61 "No Release Restrictions" – Foreign information may have restrictions regarding the citizenship of the personnel who are permitted to access the information. Please ensure that the information you release to a contractor has no such restrictions (e.g. "Canadian Eyes Only", "Restricted to", "Release to", etc.). Some information may have been approved for release only to citizens of specific countries. You would list these countries here, under Block 7(b).

8.62 BLOCK 7(c): For each country's information to be released to the contractor indicate the levels. Please indicate **all** levels and not just the highest level. Other countries do not use the

"PROTECTED" designation. Under NATO and Foreign information you would normally check PROTECTED A or B to identify foreign RESTRICTED information. CISD will ensure that the appropriate equivalency is conveyed to the contractor for both access and safeguarding requirements. A requirement for access to NATO classified or Foreign classified will trigger a Foreign Ownership Control and Influence (FOCI) evaluation of the company. This evaluation must be completed before you can allow a contractor access to any classified information or assets.

8.63 BLOCK 8: COMSEC information has certain restrictions concerning release and safeguarding therefore you must indicate "YES" and list all the levels (e.g. Secret). If the answer to this block is YES, Notes 1 and 3 at the end of this aide memoire apply. A requirement for access to COMSEC information will trigger a FOCI evaluation of the company.

8.64 BLOCK 9: INFOSEC is a special category of classified Communications Electronic Security (COMSEC) information. Access to INFOSEC will trigger a FOCI evaluation of the company.

Part B

8.65 BLOCK 10(a): In this block you must indicate the levels of clearance required by the contractor. Multiple levels can be selected if the work can be separated by categorization (e.g. certain work is only Protected A, other work is Secret), then each contractor must hold a clearance commensurate with the information to be accessed. If the work cannot be separated in this manner, the contractor must have a security clearance commensurate with the highest level of information to be accessed.

8.66 BLOCK 10(b): Unscreened personnel are permitted to work on unclassified portions of the contract. Access beyond a reception or public zone is not permitted without the appropriate security clearance level which for an operations zone is Reliability, for a Security Zone is Secret and for a High Security zone is Top Secret. If contractor personnel are working off site and will not have access to any Classified or Protected information assets and resources then 10b would be answered YES and then NO for the second question.

Part C

8.67 BLOCK 11(a): If a contractor will be required to safeguard protected or classified information, assets or resources at their own site, they must have a Document Safeguarding Capability (DSC) commensurate with the highest level of information to be retained. Indicating "YES" will ensure that CISD has cleared the contractor to safeguard this type of information.

8.68 BLOCK 11(b): Same as above

8.69 BLOCK 11(c): Production means production of equipment vice paper production (e.g. assembly line type work with classified components/parts etc.).

8.70 BLOCK 11(d): If the contractor will be required to use their own IT systems to process electronically protected or classified information "YES" must be checked. This will ensure that CISD has verified that their IT systems meet the requirements for processing of Protected or Classified information (see Note 2 at the end of this aide memoire).

8.71 BLOCK 11(e): A link from the contractor's facility to a protected or classified DND IT system requires that the contractor follow specific IT requirements (see Note 2 at the end of this aide memoire).

Note: If you are completing this form online, a pop-up window will be generated when filling out blocks 11a to 11e. This pop-up window will ask you for the various levels of information to be safeguarded at the contractor's facility. When completing a printed copy of this form the chart on page three of the SRCL must be completed by hand. You may complete the form electronically and submit a signed .pdf copy to the +SRCL@VCDS DGDS@Ottawa-Hull mailbox.

8.72 BLOCK 12(a): Indicate "YES" if any of the information provided on the SRCL form itself is of a Protected or Classified nature (e.g. Contract description – **Block 4**).

8.73 BLOCK 12(b): Indicate "YES" if any of the supporting contractual documentation (Statement of Work, RFP etc.) is of a Protected/Classified nature. In this instance, the SRCL must also be marked with the highest classification of the supporting documentation (e.g. "SECRET // Unclassified Less Attachments").

8.74 BLOCK 13: To be signed by Requirement Owner or equivalent.

8.75 BLOCK 14: The only acceptable signature is that of the DGDS Contract Security Analyst.

8.76 BLOCK 15: If there are special security requirements above and beyond those in the Policy on Government Security (PGS) "YES" would be indicated. Please indicate any special requirements in a separate attachment.

8.77 BLOCK 16: For contracts where PSPC is the signing authority, the PSPC Procurement Officer signs here. For contracts where DND has the delegated signing authority the appropriate DND Procurement Authority will sign.

8.78 BLOCK 17: Always write PSPC.

Administrative Process

8.79 The Requirement Owner is responsible for completing the Security Requirements Check List (SRCL). After the Requirement Owner has completed the SRCL (see Notes 2 and 3 at the end of this aide memoire) it must be forwarded along with the contractual documentation (Request for Proposal, Statement of Work, etc.) via e-mail to: +SRCL@VCDS DGDS@Ottawa-Hull.

8.80 If the SRCL or supporting documentation is above Protected A, you must send via mail to:

DGDS/DDSO Industrial Security
SRCL and Visits Section
Department of National Defence
National Defence Headquarters
101 Colonel By Drive
Ottawa, Ontario
K1A 0K2

8.81 The Corporate Security Support Analyst will conduct a review of the SRCL package to determine that all relevant information has been provided. The SRCL will be registered in our database and placed in the queue. The SRCL Analyst will analyse the SRCL package and interact directly with the DND Project Authority where questions exist or clarification of the submission is required. At completion of analysis, the SRCL Analyst will sign **Block 14** of the SRCL and attach a Security Guide. A signed electronic copy of the SRCL will be sent directly to CISD and the DND OPI will be carbon-copied (cc'd).

NOTE 1 – Canadian Citizenship Requirements

8.82 There is an existing process for determining and communicating the national security-related requirements on the part of Security and Intelligence (S&I) departments to restrict some government contracts to Canadian citizens only. This process requires the S&I departments to take a rigorous look at their requirements, engage with their legal services and PSPC's legal services and provide letters that explain the process followed, refer to international agreements, assess the risks associated with their requests, and assume responsibility for such risks.

8.83 The National Security Special Contracting Caveat (NSSCC) provides departments with direction concerning determining and then documenting the decision to restrict a contract or portions thereof, to Canadian citizens.

8.84 The Interim Protocol (ADM level sign off) only applies to those contracts where PSPC is the contracting authority. Some scenarios that will trigger the requirement to restrict a contract in whole or in part, to Canadian citizens are:

- **a.** the contractor will require access to Canadian or Canadian/another country "eyes only" information, assets or resources;
- **b.** the contractor will require access to Top Secret/SIGINT information, assets or resources;
- **c.** the contractor will require access to COMSEC information, assets or resources; or
- **d.** an MOU requires that contractor personnel having access to the information be a citizen of the participating countries.

NOTE 2 – IT Security Requirements Document

8.85 PSPC CISD requires that departments advise them of any specific requirements that contractors must follow when processing classified or protected information on their own IT systems – **Block 11(d)** of SRCL (e.g. specific password or system architecture requirements). This information must be outlined in the **IT Security Requirements Document** and submitted with the SRCL. PSPC will ensure that contractors comply with these requirements. Assistance with completing the **IT Security Requirements Document** or review of the document can be sought via e-mail at ++DWAN National ISSO-OSSI National du RED@ADM(IM) DIM Secur@Ottawa-Hull.

NOTE 3 – COMSEC

8.86 All contracts that identify a requirement for access to Accountable COMSEC Material (ACM) or COMSEC information, assets, or resources must be sent to the Departmental COMSEC Authority (DCA) for review prior to being sent to DGDS. The DCA will confirm via e-mail that the SRCL identifies and addresses the applicable COMSEC policy and procedural requirements for ACM associated with the contract are met. This confirmation e-mail must accompany the SRCL when sent to DGDS Industrial Security. The SRCL and the Statement of Work should be sent to the following positional mailbox for the COMSEC review: **DWAN**: ++DIM Secur COMSEC ADMIN@ADM(IM) DIM Secur@Ottawa-Hull or **CSNI**: +DIM Secur COMSEC ADMIN@ADM(IM) DIM Secur@Ottawa-Hull.

Annex D: Obtaining Security Services from other Organizations

Introduction

8.87 Security services are provided by other government departments, agencies and industry to support DND and the CAF, as required or mandated (e.g. security guard services).

8.88 The use of contracted security services provides the supervisor or manager of a project or organization the ability to maintain a baseline level of security. Any use by DND and the CAF of contracted security services must be appropriate for, and consistent with, the relevant security posture. Given the security risks associated with contracted security services, other security measures should be assessed first, such as the installation of signs, barriers, etc. Provision of these measures may reduce or eliminate the requirement for contracted services.

8.89 The procedures outlined here apply only to the employment of civilian security services that perform a direct security function, such as access control, traffic control, visitors' escort, security patrols, etc. Approved procedures or Post Orders must be in place outlining the duties and responsibilities of the security guards in all such functions.

8.90 The objectives of this Annex are to ensure that:

- **a.** service providers are able to provide the security service levels which are required by DND and the CAF in order to deliver essential services; and
- **b.** security services acquired by DND are supported by contracts that will ensure the continuous delivery of essential services and support.

8.91 When additional security services are obtained, a contract must be put in place to clearly state the respective responsibilities of DND and the CAF and the service provider.

8.92 When contracting security services and before any security services are provided, the security screening level for required personnel must be confirmed through the Visit Clearance Request (VCR) process. The statement of requirements must clearly outline:

- **a.** the respective responsibilities of DND, the CAF and the service provider to ensure that the service provider holds the relevant license; and
- **b.** that the requested security services are relevant to each site. This can be determined by a Threat and Risk Assessment.

8.93 Contracted security guards must:

- **a.** hold an appropriate license within the province or territory or country of placement in which the Defence Organization is located;
- **b.** hold the required level of security screening; and
- **c.** be employed by a company registered with PSPC's Controlled Goods Program when delivering their services during silent hours at a site where they have access to controlled goods or perform escort duties aimed at preventing examination of a controlled good by an unregistered contractor.

8.94 Guards must be security screened at least to the level of sensitive (classified or protected) information or assets to which they have direct access. In this context, the meaning of direct access includes access by guards because they hold keys to security containers, offices and control monitoring systems. It also means having the appropriate screening for escorting of

individuals in restricted areas. Direct access does not mean access resulting from the discovery of a security breach. Examples of the work permitted at various security screening levels are:

a. **Reliability Status** – Gate guards or escorts who will have no access to attractive items, weapons, ammunition, explosives or classified information;

b. **Secret** – Guards or escorts for a building where classified information or assets (up to Secret), weapons, ammunition, explosives, or controlled goods are held; and for guards monitoring intrusion alarm systems; and

c. **Top Secret** – Guards that have access to areas containing Top Secret information.

Enquiries

8.95 Any enquiries pertaining to this Annex are to be addressed to the Director General Defence Security (DGDS) Industrial Security Staff at DND-Industrial.Security-Security.Industriel-MND@forces.gc.ca.

Annex E: Canadian Industry Visits to Defence Establishments

Introduction

8.96 Industry may require access to DND and CAF property, or to Protected or Classified information, assets, or resources. In some cases, a contract will outline the security clearance requirements for the company and its employees by way of a Security Requirements Check List. Before a company or its employees can be given access to DND or CAF property that contains protected or classified information, assets or resources, a security screening must be verified using a Visit Clearance Request (VCR).

8.97 Public Services and Procurement Canada/Industrial Security Sector (PSPC/ISS) is the department responsible for the verification of personnel security screenings for all companies and their employees registered with PSPC's program.

