

Addendum / Addenda

Project Description / Description de projet Smart Building Monitoring and On-Going Commissioning - Trenton, Kingston		
Solicitation No./N° de sollicitation 17-22057	Project No./N° de projet	W.O. No./N° d'ordre de travail
Departmental Representative / représentant ministériel Scott Shillinglaw		Date October 16, 2017
Notice: 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.		Nota: 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

17-22057 – Smart Building Monitoring and On-going Commissioning – Trenton , Kingston

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 Technical 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 October 31, 2017 completed March 31, 2018 and in "Appendix C" Mandatory Requirements Checklist award date is January 8, 2018

Answer: The date of October 31, 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. The List of Buildings states that all 3 buildings have 5,000 BAS points. Are these estimates or representative of the true number of BAS points?

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

12. 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.

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

Answer: Yes, the BAS at B605 - TEME communicates with BACnet protocol. Assume that all devices have unique IDs.

14. 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.

15. 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.

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

Answer: No.

17. 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

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 SRCL 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).

18. What are the DND approved network connectivity methods?

Answer: Cellular communication with VPN setup.

19. What loads (HVAC, lighting) are controlled by the BAS to which we are connecting?

Answer:

TEME: HVAC is connected to the BAS. Lighting is not connected to the BAS.

Hanger 1 and 2: HVAC and lighting are connected to the BAS

20. How many main meters are there for each building? Is main meter data available via BAS?

Answer: Assume two main meters: electricity and steam or gas. Assume the main meter data are available via BAS.

21. What other network is Hangar 2 located on? Is it related to the other buildings?

Answer: Hangar 2 is on the FACNET. It is not related to other buildings. TEME and Hangar 1 are standalone systems.

22. 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.

**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	<p>All requirements in section 2.20 Coordination and Schedule</p> <p>Selected Bidder shall be ready to provide the services as required (i.e. facilities and personnel already in place).</p> <p>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.</p> <p>The Bidder shall submit a proposed schedule with their bid.</p> <p>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.</p>		
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	



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

Security Classification - Classification de sécurité	
Our File - Notre référence	
Your File - Votre référence	
Date	16 October 2017

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).



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 Organization / 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. 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 SM	NATO / OTAN	Foreign / Étranger
------------------	-------------	--------------------

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions / Aucune restriction relative à la diffusion	All NATO countries / Tous les pays de l'OTAN	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 :	Restricted to: / Limité à : Specify country(ies): / Préciser le(s) pays :	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?
 Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui
 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?
 Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? No / Non Yes / Oui

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

<input checked="" type="checkbox"/>	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?
 Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? No / Non Yes / Oui
 If Yes, will unscreened personnel be escorted?
 Dans l'affirmative, le personnel en question sera-t-il escorté? No / Non Yes / Oui

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?
 Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui

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

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?
 Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? No / Non Yes / Oui

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?
 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? No / Non Yes / Oui

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



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			CONFIDENTIAL	SECRET	TOP SECRET / TRÈS SECRET
											A	B	C			
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, classifiez 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, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquez qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées) Luc Boulanger		Title - Titre Mechanical Engineer	Signature 
Telephone No. - N° de téléphone 613-922-8778	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel luc.boulanger3@forces.gc.ca	Date 2017-08-31


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

Name (print) - Nom (en lettres moulées) Sasa Medjovic - DDSO - Industrial Security Senior Security Analyst		Title - Titre	Signature 
Telephone No. - N° de téléphone 613-996-0286	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel E-mail: sasa.medjovic@forces.gc.ca	Date 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 Yes
Non Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées) Collin Long		Title - Titre Procurement Officer	Signature 
Telephone No. - N° de téléphone 613-993-0431	Facsimile No. - N° de télécopieur 613-991-3297	E-mail address - Adresse courriel Collin.Long@nrc-cnrc.gc.ca	Date Sept. 11, 2017

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)		Title - Titre	Signature
Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

National Defence Security Orders and Directives

Chapter 8: Industrial and Contract Security



Department of National Defence and Canadian Armed Forces

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

Section 1: General

- Application
- Context
- Objectives, Requirements and Expected Results
- Contract Security Process
- Roles and Responsibilities
- References
- Enquiries
- Definitions

Annex A: Contract Security Process Aids

- Introduction

Annex B: Security Identification Document (SID)

- Security Identification Document Form

Annex C: Security Requirements Check List Instructions

- Introduction
- Process
- Risk Mitigation Plan Template
- Aide Memoire to SRCL Completion

Appendix 1: Aide Memoire to SRCL Completion

- Part A
- Part B
- Part C

Annex D: Obtaining Security Services from other Organizations

- Introduction
- Enquiries

Annex E: Canadian Industry Visits to Defence Establishments

- Introduction
- Procedures
- Temporary Help Services Contracts

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

- Introduction
- Procedures

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

- Introduction
- Procedures



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.DGDS Policies-DGSD Politiques.MDN@forces.gc.ca.