Procedures

8.98 For recurring visits the process is:

- **a.** the security officer for the visiting company will initiate the VCR process by submitting a VCR form to PSPC/ISS; and
- **b.** PSPC/ISS will verify that the contract stated on the VCR is current and valid, that a Security Requirements Check List has been completed and that the personnel listed on the VCR hold the requisite clearance. For pre-contractual discussions of a protected or classified nature, the company must include a letter of invitation from DND with their VCR submission to PSPC/ISS:
  - **i.** once PSPC/ISS has completed its verification, the VCR is forwarded to the DGDS/DDSO Industrial Security section;
  - **ii.** the DGDS/DDSO Industrial Security section generates a visit approval; and
  - **iii.** the visit approval is then forwarded to the DND Requirement Owner and to the PSPC/ISS who will inform the company that the visit has been approved.

8.99 For **one time visits** (less than one week) a DND Requirement Owner may forgo the formal VCR process and request clearance confirmation via the DGDS/DDSO positional mailbox at +Visit Clearance Requests@VCDS DGDS@Ottawa-Hull. DGDS/DDSO Industrial Security section will verify the individual's security clearance and provide an e-mail confirmation to the originator. The following information must be sent to DGDS/DDSO:

- **a.** full name and date of birth of contractor;
- **b.** dates of visit;
- **c.** purpose of visit; and
- **d.** Security clearance required.

Note: The visit approval will only indicate a clearance level commensurate with the level of information required to be accessed (e.g. if the person holds a Top Secret but the contract only requires access to Secret, the visit approval will show the contractor's clearance as Secret).

8.100 The visit approval does not automatically provide access to Defence establishments. The requirement for access or for access passes is determined locally by the DND Requirement Owner.

Temporary Help Services Contracts

8.101 Temporary Help Services can provide short-term contracts, up to a maximum of 48 weeks in length, which may be used to fill a gap in staffing, emergency provision of services, or to meet a short term requirement that cannot be filled through normal processes.

8.102 DND and CAF Organizational Authorities requiring confirmation of personnel security clearance or reliability screening for personnel employed through temporary services, must e-mail the DGDS Industrial Security at: +Visit Clearance Requests@VCDS DGDS@Ottawa-Hull, and provide the following information:

- **a.** individual's full name and date of birth;
- **b.** standing Offer number;
- **c.** company which employs the individual;
- **d.** security clearance required; and
- **e.** duration of their employment with DND or the CAF.

8.103 The DGDS/DDSO Industrial Security will confirm the security clearance or reliability status with PSPC/ISS, and provide a visit approval via e-mail to the DND or CAF Requirement Owner. Personnel must **not** be engaged until this process has been completed.

Annex F: Visits of DND Employees and CAF Members to Industry

Introduction

8.104 Once industry is awarded a contract they have a responsibility to ensure that anyone having access to protected or classified information, assets, or resources that they are safeguarding, must have the proper security clearance. This includes DND employees and CAF members. As such, a Visit Clearance Request (VCR) will be staffed from DND or the CAF to Industry.

Procedures

8.105 When sending DND employees or CAF members to industry, the following steps must be completed:

- **a.** the DND or CAF Requirement Owner must ensure that there is a valid contract;
- **b.** the DND or CAF Requirement Owner must verify that that there is a Security Requirements Check List included in the contract documentation;
- **c.** the DND or CAF Requirement Owner must verify (through their USS) that each DND employee or CAF member to visit industry holds a valid clearance commensurate with the requirements of the contract;
- **d.** the DND or CAF Requirement Owner must complete the VCR form and sign section 10 indicating that they have confirmed the security requirements and all security clearances;
- **e.** the DND or CAF Requirement Owner must send the VCR form via e-mail to +Visit Clearance Requests@VCDS DGDS@Ottawa-Hull to DGDS/DDSO Industrial Security;
- **f.** DGDS/DDSO Industrial Security generates a request and forward it to PSPC/ISS, and PSPC/ISS will forward the request to the Company Security Officer (CSO);
- **g.** the CSO will approve or reject the request and advise PSPC/ISS. PSPC/ISS will advise the Visits Section of DGDS/DDSO Industrial Security of the approval or rejection; and
- **h.** DGDS/DDSO Industrial Security will then generate an approval or rejection reply and notify the DND or CAF Requirement Owner.

8.106 Contractor personnel who are required by DND or CAF to visit another company in relation to a DND contract can be added to a DND to Canadian Industry visit provided that:

- **a.** the individual is on a valid “Industry to DND” visit; and
- **b.** the individual’s company does not have a related contract with the company to be visited.

Note: If the contracted individual’s company has a related contract with the company to be visited, the company must submit a “Company to Company” VCR through PSPC.

Annex G: Visits of Representatives of Other Government Departments and Agencies to Defence Establishments

Introduction

8.107 Personnel from Other Government Departments (OGDs) or agencies who are required to visit Defence establishments for the purpose of accessing property, or protected or classified information, assets or resources must meet the security clearance requirements.

Procedures

OGD to Defence – Recurring Visits

8.108 The departmental security office's personnel security screening section of the OGD must provide DND or the CAF Requirement Owner with confirmation of each visiting individual's security clearance with date of expiry.

8.109 The DND or CAF Requirement Owner must then forward the confirmation to the DDSO Industrial Security along with the following information:

- **a.** the duration of the visit;
- **b.** the purpose of the visit;
- **c.** the security clearance required for visit;
- **d.** the full name and contact information of the DND or CAF Requirement Owner (if different from the person who submitted the request); and
- **e.** the DGDS/DDSO Industrial Security will generate a VCR approval and send back to the DND or CAF Requirement Owner.

OGD to Defence – One Time Visits

8.110 For **one time visits** (less than one week) a DND or CAF Requirement Owner may forgo the VCR process above and request clearance confirmation via the DGDS/DDSO positional mailbox at +Visit Clearance Requests@VCDS DGDS@Ottawa-Hull. The following information must be included:

- **a.** full name and date of birth of contractor or employee;
- **b.** name of OGD;
- **c.** purpose of visit; and
- **d.** Security clearance required.

8.111 DGDS/DDSO Industrial Security section will verify the individual's security clearance and provide an e-mail confirmation to the Requirement Owner.

Defence to OGD

8.112 DND employees or CAF members who will be visiting OGDs or Agencies are required to provide proof of security clearance upon request by the OGDs.

Défense nationale National Defence

Ordonnances et directives de sécurité de la Défense nationale

Chapitre 8 : Sécurité industrielle et des contrats

Ministère de la Défense nationale et Forces armées canadiennes

Version 2.0 Ce document contient : 35 pages État : Final

Date d'entrée en vigueur : 2015-06-08

Références annulées :

- Politique de sécurité du ministère de la Défense nationale
- Instructions de sécurité de la Défense nationale
- Manuel de sécurité de la Défense

Les politiques, directives et normes du MDN et FAC pertinentes pour ce chapitre des ODSDN :

- DOAD 2006-0, Sécurité de la Défense

Date de la dernière mise à jour et de la modification d'une section :

2016-05-03 – Changements majeurs

- Annexes D à G ajoutées

2016-06-15 – Changements mineurs

- De nouvelles instructions de manutention à la page 1.

2016-08-11 – Changements mineurs

- De nouvelles instructions de manutention à la page 1.

2017-09-11, Changement corrélatif

- Ajouter au Tableau 1 : Commandant du commandement du renseignement des forces canadiennes et chef du renseignement de la défense;
- Mise à jour du Tableau 3 : des exigences pour l'accès aux zones de haute sécurité et l'accès à un local isolé pour matériel spécial
- Révisions à l'Annexe E, paragraphe 8.99.b, Accès à la propriété du MDN et FAC re des visites ponctuelles
- Mise en place d'un nouveau système de navigation affectant les en-têtes, les pieds de page et tous les numéros de paragraphe

Table des matières

Cette page est intentionnellement laissée en blanc

Section 1: Généralités

Les présentes Ordonnances et directives de sécurité de la Défense nationale (ODSDN) sont publiées sous l'autorité du Directeur général – Sécurité de la défense (DGSD) pour le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC). Les ODSDN sont destinées à l'usage du MDN et des FAC et ne doivent pas être diffusées au public. Les ODSDN peuvent être partagés, au besoin, avec les contracteurs à n'importe quel moment du processus contractuel. Seules les sections jugées nécessaires à l'octroi ou à l'exécution du contrat doivent être fournies.

Toute demande concernant la sécurité et le traitement approprié des ODSDN doit être acheminée au Directeur – Politique, instruction et sensibilisation (Sécurité de la défense) à l'adresse DND.DGDSPolicies-DGSDPolitiques.MDN@forces.gc.ca.

Application

8.1 Les Ordonnances et directives de sécurité de la défense nationale (ODSDN) concernent les activités et les opérations du MDN et des FAC. Elles sont des directives qui s'appliquent aux employés du ministère de la Défense nationale (employés du MDN) et des ordonnances qui s'appliquent aux officiers et aux militaires du rang des Forces armées canadiennes (membres des FAC).

Contexte

8.2 Le Ministère de la Défence nationale prend des engagements contractuels avec l'industrie pour le MDN et les FAC, en vue de l'acquisition de biens, de la prestation de services, d'activités de construction et de services de location. Dans le contexte de ce chapitre, un contrat est une entente (de son élaboration à sa fermeture) entre un responsable des achats et l'autorité contractante, et un individu ou une firme, avec le but de fournir un bien, donner un service, construire un bâtiment ou pour louer un site contre rémunération.

8.3 Dans certains cas, une seule organisation combine les fonctions de responsable des achats et d'autorité contractante. Il incombe au directeur général – Sécurité de la Défense (DGSD) de s'assurer que les exigences de sécurité sont identifiées, sont mises en place et sont maintenues en ce qui concerne les contrats conclus entre le MDN, les FAC et l'industrie. Ce chapitre relate ce qui doit être mis en application pour assurer la sécurité dans les ententes contractuelles avec l'industrie.

Remarque : La sécurité industrielle et des contrats consiste en la mise en place de mesures et de procédures de protection pour prévenir, détecter et récupérer de la perte ou de la compromission d'informations sensibles partagées avec l'industrie à des fins contractuels.

Objectifs, exigences et résultats attendus

Objectifs

8.4 Les objectifs présentés dans ce chapitre visent à s'assurer que :

a. les contrats conclus par le MDN et les FAC bénéficient du niveau de protection approprié grâce à l'intégration de mesures de sécurité à toutes les phases de leurs cycles de vie ;

b. les exigences en matière de sécurité sont déterminées, officiellement documentées, respectées et surveillées de manière uniforme et précise pour tous les contrats conclus en vue de l'acquisition de biens, de la prestation de services, d'activités de construction et de services de location ;

c. toute personne devant avoir accès à des biens sensibles du MDN ou des FAC, à l'information ou aux ressources doit faire l'objet d'un filtrage de sécurité au niveau approprié avant le début de leurs tâches ;

d. les informations, les biens et les ressources, protégés ou classifiés, confiés aux entrepreneurs et aux organisations ou créés par ces derniers dans le cadre d'un contrat avec le MDN ou les FAC sont protégés conformément aux lois, règlements et politiques, en matière de sécurité ;

e. l'état final de la sécurité globale d'un contrat est clairement défini ; et

f. les risques résiduels sont acceptés de façon officielle par l'autorité compétente (voir le Chapitre 3 : Gestion des risques liés à la sécurité).

Exigences

8.5 Les exigences en matière de sécurité doivent faire partie intégrante du contrat conclu entre le MDN et les FAC et l'entrepreneur en ce qui concerne tous les contrats passés en vue de l'acquisition de biens, de prestations de services, d'activités de construction et de services de location. Ces exigences en matière de sécurité s'appliquent aux dispositions contractuelles, aux contrats de services professionnels et aux contrats d'entretien des installations, mais ne se limitent pas aux projets de construction et d'acquisition de matériel.

8.6 Tous les employés du MDN et les membres des FAC doivent déterminer les mesures de sécurité et les intégrer aux contrats, ceci à toutes les phases de leur mise en œuvre, afin de s'assurer que les informations, les biens et les ressources relatifs au MDN et aux FAC confiés aux entrepreneurs et aux organisations ou créés par ces derniers sont protégés conformément aux normes définies par le MDN et les FAC.

8.7 Toutes modifications apportées aux mesures minimales de référence relatives à la sécurité décrites dans ces Ordonnances et directives de sécurité doivent être appliquées conformément à un processus officiel de gestion des risques (voir le Chapitre 3 : Gestion des risques liés à la sécurité). Dans l'éventualité où une organisation serait dans l'incapacité de se conformer aux normes de référence, une autorisation écrite (une dérogation) pour toute dérogation doit être obtenue auprès du DGSD.

Résultats attendus

8.8 Les résultats attendus dans le présent chapitre sont les suivants :

a. le MDN et les FAC instaurent des mesures de sécurité à toutes les phases des contrats conclus en vue de l'acquisition de biens, de prestations de services, d'activités de construction et de services de location ;

b. le processus de gestion des risques en matière de sécurité défini par le MDN et les FAC est appliqué et respecté de manière constante et correcte dans le cadre des contrats conclus par ces derniers, tel que prévu dans les présentes Ordonnances et directives ;

c. les informations, les biens et ressources, protégés ou classifiés, relatifs au MDN et aux FAC, détenus par les entrepreneurs ou d'autres organisations ou mis à leur disposition, sont protégés conformément aux présentes Ordonnances et directives ; et

d. les risques résiduels, le cas échéant, sont acceptés par les autorités compétentes.

Processus relatif à la sécurité dans les contrats

8.9 Il est essentiel que les exigences relatives à la sécurité soient identifiées et évaluées dès le début, au cours de la phase d'identification, et réévaluées tout au long des phases du projet. Tout manquement en ce sens entraîne souvent une augmentation des risques à la sécurité et une hausse des coûts, des ressources gaspillées et des retards. Il est impératif que les conseillers de sécurité locaux (p. ex., l'officier de la sécurité des systèmes d'information (OSSI), le surveillant de la sécurité de l'unité (SSU), la police militaire (PM), etc.) soient consultés afin de s'assurer que les exigences relatives à la sécurité sont bien définies. Si des précisions et une orientation supplémentaires sont requises, les Agents régionaux de sécurité du ministère (ARSM), les autorités fonctionnelles (directeur de la Sécurité de la gestion de l'information (Dir Sécur GI), le centre national spécial, bureau de l'accès et du transfert de la technologie contrôlée (ATTC) ou le DGSD peuvent être consultés. Pour gérer le processus relatif à la sécurité des contrats du projet, il convient de suivre les étapes indiquées à l'Annexe A, Tableau 2: Processus relatif à la sécurité des contrats.

8.10 Le processus relatif à la sécurité dans les contrats explique les activités essentielles liées à la sécurité à inclure dans les contrats. Ces dernières concernent les documents d'identification de la sécurité (DIS), des évaluations de la menace et des risques (ÉMR) relatives au projet, une liste de vérification des exigences relatives à la sécurité (LVERS), une demande de permis de visite (DPV). À titre d'aide pour les exigences de filtrage de sécurité, Annexe A : Tableau 3 : Niveaux de sécurité minimaux pour les activités liées aux contrats contient les niveaux de sécurité minimaux pour diverses activités relatives aux contrats.

8.11 Le détenteur du besoin est l'entité administrative responsable de l'identification des exigences en matière de sécurité. Le détenteur du besoin est aussi responsable de s'assurer que tous les contrats disposent d'une ÉMR à jour et complète. Le format et la portée de l'ÉMR ne sont pas strictement définis. La souplesse ainsi offerte permet à l'ÉMR de satisfaire aux besoins de chaque contrat. En général, les auteurs des ÉMR doivent envisager les risques de sécurité tout au long de la durée du contrat, à compter de l'identification d'un produit livrable, puis tout au long du cycle de vie du produit livrable, le cas échéant, y compris lors de la destruction du matériel ou des informations générées par le contrat.

> Remarque : Le détenteur du besoin, en tant qu'autorité contractante, est la personne ou l'organisation détentrice des exigences en matière de sécurité.

8.12 Une ÉMR de base locale peut être utilisée en remplacement d'une ÉMR spécifique pour un contrat lorsque les risques liés au dit contrat sont couverts par l'ÉMR de base. Lorsque l'utilisation d'une ÉMR de base est envisagée, il est conseillé de consulter l'ARSM local. Pour plus de détails sur les ÉMR, se reporter Chapitre 3 : Gestion des risques liés à la sécurité.

Document d'identification de la sécurité (DIS)

8.13 Le DIS est un document du DGSD qui fournit aux autorités contractuelles et les chargés de projets une référence afin de faciliter leur tâche dans l'élaboration des ÉMR et des listes de

vérification des exigences relatives à la sécurité (LVERS). Le DIS permet d'informer le DGSD des exigences relatives à la sécurité dans des contrats spécifiques. La partie A du DIS doit être remplie pour les contrats qui ont trait aux marchandises contrôlées et aux activités menées dans une pièce sécurisée d'une zone de sécurité ou dans une zone de haute sécurité. La partie B du DIS doit être remplie pour les contrats qui exigent que l'entrepreneur ait accès aux systèmes d'information du MDN ou des FAC, et dans le cadre desquels les installations de l'entrepreneur traitent les données électroniques ou transmettent des données au MDN ou aux FAC par voie électronique. Par ailleurs, la partie B du DIS doit être remplie pour chaque installation de l'entrepreneur et pour chaque entrepreneur participant à un contrat. Une fois rempli, le DIS doit être envoyé à la section de la sécurité industrielle du DGSD. Une analyse du DIS par le personnel de la sécurité industrielle permettra de déterminer le niveau d'intervention requis au contrat. Le modèle du DIS se trouve à l'Annexe B : Document d'identification de la sécurité (DIS).

> **Remarque :** Pour plus d'information sur les contrats liés à des biens contrôlés, les employés du MDN ainsi que les membres FAC peuvent consulter la DOAD 3003-1, Exigences relatives aux marchandises contrôlées en matière de gestion, de sécurité et d'accès, tableau des mesures de protection pour les biens contrôlés non-classifiés.

Liste de vérification des exigences relatives à la sécurité (LVERS)

8.14 La LVERS est un formulaire du Conseil du Trésor (CT) utilisé pour définir les exigences de sécurité associées à **tous** les contrats. La LVERS permet de s'assurer que les clauses de sécurité appropriées sont déterminées par l'autorité contractante (AC), de sorte qu'elles puissent être intégrées au contrat, ce qui a pour effet d'engager juridiquement l'entrepreneur à satisfaire aux exigences relatives à la sécurité du contrat. La LVERS doit accompagner tous les documents contractuels, y compris les contrats de sous-traitance qui contiennent des exigences relatives à la sécurité. Des directives sur l'élaboration de la LVERS se trouvent à l'Annexe C : Instructions concernant la liste de vérification des exigences relatives à la sécurité.

8.15 En ce qui concerne les contrats impliquant des dépendances ou des implications relatives aux technologies de l'information (TI), le document comprenant les exigences en matière de sécurité TI doit être rempli. Ce document présente les exigences en matière de sécurité spécifiques aux TI auxquelles l'entrepreneur devra satisfaire pour pouvoir traiter les informations électroniques protégés, classifiés ou sensibles du MDN et des FAC. Des directives sur l'élaboration du document comprenant les exigences en matière de sécurité TI sont disponibles sur le site Web du Dir Sécur GI.

8.16 La LVERS doit être remplie et signée par le détenteur du besoin. La LVERS doit être transmise pour approbation au responsable de la sécurité de l'organisme (+SRCL@VCDS DGDS@Ottawa-Hull) accompagnée de la documentation contractuelle applicable. Après vérification, le DGSD envoie la LVERS à l'autorité contractante en matière de sécurité (Direction de la sécurité industrielle canadienne (DSIC) des Services publics et Approvisionnement Canada (SPAC) pour vérification et en vue de la définition des clauses de sécurité appropriées à intégrer dans tous les contrats à venir.

8.17 S'il est déterminé qu'aucune exigence relative à la sécurité n'est requise dans un contrat, le détenteur du besoin devra signer la LVERS. Dans un tel cas, il n'est pas nécessaire d'expédier la LVERS au DGSD pour signature, toutefois, une copie signée doit être conservée dans le dossier du contrat.

Niveau de filtrage de sécurité des entrepreneurs

8.18 Les entrepreneurs qui retiendront ou auront besoin d'accéder à des marchandises contrôlées, à des installations, des informations, des actifs ou des ressources protégés ou classifiés ou de les conserver devront obtenir les niveaux de filtrage de sécurité comme suit :

- **a.** les entrepreneurs doivent être filtrés au plus haut niveau de sécurité des informations et des biens qui leur sont confiés, c.-à-d. :
  - **i.** vérification d'organisation désignée (VOD) pour les contrats de niveau protégé uniquement ; et
  - **ii.** attestation de sécurité d'installation (ASI) pour les contrats de niveau classifié ;
- **b.** les entrepreneurs qui traiteront par voie électronique des informations protégées ou classifiées doivent disposer d'une capacité de traitement TI approuvée correspondant au niveau de classification de sécurité des renseignements à traiter, et doivent avoir obtenu le niveau de filtrage de sécurité correspondant à l'accès requis pour les informations ou les biens ; et
- **c.** les contracteurs ayant accès à des biens contrôlés doivent s'enregistrés auprès du programme de biens contrôlés des SPAC ou bien être déclarés exemptés du programme.

8.19 Les procédures contractuelles doivent être élaborées afin d'allouer le temps nécessaire afin que les personnes embauchées, ainsi que leur personnel, puissent obtenir les niveaux de filtrage de sécurité requis à temps pour le début des travaux ou la mise en place des services visés.

> Remarque : L'inscription au Programme des marchandises contrôlées est obligatoire en vertu de la loi pour toute personne qui examine, qui a en sa possession ou qui transfère des marchandises contrôlées au Canada. De l'information additionnelle est disponible pour les employés du MDN et les membres des FAC via la DOAD 3003-1 ; Exigences relatives aux marchandises contrôlées en matière de gestion, de sécurité et d'accès, et le tableau des mesures de protection pour les marchandises contrôlées non classifiées.

Local pour conversation sensible situé à l'extérieur d'un établissement de la défense

8.20 Lorsqu'un local de conversation sensible est situé dans les locaux d'un entrepreneur, services publics et approvisionnement Canada (SPAC) est responsable pour sa certification. Lorsque ce local est utilisé pour sauvegarder de l'information du Gouvernement du Canada, sa conception, sa construction et le filtrage de sécurité des contractants doivent être en accord avec ces ordres et directives. La police militaire peut assister en tant que conseiller, mais les LCS des entrepreneurs ne tombent pas dans son mandat principal.

Incapacité de répondre aux exigences en matière de sécurité

8.21 Lorsque des contracteurs n'ont pas encore obtenu l'attestation de sécurité requise pour leur personnel devant accéder à une zone de travail alors que les démarches d'obtention sont en cours avec SPAC, ou un gestionnaire supérieur peut prendre la responsabilité du risque et permettre aux contracteurs d'accéder, sous observation continue, à une zone de travail. L'état des procédures liées à l'obtention d'une attestation de sécurité peut être identifié en communiquant avec SPAC - Programme de Sécurité des contrats. Les cas d'atténuation du risque doivent être coordonnés avec un ARSM et conservés dans un registre local pour fins de vérifications et d'analyse tendancielles. Le registre devra inclure la date à laquelle un contracteur aura finalement obtenu son attestation de sécurité.