© Government of Canada 2016 All Rights Reserved


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	<ul style="list-style-type: none"> ▪ providing security advice on contracts and contractual arrangements 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)	<ul style="list-style-type: none"> ▪ 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)	<ul style="list-style-type: none"> ▪ 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)	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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...
	<ul style="list-style-type: none"> ▪ ensuring that the security risk mitigation procedures identified within the Security Guide attached to the contract are implemented and enforced.
<p>Commanding Officers, Managers and Supervisors at all levels</p>	<ul style="list-style-type: none"> ▪ identifying security requirements for information, assets and resources with respect to contracts for goods, services, construction, and leases.
<p>Procurement and Contracting Authority</p>	<ul style="list-style-type: none"> ▪ 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. <p>Note: Depending on the level of the delegation, the appropriate Contracting Authority (CA) could be DND or PSPC.</p>

 **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	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> Determined during identification 	<ul style="list-style-type: none"> Local TRA authority
3	Assess whether to establish a Project Security Working Group (SWG)	<ul style="list-style-type: none"> Dependent on contract activities Early assessment of security issues will benefit the contract 	<ul style="list-style-type: none"> DGDS
4	Determine the Information System security requirements	<ul style="list-style-type: none"> Determined during identification of contract or project requirements or as required 	<ul style="list-style-type: none"> DIM Secur and regional or local Information System Security Officer (ISSO)
5	Assess the need for secure contract communications	<ul style="list-style-type: none"> Determined when identifying contract or project requirements Requirement will need to be reconsidered as contract participants and activities change 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Assessed well in advance of the tendering process 	<ul style="list-style-type: none"> DGDS

Step	Action	Schedule	Responsibilities
7	Assess PSPC Controlled Goods Program's registration requirements for firms and contractors if controlled goods are involved	<ul style="list-style-type: none"> Assessed well in advance of the release of any controlled goods to contractors 	<ul style="list-style-type: none"> CTAT Office
8	Assess foreign authorization requirements such as International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR)	<ul style="list-style-type: none"> Assessed well in advance to permit sufficient time to receive foreign authorizations prior to industry briefings and RFPs (Request for Proposals) 	<ul style="list-style-type: none"> CTAT Office
9	Develop a Security Requirements Check List (SRCL) and IT Security Requirement Document (when applicable)	<ul style="list-style-type: none"> Assessed well in advance of the tendering process 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Contract Security Requirements Document is created following identification This will be delivered once the bidding process is completed and the contract has been signed 	<ul style="list-style-type: none"> Defence Risk Management Framework for Security Aide-Memoire
11	Assess security requirements to be included in any Invitation to Register interest	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> DGDS Contracting Authority Procurement Authority
12	Assess security requirements for any Industry Briefing	<ul style="list-style-type: none"> Assessed well in advance of the conduct of an Industry Briefing 	<ul style="list-style-type: none"> DGDS Contracting Authority
13	Assess security requirements to be included in any request documentation (RFP), Request for Quotation, Request for Tender, etc.	<ul style="list-style-type: none"> Assessed well in advance of the release of any request documentation 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Assessed prior to contract signature 	<ul style="list-style-type: none"> Contracting Authority DND Procurement Officer
15	Review contractors' Security Implementation Plan	<ul style="list-style-type: none"> The contractor will produce their own Security Implementation Plan as a result of the Contract Security Requirements Document 	<ul style="list-style-type: none"> 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](mailto:++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](mailto:++DIM Secur COMSEC ADMIN@ADM(IM) DIM Secur@Ottawa-Hull) or **CSNI:** [+DIM Secur COMSEC ADMIN@ADM\(IM\) DIM Secur@Ottawa-Hull](mailto:+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.Industrial-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](mailto:+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 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](mailto:+VisitClearanceRequests@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](mailto:+VisitClearanceRequests@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.