8.22 Pour les cas non couverts, le détenteur du besoin ne peut pas assumer un niveau de risque qui réduirait la posture de sécurité sous la norme de sécurité dictée par ces ordres et directives. Lors de telles situations, le détenteur du besoin devra remplir un formulaire officiel, soit le plan d'atténuation du risque (voir le Plan d'atténuation du risque). Ce plan doit inclure une description de la situation, les exigences de sécurité ne pouvant être rencontrées, les impacts sur les opérations et les mesures d'atténuation du risque devant être appliquées. Le formulaire d'atténuation du risque et la LVERS doivent être expédiées à l'ARSM pour initier la procédure d'approbation.

Accompagnement

8.23 L'accompagnement des entrepreneurs qui ne satisfont pas au niveau de sécurité requis pour pouvoir accéder librement à un site peut être approuvé par le DGSD dans des circonstances particulières, mais pas comme stratégie récurrente d'atténuation de risques en matière de sécurité. En cas d'accompagnement, il est important de noter ce qui suit :

- **a.** les escortes ne doivent pas être utilisées pour des travaux effectués à l'intérieur d'un local isolé pour matériel spécial (LIMS) sans recevoir l'approbation du Centre national spécial (CNS) et du DGSD ;
- **b.** les escortes ne doivent pas être utilisées pour permettre à du personnel ne détenant pas une cote de sécurité appropriée l'accès aux zones de sécurité ou de haute sécurité. Toutefois, l'utilisation d'une escorte peut être justifiée afin de minimiser les risques à la sécurité sur les sites accessibles aux contracteurs détenant l'attestation de sécurité appropriée selon les normes minimales établies ;
- **c.** lorsque les entrepreneurs doivent travailler dans une zone de travail pour laquelle ils ne disposent pas du niveau de filtrage de sécurité approprié, des escortes peuvent être demandées grâce au processus indiqué ci-haut (8.22). Cependant, pour ce faire, l'entrepreneur doit avoir entamé le processus de filtrage de sécurité avec le programme de sécurité des contrats de SPAC et continuer ses efforts pour compléter le processus ;
- **d.** en cas de réparations d'urgence, c.-à-d. de réparations imprévues habituellement de moins d'une semaine, les escortes peuvent être autorisées par l'officier du Génie construction de l'unité ou une autorité équivalente en collaboration avec la police militaire locale et les ARSM ; et
- **e.** les personnes nécessitant accès à une zone de travail en support à un contrat futur avec le MDN et ne détenant pas la cote de sécurité appropriée peuvent se voir autorisées l'accès, avec des mesures de contrôles de sécurité, pour les visites requises avant l'octroi d'un contrat.

Vérifications

8.24 Le DGSD peut effectuer des visites de conformité pour vérifier que les mesures d'atténuation du risque approuvées sont mises en œuvre comme prévu et que les pratiques en cours sont conformes aux présentes exigences de sécurité. Les exigences de conformité se retrouvent au Chapitre 2 : Surveillance, contrôle et conformité (le Cadre de conformité à la sécurité).

Demandes de permis de visite (DPV)

8.25 Bien remplir les DPV assure la conformité et réduit le risque que des personnes ou des organismes non légitimes aient accès aux organisations et aux biens sensibles de la défense. Pour en savoir plus sur les DPV, se reporter à l'Annexe E : Visites de représentants de l'industrie canadienne aux établissements de défense.

8.26 Il incombe au BPR du MDN (p. ex., le détenteur du besoin, ou le chargé de projet) et au SSU d'assurer l'application des mesures de sécurité liés tant à une entente contractuelle qu'à toutes visites de représentants de personnes embauchées aux installations du MDN. En ce sens, le BPR du MDN doit s'assurer de limiter l'accès à la propriété, à l'information, aux biens et ressources ainsi qu'aux secteurs et lieux sécurisés uniquement au personnel visé par une entente contractuelle et démontrant une légitimité face au besoin de savoir et aux besoins d'accès. Le BPR du MDN doit confirmer qu'un tel accès correspond aux niveaux de sécurité indiqués pour chaque individu identifié sur la formule de visite approuvée. Le BPR du MDN est responsable de la coordination pour les laissez-passer et doit informer le SSU responsable de chaque site visité des détails (date, horaire, lieu, etc.).

Obtention de services de sécurité

8.27 Se reporter à l'Annexe D : Obtention de services de sécurité auprès d'autres organisations pour en savoir plus sur les contrats de services de sécurité civils relatifs à une fonction de sécurité directe, p. ex., le contrôle d'accès, le contrôle de la circulation, l'escorte des visiteurs, les patrouilles de sécurité, etc.

Rôles et responsabilités

Tableau 1 : Rôles et responsabilités

Le(s)...	est / sont responsable(s) de...
Directeur général de la Défense et sécurité	▪ donner des conseils relatifs à la sécurité à propos des contrats et des dispositions contractuelles conclus pour des biens, des services, des activités de construction, et des services de location ; ▪ assurer la surveillance et la conformité de la sécurité pour les contrats conclus pour des biens, des services, des activités de construction, et des services de location ; ▪ rendre compte au VCEMD à propos de tout risque de sécurité important associé à un contrat ; ▪ signer en tant que responsable de la sécurité de l'organisation pour la LVERS ; et ▪ coordonner le programme de DPV pour les contrats.
Sous-ministre adjoint (Infrastructure et environnement)	▪ s'assurer du respect des présentes Ordonnances et directives dans le cadre de tous les marchés immobiliers ; et ▪ mettre en œuvre des politiques et procédures décrivant la façon dont toutes les activités de passation de marchés immobiliers seront exécutées au MDN.
Sous-ministre adjoint (Matériels)	▪ acquisition et contrats pour le ministère de la Défense nationale ; et ▪ voir à la conformité de l'application des contrôles de la défense (International Traffic In Arms Regulation (ITAR)) et le programme de gestion des SPAC sur les biens contrôlés.

Le(s)...	est / sont responsable(s) de...
Sous-ministre adjoint (Gestion de l'information)	▪ passer en revue les LVERS et recommander l'approbation des exigences en matière de sécurité TI ; et ▪ présenter la politique et les procédures en matière de sécurité des TI pour toutes les acquisitions TI et les activités de passation de marchés menées par le MDN.
Commandant du commandement du renseignement des forces canadiennes et chef du renseignement de la défense	▪ s'assurer de l'application du contrôle d'accès sécurisé et le système de manutention des informations sensibles cloisonnées (SCI) ainsi que du matériel interne au MDN/FAC (comme le Talent Keyhole (TK) et le renseignement spécial (SI)) ; ▪ encadrer l'utilisation et la certification des locaux isolés pour matériel spécial (LIMS) ; et ▪ faire respecter, au nom du centre de la sécurité des télécommunications (CST), les normes de sécurité canadiennes pour le SIGINT au sein du MDN/FAC.
Groupe de la Police militaire des Forces canadiennes	▪ soutenir les responsables de la sécurité du MDN et des FAC en ce qui à trait la prestation de conseils de sécurité concernant les contrats conclus en vue de l'acquisition de biens, de prestations de services, d'activités de construction et de services de location ; et ▪ fournir des conseils à l'autorité contractante à propos de l'utilisation de services de sécurité.
Niveaux 1	▪ informer le DGSD des nouvelles idées de projet en soumettant les DIS au DGSD ; ▪ identifier les autorités opérationnelles et s'assurer que ces dernières connaissent le processus relatif à la sécurité dans les contrats ainsi que les organisations responsables ; ▪ veiller à ce que les procédures d'atténuation des risques relatifs à la sécurité tel qu'identifiées soient mise en application, gérant ainsi la mise en œuvre des mesures de sécurité tel qu'identifiées dans le guide de sécurité joint au contrat ; ▪ soumettre une LVERS lorsqu'un entrepreneur doit avoir accès à des marchandises contrôlés, à des informations protégées ou classifiées, des biens , des ressources ou des installations dans le cadre de ses tâches ; ▪ veiller à ce que les DPV soient soumis, le cas échéant ; ▪ s'assurer que les exigences relatives à la sécurité aient été déterminées tout au long du contrat ; et ▪ s'assurer que les procédures d'atténuation des risques relatifs à la sécurité déterminées dans le guide de sécurité joint au contrat sont mises en œuvre et mises en application.
Commandants, Gestionnaires et superviseurs de tous les niveaux	▪ déterminer les exigences en matière de sécurité des informations, des biens et des ressources en ce qui a trait aux contrats conclus en vue de l'acquisition de biens, de prestations de services, d'activités de construction et de services de location.

Le(s)...	est / sont responsable(s) de...
Responsable des achats et autorité contractante	▪ s'assurer que les exigences nécessaires en matière de sécurité pour protéger les information, les biens, les ressources et les systèmes d'information du gouvernement sont prises en compte dans les modalités des contrats ; ▪ s'assurer que les entrepreneurs et leurs employés, qui ont besoin d'accéder aux informations, biens et ressources protégés et classifiés ont le niveau de filtrage de sécurité requis ; et ▪ s'assurer que le DGSD est informé du renvoi de tout contracteur pour des raisons liées à la sécurité. Cette procédure doit être suivie par l'envoi d'un courriel au personnel de la sécurité industrielle du DGSD : +Industrial Security@VCDS DGDS@Ottawa-Hull. Remarque : En fonction du niveau de délégation, l'autorité contractante appropriée pourrait être le MDN ou SPAC.

Remarque : Services publics et Approvisionnement Canada (SPAC) administre le Programme de Sécurité contrats et gère le programme de Marchandises contrôlées pour le gouvernement du Canada. SPAC veille au filtrage de sécurité des compagnies du secteur privés et leurs employés (p. ex., Vérifications d'organisations désignées, Attestation de sécurité d'installation et Autorisation de détenir des renseignements) en spécifiant des clauses contractuelles via le processus lié à la liste de vérification des exigences relatives à la sécurité (LVERS) et en vérifiant les niveaux de filtrage de sécurité ainsi que le besoin de connaître via le processus de demande de permis de visite. Pour certains contrats du MDN et des FAC, SPAC agira comme autorité contractante, de sorte que le sous-ministre adjoint (matériel) (SMA (Mat)) sera le responsable des achats. Cette procédure sera requise pour les contrats dont la valeur excède un certain montant.

Références

Références externes

Liste de vérification des exigences relatives à la sécurité

Manuel de la sécurité industrielle des SPAC

Norme de sécurité et de gestion des marchés

Outil d'évaluation de la complexité et des risques des projets

Programme de Sécurité contrats des SPAC

Politique sur la sécurité du gouvernement

Références internes

Directive d'approbation des projets

DOAD 3003-0, Marchandises contrôlées

DOAD 3003-1, Exigences relatives aux marchandises contrôlées en matière de gestion, de sécurité et d'accès

DOAD 3016-0, Exception au titre de la sécurité nationale dans les accords commerciaux

DOAD 6003-0, Sécurité des technologies de l'information

DOAD 6003-2, Gestion du risque lié à la sécurité des technologies de l'information

Manuel d'administration des achats

Demandes de renseignements

8.28 Les demandes de renseignements concernant les chapitres doivent être transmises au directeur général – Sécurité de la défense, Section des politiques à l'adresse suivante : DND.DGDSPolicies-DGSDPolitiques.MDN@forces.gc.ca.

Définitions

8.29 Toutes les définitions sont disponibles dans le glossaire des ODSDN.

Annexe A : Aide-mémoire concernant le processus relatif à la sécurité dans les contrats

Introduction

8.30 Les étapes présentées dans le tableau ci-dessous fournissent une orientation dans le cadre du processus de mise en œuvre des mesures de sécurité dans les contrats. En raison de la diversité des exigences liées aux contrats, toutes les étapes ne s'appliquent pas à chaque cas. Les demandes de renseignements spécifiques à propos de ce processus peuvent être adressées au personnel responsable de la sécurité industrielle du DGSD (+Industrial Security@VCDS DGDS@Ottawa-Hull).

Tableau 2: Processus relatif à la sécurité des contrats

Étape	Mesure	Horaire	Responsabilités
1	L'élaboration d'un document d'identification de la sécurité (DIS) est requise lorsqu'un contrat a trait à des marchandises contrôlées, de l'information contrôlée et des activités qui se trouvent ou se dérouleront au sein d'une zone de sécurité ou d'une zone de haute sécurité	▪ La rédaction du DIS facilite l'identification des exigences contractuelles et permet l'identification de documents connexes tel que l'énoncé de projet (ÉP) ▪ Il doit être révisé avant toute modification majeure apportée à l'énoncé de besoin (ÉB)	▪ Document d'identification de la sécurité (Annexe B : Document d'identification de la sécurité (DIS))
2	Déterminer l'autorité pertinente en matière de sécurité pour le projet, et mener à bien une évaluation de la menace et des risques (ÉMR)	▪ Détermination lors de l'identification	▪ Autorité locale en matière d'ÉMR
3	Envisager de mettre en place un groupe de travail sur la sécurité du projet (GTSP)	▪ Variable selon les activités du projet ▪ Prise en compte précoce des questions relatives à la sécurité qui seront bénéfique au projet	▪ DGSD
4	Déterminer les exigences du système d'information en matière de sécurité	▪ Détermination lors de l'identification des exigences du contrat ou du projet, au besoin	▪ Dir Sécur GI et l'officier de sécurité du système d'information (OSSI) régional ou local
5	Envisager le besoin de communications sécurisées dans le cadre du projet	▪ Détermination lors de la définition du contrat ou selon les exigences du projet ▪ Les exigences devront être reconsidérées s'il y a modification des participants au projet ainsi qu'aux activités	▪ DGSD ▪ Dir Sécur GI

Étape	Mesure	Horaire	Responsabilités
6	Envisager l'exigence pour tout entrepreneur de disposer de niveaux de filtrage de sécurité ou d'un parrainage de Services publics et Approvisionnement Canada (SPAC) si l'entreprise n'est pas déjà enregistrée	▪ Considération bien à l'avance du processus d'appel d'offres	▪ DGSD
7	Envisager les exigences d'enregistrement au programme des marchandises contrôlées des SPAC appliquées aux sociétés et aux entrepreneurs si des marchandises contrôlées sont impliquées	▪ Considération bien avant l'approvisionnement des entrepreneurs en marchandises contrôlées	▪ Bureau ATTC
8	Évaluer les autorisations étrangères requises tel que selon International Traffic in Arms Régulations (ITAR) et Export Administration Régulations (EAR)	▪ Prévoir les délais requis afin d'obtenir les autorisations étrangères avant la diffusion de la demande de proposition	▪ Bureau ATTC
9	Élaborer une liste de vérification des exigences relatives à la sécurité (LVERS) et un document comprenant les exigences en matière de sécurité TI (le cas échéant)	▪ Considération bien à l'avance du processus d'appel d'offres	▪ DGSD ▪ Dir Sécur GI ▪ SPAC
10	Élaborer un document sur les exigences en matière de sécurité des contrats à l'aide de informations venant de l'EMR afin d'effectuer la livraison à l'entrepreneur dans le cadre de l'EDT	▪ Le document sur les exigences en matière de sécurité des contrats est créé après détermination ▪ Il sera fourni une fois le processus de soumission terminé et le contrat signé	▪ Aide-mémoire relatif au Cadre de gestion du risque lié à la sécurité de la défense
11	Envisager les exigences relatives à la sécurité à inclure dans toute invitation en vue d'un enregistrement	▪ Considération bien avant l'envoi de l'invitation ▪ Envisager d'envoyer un avis d'achats anticipés avec la LVERS afin de permettre aux entrepreneurs d'entreprendre le processus de filtrage de sécurité	▪ DGSD ▪ Autorité contractante ▪ responsable des achats
12	Envisager les exigences relatives à la sécurité pour une séance d'information de l'industrie	▪ Considération bien avant l'organisation d'une séance d'information de l'industrie	▪ DGSD ▪ Autorité contractante

Étape	Mesure	Horaire	Responsabilités
13	Envisager les exigences en matière de sécurité à inclure dans tout document de demande (demande de propositions), demande de prix, appel d'offres, etc.	▪ Considération bien avant la diffusion de documents de demande	▪ DGSD ▪ Autorité contractante ▪ Responsable des achats ▪ SMA(Mat) ▪ Chargé de la gestion des contrats du MDN
14	Envisager les exigences relatives à la sécurité à inclure dans les contrats	▪ Considération avant la signature des contrats	▪ Autorité contractante ▪ responsable des achats du MDN
15	Examiner le plan de mise en œuvre de sécurité des entrepreneurs	▪ L'entrepreneur sera tenu de soumettre son propre plan de mise en œuvre de la sécurité, conformément au document sur les exigences en matière de sécurité des contrats	▪ DGSD

8.31 Le tableau ci-dessous identifie les normes minimales acceptables pour le filtrage de sécurité des personnes embauchées. En autorisant l'accès pour entrer dans l'aire, c'est important de restreindre l'accès à l'information, conformément au Chapitre 6 : Sécurité de l'information et aux Normes de sécurité de l'information. L'accès à de l'information délicate doit toujours être limité aux individus avec le niveau de filtrage de sécurité approprié et qui ont démontrés un besoin de savoir.

Tableau 3 : Niveaux de sécurité minimaux pour les activités liées aux contrats

Tâche/exigence		Niveau de filtrage de sécurité
Accès à la zone de travail	Activités de logistique (livraison, réception, collecte de rebus, etc.)	Non requis sous contrôle intégral
	Passer sans s'arrêter (pas de travail)	Non requis sous contrôle intégral
	Visites sans contrat octroyé	Non requis sous contrôle intégral
	Toutes autres activités contractuelles	Cote de fiabilité
Accès aux zones de sécurité		Secret
Accès aux zones de haute sécurité		Secret avec Très Secret escorte

Tâche/exigence	Niveau de filtrage de sécurité
Accès à un local isolé pour matériel spécial (LIMS)	Secret avec Très Secret SCI escorte
Entrepreneurs intégrés qui accèdent aux marchandises contrôlées dans les locaux du MDN et ou des FAC	Secret
Construction d'une installation dont l'utilisation finale sera une zone de travail d'opérations	Cote de fiabilité
Construction d'une installation dont l'utilisation finale sera une zone de sécurité sans salle spéciale	Cote de fiabilité
Conception et construction d'une installation dont l'utilisation finale sera une zone de sécurité avec un local pour conversations sensibles (LCS)	Secret
Conception d'une pièce pour l'entreposage d'armes, d'une salle des communications sécurisée ou d'une salle d'entreposage sécurisée dotée de systèmes de sécurité électroniques	Secret
Conception et construction d'une pièce pour l'entreposage d'armes, d'une salle des communications sécurisée ou d'une salle d'entreposage sécurisée sans système de sécurité électronique	Cote de fiabilité
Conception et construction d'une installation dont l'utilisation finale sera une zone de haute sécurité ou un local isolé pour matériel spécial (LIMS)	Secret
Manipulation ou expédition d'armes légères, d'explosifs ou d'équipement classifié	Secret
Participation à la conception et l'installation de tout élément d'un réseau de distribution protégé	Secret
Conception et installation d'un système de sécurité électronique, avec alarme d'intrusion, contrôle d'accès et systèmes de surveillance (systèmes protégés)	Cote de fiabilité
Conception et installation d'un système de sécurité électronique, avec alarme d'intrusion, contrôle d'accès et systèmes de surveillance (systèmes classifiés)	Secret
Conception et installation d'un système de sécurité électronique, avec alarme d'intrusion, contrôle d'accès et systèmes de surveillance (entreposage d'armes)	Secret

Annexe B : Document d'identification de la sécurité (DIS)

Document d'identification de la sécurité

8.32 Les parties A et B du Document d'identification de la sécurité sont disponibles dans la Répertoire des formulaires de la Défense : Partie A DND 4133-F et Partie B DND 4134-F.

Partie A

8.33 La partie A de la DIS doit être complétée pour les projets ou contrats impliquant les besoins d'accès de contracteurs à une salle spéciale dans une zone de sécurité; dans une zone de haute sécurité ou donnant accès à de l'information, des biens et des ressources classifiés de niveau II ou plus. La DIS est un document requérant d'être maintenu à jour avec toute nouvelle information pertinente accumulée. Le supplément aux systèmes d'information pour la DIS doit être soumis par le gestionnaire de projet à l'équipe de sécurité industrielle du Directeur général – Sécurité de la Défense (+Industrial Security@VCDS DGDS@Ottawa-Hull).

Partie B

8.34 La partie B de ce formulaire doit être complétée pour les projets ou contrats requérant que les personnes embauchées aient accès aux systèmes informatiques du MDN et des FAC ou lorsque les établissements manipulent et transmettent des données électroniques de manière électronique. De plus, cette partie doit aussi être complétée pour chaque établissement en question et pour chaque contracteur impliqué dans le contrat.

8.35 Le supplément aux systèmes d'information pour la DIS doit être soumis par le gestionnaire de projet à l'équipe de sécurité industrielle du Directeur général – Sécurité de la défense (+Industrial Security@VCDS DGDS@Ottawa-Hull).

Annexe C : Instructions concernant la liste de vérification des exigences relatives à la sécurité

Introduction

8.36 La Liste de vérification des exigences relatives à la sécurité (LVERS) est un formulaire du Conseil du Trésor (CT) à utiliser pour définir les exigences de sécurité associées à un contrat.

8.37 La LVERS doit accompagner tous les contrats et les contrats de sous-traitance. La LVERS vise aussi les commandes subséquentes aux offres à commandes et aux accords d'approvisionnement.

8.38 La LVERS et le document sur les exigences en matière de sécurité TI (le cas échéant) garantissent que les clauses appropriées relatives à la sécurité sont incorporées à un contrat par la Direction de la sécurité industrielle canadienne (DSIC) des SPAC, ce qui a pour effet d'engager juridiquement l'entrepreneur pour s'assurer que les exigences en matière de sécurité sont respectées. Si ces clauses ne sont pas incluses, l'entrepreneur n'a aucune obligation juridique de protéger les informations, les biens et les ressources du MDN ou des FAC qui lui sont confiés.

8.39 La LVERS doit être jointe à tous les contrats. Avec la LVERS, les exigences en matière de sécurité TI (le cas échéant) doivent être soumises dans un document séparé.

Processus

8.40 La LVERS, ainsi que les exigences en matière de sécurité TI (le cas échéant) doivent être remplies et signées par le détenteur du besoin. Se reporter à Appendice 1 : Aide-mémoire pour remplir la LVERS pour connaître les détails sur la façon de remplir la LVERS. Pour connaître les détails relatifs au Document en matière de sécurité informatique, se reporter au site Web du Dir Sécur GI.

> Remarque : La LVERS doit être envoyée avec les documents contractuels applicables à la section de la sécurité industrielle du DGSD pour approbation +SRCL@VCDS DGDS@Ottawa-Hull.

8.41 La section de la sécurité industrielle du DGSD acheminera la LVERS au personnel de la DSIC des SPAC aux fins d'approbation et de rédaction des clauses de sécurité à inclure dans le contrat. La LVERS et les clauses de sécurité connexes indiquent à l'entrepreneur les exigences de sécurité associées à l'invitation à soumissionner et au contrat subséquent.

8.42 Une LVERS est toujours requise et doit être documentée dans le dossier du contrat. Lorsque le contrat ne fait pas l'objet d'exigences en matière de sécurité, une copie de toute LVERS remplie doit quand même être conservée dans le dossier du contrat.

Incapacité de répondre aux exigences en matière de sécurité

8.43 Lorsque les exigences de sécurité jugées requises ne peuvent être mises en application, le détenteur du besoin ne doit pas en assumer le risque lorsqu'une telle situation réduit la posture de sécurité à un niveau inférieur aux exigences établies dans les présentes ordonnances et directives. Dans un tel cas, le détenteur du besoin devra remplir et soumettre le formulaire d'atténuation du risque comme décrit à l'Annexe C, Plan d'atténuation du risque.

8.44 Le Chapitre 3 : Gestion des risques liés à la sécurité, décrit le processus d'atténuation des risques. Cette approche doit indiquer la situation, les exigences de sécurité ne pouvant être remplies, les impacts sur les opérations ainsi que les mesures d'atténuation permettant de maintenir un niveau de risque BAS. La stratégie d'atténuation du risque doit être transmise à l'Agent régional de sécurité ministérielle (ARSM) qui devra initier la procédure d'approbation.

Vérifications

8.45 Le DGSD peut effectuer des visites pour vérifier que les mesures d'atténuation du risque approuvées ont été mises en œuvre tel qu'indiqué et que les pratiques en cours sont conformes à la politique de sécurité.

Plan d'atténuation du risque

8.46 Ce plan, ainsi que la LVERS correspondante (si disponible), doivent être envoyées à l'ARSM approprié.

a. Un modèle du Plan d'atténuation du risque est disponible dans la Répertoire des formulaires de la Défense, Formulaire DND 4135.

Aide-mémoire pour Remplir la LVERS

8.47 Voir l'Appendice 1 : Aide-mémoire pour remplir la LVERS.

Appendice 1 : Aide-mémoire pour remplir la LVERS

Introduction

Le présent aide-mémoire aidera les utilisateurs à remplir la LVERS (TBS/SCT 350-103). Même s'il y a de nombreuses situations possibles, une définition générale de chaque bloc figure ci-dessous.

> Remarque : Les questions ou préoccupations concernant ce processus peuvent être adressées à +SRCL@VCDS DGDS@Ottawa-Hull.

Partie A

8.48 BLOC 1 : MDN

8.49 BLOC 2 : Direction (p. ex., VCEMD/DGSD/DOSD)

8.50 BLOC 3(a) : Ignorer – utilisé uniquement pour les contrats principaux ou en sous-traitance

8.51 BLOC 3(b) : Ignorer – utilisé uniquement pour les contrats principaux ou en sous-traitance

8.52 BLOC 4 : Résumé succinct du travail à exécuter

8.53 BLOC 5(a) : Le Programme de marchandises contrôlées géré par SPAC garantit la protection de la propriété, des informations, des biens et des ressources (marchandises contrôlées) qui ont été modifiés à des fins militaires. Certaines marchandises contrôlées sont classifiées, tandis que d'autres sont non classifiées. Aux fins du présent document, les énoncés suivants s'appliquent principalement aux marchandises contrôlées non classifiées, conformément aux exigences de la DOAD 3003-1.

a. Si les personnes embauchées au moyen d'un contrat seront intégrées, bloc 5(a) doit indiquer par un « OUI ». L'entreprise **doit** être enregistrée au Programme des marchandises contrôlées des SPAC et les personnes embauchées au moyen d'un contrat doivent détenir une cote de sécurité SECRET.

> Remarque : Un contracteur intégré est un individu travaillant pour un entrepeneur ayant une entente contractuelle avec le ministère de la Défense nationale (MDN) , celui-ci requiert d'accéder à des marchandises contrôlées ; et accomplit son travail dans une installation du MDN (une installation contrôlée par le MDN et pour lequel le MDN conserve l'autorité et la responsabilité des mesures de sécurité), que ce soit à temps partiel ou à temps plein (aucun travail est accompli hors-site). Le terme « contracteur intégré » réfère à un individu travaillant dans une installation du MDN et non l'entreprise pour laquelle l'individu travaille ou avec qui il détient un contrat de services. Un contracteur intégré ne peut informer son employeur de la nature de son travail et se doit de signer un document afin de formaliser cette exigence.

b. Si les personnes embauchées au moyen d'un contrat exécutent 100 % de leur travail au MDN, mais n'ont pas besoin d'accéder à des marchandises contrôlées, elles ne sont pas considérées comme « intégrées » et la case « NON » du bloc 5a doit être cochée.

Remarque : Si la personne embauchée accomplit son travail à l'intérieur de son propre établissement et nécessitent l'accès à des marchandises contrôlées non classifiées (pas accès à de l'information protégé ou classifié), aucun LVERS est requis, mais il doit être enregistrés au programme de marchandises contrôlées de Services publics et Approvisionnement Canada. Pour de plus amples informations sur les marchandises contrôlées ou pour connaître les informations/biens qui sont contrôlés, veuillez consulter le site Web Accès et transfert de la technologie contrôlée (ATTC).

8.54 BLOC 5(b) : Les données techniques militaires non classifiées diffèrent quelque peu de celles du Programme des marchandises contrôlées. Les entrepreneurs doivent être inscrits au Programme mixte d'agrément. Les questions concernant ce programme doivent être acheminées au site Web du DGPII (directeur général – Programmes internationaux et industriels).

8.55 BLOC 6(a) : Si l'entrepreneur a besoin d'accéder à des informations protégés ou classifiés, la case « OUI » de ce bloc doit être cochée.

8.56 BLOC 6(b) : La case « OUI » de ce bloc doit être cochée si l'entrepreneur a besoin de travailler dans des zones dont l'accès pourrait être réglementé (niveau de filtrage de sécurité requis pour l'accès) alors qu'il n'a **pas** besoin d'accéder à quelque information protégé ou classifié que ce soit (p. ex., les aires de trafic d'aérodrome, les salles ou zones à accès réglementé de l'organisation).

Remarque : L'accès aux installations du MDN impose aux personnes embauchées l'obtention d'un niveau de filtrage de sécurité selon les mesures de contrôle d'accès en place des établissements ou d'installation du MDN. Il est requis d'assurer une identification des individus et l'utilisation de mesures de contrôle d'accès reconnues, etc. Sans exceptions, les exigences à la sécurité contenues dans les présentes ordonnances et directives doivent être appliquées. De plus, des mesures plus restrictives pourraient être mises en œuvre.

8.57 BLOC 6(c) : Ce bloc concerne les messagers locaux (p. ex., messagers à bicyclette, porteurs de main à main). Ces sociétés ne possèdent pas la cote de sécurité leur permettant d'assurer la protection des informations protégés ou classifiés, aussi la sauvegarde de tels informations jusqu'au jour suivant ne leur est-elle pas permise. Le colis doit être retourné à l'expéditeur s'il ne peut pas être livré.

8.58 BLOC 7(a) : Tous les types d'informations auxquels l'entrepreneur aura accès doivent être énumérés ici (canadiens, OTAN, étrangers).

8.59 BLOC 7(b) : Pour certaines informations, il y a des restrictions quant à la diffusion. Vous devez indiquer dans ce bloc si les informations font l'objet de telles restrictions. Se reporter à la remarque 1 à la fin de cet aide-mémoire si le contrat est limité aux citoyens canadiens.

a. Aucune restriction relative à la diffusion **:** les renseignements peuvent être diffusés dans tout pays avec lequel le Canada a établi un protocole d'entente (PE) industriel pour l'échange d'informations protégés, classifiés, ou communiqués à une personne de toute citoyenneté, du moment qu'elle détient le niveau de filtrage de sécurité requis ;

b. À ne pas diffuser : par exemple, « réservé aux Canadiens » ; et

c. Restreint à : la diffusion de certaines informations n'a été approuvée que dans certains pays ou pour des citoyens de certains pays. Vous devez dresser la liste de ces pays ici.

Renseignements de l'OTAN

8.60 L'OTAN ne permet pas la communication de toutes ses informations à tous ses pays membres ; les restrictions à la diffusion doivent être indiquées sous la case « Restreint à » cochée. Voir Chapitre 6 : Sécurité de l'information pour plus de détails.

Renseignements étrangers

8.61 « Aucune restriction de diffusion » – il peut y avoir certaines restrictions concernant la diffusion d'informations de gouvernements étrangers (même relativement aux informations non classifiés). Veuillez-vous assurer que les informations que vous communiquez à un entrepreneur ne font pas l'objet de restrictions (p. ex., « Réservé aux Canadiens », « Restreint à », « Autorisée à », etc.). La diffusion de certaines informations n'a été approuvée que dans certains pays ou pour des citoyens de certains pays. Vous devez dresser la liste de ces pays ici, en dessous de Bloc 7(b).

8.62 BLOC 7(c) : Veuillez indiquer les niveaux auxquels l'entrepreneur est autorisé à divulguer des informations de chaque pays. Veuillez indiquer quels sont les niveaux, au lieu de seulement le niveau le plus élevé. Certains autres pays n'utilisent pas la désignation « PROTÉGÉ ». En ce qui a trait aux renseignements de l'OTAN ou de gouvernements étrangers, vous devez habituellement cocher « PROTÉGÉ A » ou B pour indiquer ceux dont la diffusion est RESTREINTE. La DSIC veillera à ce que l'équivalence appropriée soit communiquée à l'entrepreneur, tant pour les exigences d'accès que pour celles relatives à la protection. Une demande d'accès à de l'information classifié de l'OTAN initiera une évaluation de la compagnie selon les exigences de Participation, contrôle et influence étrangers (PCIE). Cette évaluation doit être complétée avant de pouvoir donner accès à l'entrepreneur à de l'information ou des ressources classifiées.

8.63 BLOC 8 : Les renseignements COMSEC comportent certaines restrictions relativement à la diffusion et à la protection ; par conséquent, vous devez cocher la case « OUI » et énumérer tous les niveaux (p. ex., Secret). Si la réponse à ce bloc est OUI, les remarques 1 et 3 à la fin de cet aide-mémoire s'appliquent. Une demande d'accès à des renseignements COMSEC initiera une évaluation de la compagnie selon les exigences de PCIE.

8.64 BLOC 9 : INFOSEC est une catégorie spéciale d'informations classifiées sur la sécurité des communications électroniques (SECOM/COMSEC). Une demande d'accès à l'INFOSEC initiera une évaluation de la compagnie selon les exigences PCIE.

Partie B

8.65 BLOC 10(a) : Vous devez indiquer les niveaux de filtrage de sécurité que doit obtenir l'entrepreneur. Plusieurs niveaux de filtrage peuvent être identifiés si le travail peut être réparti selon la catégorisation (p. ex., une partie du travail peut être seulement Protégée A, tandis qu'une autre peut être seulement Secrète), chaque entrepreneur doit détenir un niveau de sécurité correspondant au niveau de classification des informations auxquels il aura accès. Si le travail ne peut être ainsi réparti, l'entrepreneur doit détenir un niveau de filtrage de sécurité correspondant au niveau de classification le plus élevé des informations auxquels il aura accès.

8.66 BLOC 10(b) : Les personnes sans autorisation de sécurité sont autorisées à travailler sur les parties sans classification d'un contrat. L'accès à une zone de réception ou publique ne requiert pas de cote de sécurité particulière alors que l'accès à une zone opérationnelle

nécessite une cote de Fiabilité, à une zone de sécurité nécessite une cote de niveau Secret et une zone de haute sécurité une cote de sécurité Très Secret. Si les entrepreneurs/employés embauchés travaillent à l'extérieur du site et n'ont pas accès à de l'information, des biens et des ressources protégé ou classifié, la réponse à la question 10b sera OUI et la réponse à la deuxième question sera NON.

Partie C

8.67 BLOC 11(a) : Si un entrepreneur est tenu de sauvegarder des informations ou des biens protégés ou classifiés à son propre lieu de travail, il doit avoir une Autorisation de détenir des renseignements (ADR) correspondant au niveau le plus élevé de sécurité des informations à sauvegarder. Si vous indiquez « OUI », cela confirmera que la DSIC des SPAC fera la vérification pour ensuite autoriser l'entrepreneur à sauvegarder ce type d'information.

8.68 BLOC 11(b) : Mêmes exigences que ci-dessus

8.69 BLOC 11(c) : Le terme « production » renvoie à la production d'équipement, et non à celle de documents papier (p. ex., production à la chaîne comprenant des composantes classifiées etc.).

8.70 BLOC 11(d) : Si l'entrepreneur est tenu d'utiliser ses propres systèmes informatiques pour traiter électroniquement des informations protégés ou classifiés, vous devez cocher la case « OUI ». Cela garantit que la DSIC vérifiera que ses systèmes informatiques répondent aux exigences de traitement des renseignements protégés ou classifiés (voir la remarque 2 à la fin de cet aide-mémoire).

8.71 BLOC 11(e) : Un lien établi entre l'installation d'un entrepreneur et un système informatique protégé ou classifié du MDN nécessite que l'entrepreneur réponde à certains critères (voir remarque 2 à la fin de l'aide-mémoire).

> Remarque : Si vous remplissez ce formulaire en ligne, une fenêtre contextuelle apparaîtra au moment de remplir les blocs 11a à 11e. Dans la fenêtre contextuelle, on vous demandera d'indiquer les différents niveaux d'information qui devront être protégés à l'installation de l'entrepreneur. Lorsque l'on remplit une copie imprimée du formulaire, le tableau à la page 3 de la LVERS doit être rempli manuellement. Vous pouvez remplir le formulaire électroniquement et soumettre une copie pdf signée en utilisant la boîte courriel +SRCL@VCDS DGDS@Ottawa-Hull.

8.72 BLOC 12(a) : Vous devez indiquer « OUI » si les informations fournies sur le formulaire LVERS sont de nature protégée ou classifiée (p. ex., description du contrat – **Bloc 4**).

8.73 BLOC 12(b) : Vous devez indiquer « OUI » si des documents contractuels à l'appui (énoncé de travail, DDP, etc.) sont de nature protégée/classifiée. Dans ce cas, la LVERS doit également indiquer le niveau le plus élevé de catégorisation attribué aux documents à l'appui (p. ex., SECRET // Non classifié sans les pièces jointes).

8.74 BLOC 13 : La signature du détenteur du besoin ou de son équivalent est requise.

8.75 BLOC 14 : La seule signature acceptable est celle de l'analyste de la sécurité des contrats du DGSD.

8.76 BLOC 15 : En présence d'exigences particulières de sécurité dépassant celles de la Politique du gouvernement sur la sécurité (PGS), il est indiqué de cocher « OUI ». Veuillez indiquer toute exigence particulière dans une pièce jointe séparée.

8.77 BLOC 16 : Pour les contrats où SPAC est le signataire autorisé, l'agent d'approvisionnement des SPAC doit apposer sa signature ici. Pour les contrats où le MDN a le pouvoir de signature délégué, le responsable de l'approvisionnement du MDN signera.

8.78 BLOC 17 : Toujours inscrire SPAC.

Processus administratif

8.79 Le détenteur du besoin est la personne en titre à qui il incombe de remplir la LVERS. Une fois complétée par le détenteur du besoin (voir les remarques 2 et 3 à la fin de cet aide-mémoire), elle doit être envoyée accompagnée du document contractuel (demande de proposition, énoncé des travaux, etc.), par courriel à +SRCL@VCDS DGDS@Ottawa-Hull.

8.80 Si la classification de la LVERS ou des documents à l'appui est supérieure à « PROTÉGÉ A », vous devez la faire suivre par courrier à l'adresse suivante :

DGSD - Sécurité Industrielle
LVERS & Visites
Ministère de la Défense nationale
Quartier général de la Défense nationale
101, promenade Colonel-By
Ottawa ON
K1A 0K2

8.81 L'analyste de soutien en matière de sécurité de l'entreprise examinera la trousse LVERS pour déterminer si toutes les informations pertinentes ont été fournies. La LVERS sera enregistrée dans notre base de données et placée en attente. L'analyste de la LVERS procède à l'analyse de la trousse LVERS et interagit directement avec le chargé de projet du MDN si des questions se posent ou si des clarifications sont requises à propos de la soumission. Une fois l'analyse terminée, l'analyste de la LVERS signe le **Bloc 14** de la LVERS et y joint un guide de sécurité. Une copie électronique signée de la LVERS est envoyée directement à la DSIC et une copie conforme est transmise au BPR du MDN (en Cc).

Remarque 1 : Exigences relatives à la citoyenneté canadienne

8.82 Il y a un processus existant visant à déterminer et à communiquer les exigences liées à la sécurité nationale de la part des ministères chargés de la sécurité et du renseignement, de sorte que certains contrats du gouvernement du Canada soient réservés uniquement à des citoyens canadiens. Ce processus exige des ministères chargés de la sécurité et du renseignement un examen rigoureux de leurs exigences. En collaboration avec des services juridiques de leur ministère et ceux des SPAC, ces ministères doivent rédiger des lettres expliquant le processus suivi et dans lesquelles ils indiquent le renvoi à des accords internationaux étayant leurs décisions, l'affirmation qu'ils sont conscients des risques associés à leur demande et qu'ils assument la responsabilité de ces risques.

8.83 Le contrat exigeant des avertissements de sécurité nationale spéciaux (ASNS) procure une orientation aux ministères en ce qui a trait à la détermination, puis à la documentation de la décision visant à restreindre l'attribution d'un contrat ou de parties d'un contrat à des citoyens canadiens.

8.84 Le protocole provisoire (signature au niveau SMA) ne s'applique qu'aux contrats dont SPAC est l'autorité contractante. Voici **certains** scénarios en vertu desquels l'attribution d'un contrat, en tout ou en partie, devra être limitée à des citoyens canadiens :

a. l'entrepreneur devra avoir accès à des propriétés, informations, biens ou ressources de nature exclusivement canadienne ou canadienne/autre pays ;

b. l'entrepreneur devra avoir accès à des propriétés, informations, biens ou ressources de nature « Très secret/renseignement d'origine électromagnétique (ROEM) » ;

c. l'entrepreneur devra avoir accès à des propriétés, informations et biens ou ressources de nature SECOM ; ou

d. un protocole d'entente (PE) exige que les employés de l'entrepreneur ayant accès aux informations soient citoyens de l'un des pays participants.

Remarque 2 : Document comprenant les exigences en matière de sécurité informatique

8.85 La DSIC exige que les ministères l'avisent de toute exigence particulière que les entrepreneurs doivent observer lors du traitement de informations protégés ou classifiés sur leurs propres systèmes de TI – **Bloc 11(d)** de la LVERS (p. ex., mot de passe spécifique ou exigences concernant l'architecture de système). Ces informations doivent être énoncés dans le **Document comprenant les exigences en matière de sécurité TI** et soumis avec la LVERS. SPAC veillera à ce que les entrepreneurs se conforment à ces exigences. Si vous avez besoin d'aide pour remplir le **Document comprenant les exigences en matière de sécurité TI** ou pour passer le document en revue, procédez par courriel à l'adresse ++DWAN National ISSO-OSSI National du RED@ADM(IM) DIM Secur@Ottawa-Hull.

Remarque 3 : SECOM

8.86 Tous les contrats qui stipulent une exigence d'accès à du matériel SECOM à comptabiliser ou à de l'information, des biens ou des ressources SECOM doivent être transmis au responsable ministériel du SECOM pour examen avant d'être transmis au DGSD. Le responsable ministériel du SECOM confirmera par courriel que les exigences liées aux politiques et aux procédures SECOM sont adéquates et ont été identifiées dans la LVERS. Ce courriel de confirmation doit accompagner la LVERS lors de son envoi au DGSD, Sécurité industrielle. La LVERS et l'énoncé de travail doivent être envoyés à l'une des adresses courriel suivante pour évaluation : **RED** : ++DIM Secur COMSEC ADMIN@ADM(IM) DIM SECUR@Ottawa-Hull ou via **CSNI** : +DIM Secur COMSEC ADMIN2ADM(IM) DIM Secur@Ottawa-Hull.

Annexe D : Obtention de services de sécurité auprès d'autres organisations

Introduction

8.87 Des services de sécurité sont fournis par d'autres ministères, agences et industries en guise de soutien au MDN et aux FAC, selon les besoins ou parce qu'ils sont mandatés (p. ex., services de gardes de sécurité).

8.88 L'utilisation de services de sécurité contractuels procure au superviseur ou au gestionnaire d'un projet ou organisation la capacité de maintenir un niveau de sécurité de base. Toute utilisation de services de sécurité contractuels par le MDN et les FAC doit être appropriée et en accord avec la posture de sécurité pertinente. Compte tenu des risques de sécurité associés aux services de sécurité contractuels, d'autres mesures de sécurité doivent d'abord être prises en considération, comme l'installation de panneaux indicateurs, de barrières, etc. La mise en œuvre de telles mesures peut réduire ou éliminer le recours à des services contractuels.

8.89 Les procédures ci-jointes ne s'appliquent qu'à l'utilisation de services de sécurité civils dont la tâche se limite à une fonction de sécurité exclusive, comme le contrôle d'accès, le contrôle de la circulation, l'escorte de visiteurs, les patrouilles de sécurité, etc. Les procédures ou les consignes de poste approuvées doivent être établis et décrire les tâches et responsabilités des gardes de sécurité pour toutes ces fonctions.

8.90 Les objectifs de cette annexe consistent à garantir que :

- **a.** les fournisseurs de services sont en mesure de procurer les niveaux de services de sécurité requis par le MDN et les FAC afin de fournir les services essentiels ; et
- **b.** les services de sécurité acquis par le MDN et les FAC sont appuyés par des ententes garantissant la prestation continue des services essentiels et des mesures de soutien.

8.91 Lors de l'obtention de services de sécurité supplémentaires, une entente contractuelle doit être établie afin d'indiquer clairement les responsabilités respectives du MDN et des FAC, ainsi que du fournisseur de services.

8.92 Lorsque vient le moment de conclure un contrat pour des services de sécurité (avant la prestation de tout service de sécurité) le niveau de filtrage de sécurité pour le personnel requis doit être confirmé dans le cadre du processus de Demande de permis de visite (DPV). L'énoncé des exigences doit clairement définir :

- **a.** les responsabilités respectives du MDN, des FAC et du fournisseur de services, et démontrer que celui-ci détient le permis pertinent ; et
- **b.** que les services de sécurité sont appropriés pour chaque site. Cela peut être déterminé par une ÉMR.

8.93 Les gardes de sécurité contractuels doivent :

- **a.** détenir un permis approprié dans la province, le territoire ou le pays d'embauche où l'organisation de la Défense est située ;

b. détenir le niveau de filtrage de sécurité requis ; et

c. être un employé d'une compagnie enregistrée au programme de biens contrôlés des SPAC pour la prestation de service pendant les heures silencieuses sur un site leur donnant accès à des biens contrôlés ou en agissant comme escorte pour éviter l'accès à un bien contrôlé par un contracteur non enregistré.

8.94 Les gardes doivent faire l'objet d'un filtrage de sécurité correspondant, au minimum, au niveau des informations sensibles ou des biens (classifiés ou protégés) auxquels ils ont un accès direct. Dans ce contexte, la notion « accès direct » comprend l'accès par des gardes, puisqu'ils détiennent les clés donnant accès aux contenants et bureaux de sécurité, ainsi qu'aux systèmes de surveillance et de contrôle. Cela signifie également que leur niveau de sécurité (déterminé par le filtrage) les autorise à escorter des personnes dans les zones d'accès restreints. La notion « d'accès direct » ne signifie pas une autorisation d'accès à la suite de la découverte d'une infraction à la sécurité. Voici des exemples de travail autorisé à divers niveaux de filtrage de sécurité :

a. **Cote de fiabilité** – Gardiens de guérite ou escortes n'ayant pas accès à des articles attrayants, armes, munitions, explosifs ou informations classifiés ;

b. **Secret** – Gardes ou escortes pour un bâtiment où l'on maintient des informations ou des biens classifiés (jusqu'au niveau SECRET), ou des armes, ou des munitions, ou des explosifs, ou des biens contrôlés; et où les gardiens surveillent les systèmes d'alarme d'intrusion ; et

c. **Très Secret** – Gardes ayant accès à des zones où l'on maintient des informations TRÈS SECRET.

Demandes d'information

8.95 Toute demande d'information concernant cette annexe doit être adressée au DGSD, section de la sécurité industrielle à DND-Industrial.Security-Security.Industriel-MND@forces.gc.ca.

Annexe E : Visites de représentants de l'industrie canadienne aux établissements de défense

Introduction

8.96 L'industrie peut devoir accéder aux biens, aux informations ou aux ressources protégés ou classifiés du MDN et des FAC. Dans certains cas, un contrat décriera les exigences en matière de cote de sécurité pour l'entreprise et ses employés dans une liste de vérification des exigences relatives à la sécurité. Avant que l'accès aux établissements du MDN ou des FAC renfermant des biens, des informations ou des ressources protégés ou classifiés puisse être accordé à une entreprise ou à ses employés, le niveau de sécurité doit être vérifié à l'aide d'une Demande de permis de visite (DPV).

8.97 Le Secteur de la sécurité industrielle (SSI) des SPAC est responsable de la vérification du niveau de filtrage de sécurité de toutes les entreprises enregistrées dans le cadre du programme des SPAC et de leurs employés.

Procédures

8.98 Les procédures à suivre pour les visites récurrentes sont les suivantes :

- **a.** L'agent responsable de la sécurité de l'entreprise qui veut faire une visite lancera le processus de DPV en présentant un formulaire de DPV au SSI des SPAC ; et
- **b.** Le SSI des SPAC devra ensuite vérifier que le contrat mentionné sur la DPV est actuel et valide, qu'une liste de vérification des exigences relatives à la sécurité a été remplie, et que les employés énumérés sur la DPV détiennent l'autorisation requise. En ce qui concerne les discussions précontractuelles dans le cadre desquelles des informations protégés ou classifiés seront échangés, l'entreprise doit joindre à la DPV qu'elle soumet au SSI des SPAC une lettre d'invitation du MDN :
  - **i.** après la vérification du SSI des SPAC, la DPV est transmise au DGSD/DOSD, Section de la sécurité industrielle ;
  - **ii.** le DGSD/DOSD, Section de la sécurité industrielle produit ensuite une approbation de la visite ; et
  - **iii.** l'approbation de la visite est par la suite envoyée aux détenteurs du besoin du MDN et au SSI des SPAC, qui informeront l'entreprise que la visite a été approuvée.

8.99 Pour ce qui est des **visites ponctuelles** (d'une durée de moins d'une semaine), les détenteurs du besoin du MDN peuvent omettre le processus de DPV et plutôt demander une confirmation de la cote de sécurité en envoyant un courriel à la boîte aux lettres générique du DGSD/DOSD à l'adresse +Visit Clearance Requests@VCDS DGDS@Ottawa-Hull. Le DGSD/DOSD, Section de la sécurité industrielle vérifiera la cote de sécurité de la personne concernée et enverra une confirmation par courriel à la personne ayant présenté la demande. Les renseignements suivants doivent être transmis au DGSD/DOSD :

- **a.** nom complet et date de naissance du fournisseur de services contractuel ;
- **b.** date(s) de la visite ;

c. but de la visite ; et

d. cote de sécurité requise.

Remarque : Le niveau de cote de sécurité indiqué dans l'approbation de la visite correspondra au niveau de cote de sécurité que doit détenir la personne pour accéder aux établissements. Par exemple, si un fournisseur de services contractuel détient une cote de niveau Très Secret, mais qu'en vertu du contrat, il doit seulement accéder à des établissements contenant du matériel classé Secret, l'approbation de la visite indiquera qu'il détient une cote de sécurité de niveau Secret.

8.100 L'approbation de la visite ne donne pas automatiquement accès aux établissements de la défense. Le détenteur du besoin du MDN déterminera si un droit d'accès ou des laissez-passer sont requis pour accéder à chacun des établissements.

Contrats de services de travail temporaire

8.101 Les services de travail temporaire peuvent fournir des contrats à court terme (d'une durée maximale de 48 semaines), qui peuvent être utilisés pour combler des lacunes en matière de dotation ou de prestation de services urgente, ou pour combler un besoin à court terme auquel on ne peut répondre par les processus habituels.

8.102 Les BPR du MDN qui ont besoin d'obtenir la confirmation d'une cote de sécurité ou d'une cote de fiabilité pour des services temporaires doivent envoyer un courriel au DGSD, Section de la sécurité industrielle à l'adresse suivante : +Visit Clearance Requests@VCDS DGDS@Ottawa-Hull. Leur message doit contenir les renseignements suivants :

a. nom complet et date de naissance de la personne concernée ;

b. numéro de l'offre à commandes ;

c. entreprise pour laquelle travaille la personne concernée ;

d. autorisation de sécurité requise ; et

e. durée de l'emploi au sein du MDN ou des FAC.

8.103 Le DGSD/DOSD, Section de la sécurité industrielle confirmera la cote de sécurité ou de fiabilité auprès du SSI des SPAC, et transmettra par courriel une approbation de la visite au détenteur du besoin du MDN. Les employés ne doivent **pas** être embauchés avant que ce processus soit achevé.

Annexe F : Visites d'employés du MDN et de membres des FAC dans des installations de l'industrie

Introduction

8.104 Une fois qu'un contrat est attribué à une entreprise, il incombe à cette dernière de veiller à ce que toute personne ayant accès aux informations, aux biens ou aux ressources protégés ou classifiés dont l'entreprise assure la protection possède une cote de sécurité appropriée. Cela s'applique aussi aux employés du MDN et aux membres des FAC. Le MDN ou les FAC doivent donc présenter une Demande de permis de visite (DPV) à l'industrie pour les visites dans les installations de celle-ci.

Procédures

8.105 Lors des visites d'employés du MDN ou de membres des FAC dans des installations de l'industrie, les mesures suivantes doivent être prises :

- **a.** les détenteurs du besoin doivent s'assurer qu'un contrat valide a été conclu ;
- **b.** les détenteurs du besoin doivent vérifier qu'une liste de vérification des exigences relatives à la sécurité a été jointe aux documents contractuels ;
- **c.** les détenteurs du besoin doivent vérifier (par l'entremise de son surveillant de la sécurité de l'unité) que chaque employé du MDN ou membre des FAC qui doit visiter des installations de l'industrie détient une autorisation valide conformément aux exigences stipulées dans le contrat ;
- **d.** les détenteurs du besoin doivent remplir le formulaire de DPV et signer la section 10, attestant ainsi qu'il confirme les exigences relatives à la sécurité et toutes les cotes de sécurité ;
- **e.** les détenteurs du besoin doivent envoyer le formulaire de DPV par courriel au DGSD/DOSD, Section de la sécurité industrielle à l'adresse suivante : +Visit Clearance Requests@VCDS DGDS@Ottawa-Hull ;
- **f.** le DGSD/DOSD, Section de la sécurité industrielle produit une demande qu'il transmet au SSI des SPAC, qui l'enverra ensuite à l'agent de sécurité d'entreprise ;
- **g.** l'agent de sécurité d'entreprise approuvera ou rejettera la demande et en informera le SSI des SPAC. Le SSI des SPAC en informera ensuite la Section des visites de la Section de la sécurité industrielle (DGSD/DOSD) ; et
- **h.** le DGSD/DOSD, Section de la sécurité industrielle approuvera ou rejettera la demande et avisera les détenteurs du besoin du MDN ou des FAC.

8.106 Le personnel du fournisseur de services contractuel qui doit, selon les directives du MDN ou des FAC, visiter une autre entreprise en raison d'un contrat du MDN peut être ajouté à une visite du MDN de l'industrie canadienne sous réserve des conditions suivantes :

a. la personne participe à une visite de l'« industrie au MDN » valide ; et

b. l'entreprise de la personne concernée n'a pas conclu de contrat connexe avec l'entreprise qui sera visitée.

Remarque : Si l'entreprise de la personne embauchée au moyen d'un contrat a conclu un contrat connexe avec l'entreprise qui sera visitée, elle devra présenter une DPV « entreprise à entreprise » par l'intermédiaire des SPAC.

Annexe G : Visites de représentants des autres ministères ou organismes gouvernementaux au sein des établissements de la défense

Introduction

8.107 Les membres du personnel des autres ministères ou organismes gouvernementaux qui doivent se rendre dans un établissement de la défense pour accéder à des informations, des biens ou à des ressources protégés ou classifiés doivent satisfaire aux exigences en matière d'autorisation de sécurité.

Procédures

Visites d'autres ministères au sein de la Défense - visites récurrentes

8.108 La section du filtrage de sécurité du Bureau de l'ASM d'un autre ministère doit confirmer avec le détenteur du besoin du MDN et des FAC que chaque visiteur possède une autorisation de sécurité, et en préciser la date d'expiration.

8.109 Le détenteur du besoin du MDN ou des FAC doit ensuite envoyer la confirmation au DGSD/DOSD, Section de la sécurité industrielle, de même que les renseignements suivants :

- **a.** la période de visite ;
- **b.** le but de la visite ;
- **c.** l'autorisation de sécurité requise pour la visite ;
- **d.** le nom complet et les coordonnées du détenteur du besoin du MDN (s'il est différent de celui de la personne qui a présenté la demande) ; et
- **e.** le DGSD/DOSD, Section de la sécurité industrielle approuvera la DPV et la renverra au détenteur du besoin du MDN.

Visites d'autres ministères au sein de la Défense - visites ponctuelles

8.110 Pour ce qui est des **visites ponctuelles** (d'une durée de moins d'une semaine), le détenteur du besoin du MDN ou des FAC peut omettre le processus de DPV mentionné précédemment et plutôt demander une confirmation de la cote de sécurité en envoyant un courriel à la boîte aux lettres génériques du DGSD/DOSD à l'adresse suivante : +Visit Clearance Requests@VCDS DGDS@Ottawa-Hull. Les renseignements suivants doivent être inclus :

- **a.** nom complet et date de naissance du fournisseur de services contractuel ou de l'employé ;
- **b.** Nom de l'autre ministère ;
- **c.** but de la visite ; et
- **d.** autorisation de sécurité requise.

8.111 La section de sécurité industrielle du DGSD/DOSD vérifiera la cote de sécurité de la personne concernée et fournira au détenteur du besoin une confirmation par courriel.

Visite de la Défense au sein des autres ministères

8.112 Les employés du MDN ou les membres des FAC qui effectuent des visites à d'autres ministères ou organismes doivent fournir une preuve de leur cote de sécurité, à la demande des ministères en question.