Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau, Québec K1A 0S5
Bid Fax: (819) 997-9776

Title - Sujet Cyber Operator Training	
Solicitation No. - N° de l'invitation W4938-20069S/A	**Date** 2019-12-17
Client Reference No. - N° de référence du client W4938-20069S	
GETS Reference No. - N° de référence de SEAG PW-$$ZH-113-37169	
File No. - N° de dossier 113zh.W4938-20069S	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-01-31**	**Time Zone** **Fuseau horaire** Eastern Standard Time EST
F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes **Plant-Usine:** □ **Destination:** □ **Other-Autre:** ☑	
Address Enquiries to: - Adresser toutes questions à: Reynolds(zh), Diane	**Buyer Id - Id de l'acheteur** 113zh
Telephone No. - N° de téléphone (613) 858-8571 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** See herein Voir aux présentes	

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

There are security requirements associated with this requirement, consult Part 6 and Part 7.

Ce besoin comporte des exigences relatives à la sécurité, consulter la Partie 6 et la Partie 7.

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Delivery Required - Livraison exigée See Herein	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature** **Date**	

Issuing Office - Bureau de distribution

Training and Specialized Services Division/Division de la formation et des services spécialisés
Terrasses de la Chaudière 5th Floo
Terrasses de la Chaudière 5e étage
10 Wellington Street,
10, rue Wellington,
Gatineau
Québec
K1A 0S5

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

PART 2 - BIDDER INSTRUCTIONS

PART 3 - BID PREPARATION INSTRUCTIONS

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

PART 5 - CERTIFICATIONS

PART 6 - SECURITY REQUIREMENTS

List of Attachments:

PART 7 - RESULTING CONTRACT CLAUSES

List of Annexes:

TITLE

Bid solicitation # W4938-20069S/A for the provision of the following professional services: cyber operator training program.

PART 1 – GENERAL INFORMATION

1.1 Introduction

The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, and the basis of selection;

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided;

Part 6 Security Requirements: includes specific requirements that must be addressed by Bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The Attachments include the Pricing Schedule, the Certifications and Additional Information, and the Technical Criteria.

The Annexes include the Statement of Work, the Security Requirements Check List and the Non-disclosure Agreement.

1.2 Summary

The Department of National Defence requires a Contractor to deliver a cyber operator training program that will satisfy the occupation performance requirements for the Canadian Armed Forces Cyber Operator Private Rank Qualification commencing in August 2020. The Contractor must provide a training site and facility which is within the geographical boundaries of Kingston, Ontario or the National Capital Region (NCR).

The period of the Contract is from date of Contract to December 31, 2021 inclusive with the irrevocable option to extend the contract by four additional periods of 17-months each.

The requirement is subject to the provisions of the North American Free Trade Agreement (NAFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Canadian Free Trade Agreement (CFTA).

There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses.

The resulting Contract is not to be used for deliveries within a Comprehensive Land Claims Settlement Area.

This bid solicitation allows bidders to use the epost Connect service provided by Canada Post Corporation to transmit their bid electronically. Bidders must refer to Part 2 entitled Bidder Instructions, and Part 3 entitled Bid Preparation Instructions, of the bid solicitation, for further information.

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person at the sole discretion of the Contracting Authority.

PART 2 – BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the Standard Acquisition Clauses and Conditions (SACC) Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada (PWGSC).

Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

The 2003 (2019-03-04), Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 4 of Section 05, Submission of Bids, of Standard Instructions 2003 incorporated by reference above, is amended as follows:

Delete: 60 days
Insert: 120 calendar days.

2.2 Submission of Bids

Bids must be submitted only to the PWGSC Bid Receiving Unit by the date, time and place indicated on page 1 of the bid solicitation.

Due to the nature of the bid solicitation, bids transmitted by facsimile will not be accepted.

Note: For bidders choosing to submit using epost Connect for bids closing at the Bid Receiving Unit in the NCR, the address is: tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Note: Bids will not be accepted if emailed directly to this email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2003, or to send bids through an epost Connect message if the Bidder is using its own licensing agreement for epost Connect.

2.3 Former Public Servant

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny and reflect fairness in spending public funds. In order to comply with Treasury Board policies and directives on contracts with FPS, bidders must provide the information required in Attachment 2 to Part 3 - Certifications and Additional Information form before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada’s request and meet the requirement within the prescribed time frame will render the bid non-responsive.

2.4 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than 10 calendar days before the bid closing date. Enquiries received after that time may not be answered.

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as “proprietary” will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all bidders. Enquiries not submitted in a form that can be distributed to all bidders may not be answered by Canada.

2.5 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in the province of Ontario, Canada.

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the bidders.

PART 3 – BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

a) Due to the nature of the bid solicitation, bids transmitted by facsimile will not be accepted;

b) The bid must be separated as follows:

Section I: Technical Bid
Section II: Financial Bid
Section III: Certifications and Additional Information;

c) If the Bidder chooses to submit its bid electronically using the epost Connect service provided by Canada Post Corporation:

- Canada requests that the bidder submits its bid in accordance with section 08, Transmission by facsimile or by epost Connect, of the 2003 standard instructions. Sub-section 2, epost connect, contains instructions and conditions; and
- The epost Connect system has a limit of 1GB per single message posted and a limit of 20GB per conversation;

d) If the Bidder chooses to submit its bid to the PWGSC Bid Receiving Unit electronically not using the epost Connect service provided by Canada Post Corporation, Canada requests one envelope containing one copy of the bid on a CD/DVD. The Bidder should ensure that the Bidder's name and address and bid solicitation number are clearly visible on the envelope;

e) Canada is not requesting hard copies of the bid. However, if the Bidder chooses to submit its bid to the PWGSC Bid Receiving Unit in hard copies, Canada requests:

Section I: four hard copies
Sections II and III: one hard copy of the two sections; and

f) If there is a discrepancy between the wording of any copies of the bid that appear on the following list, the wording of the copy that first appears on the list has priority over the wording of any copy that subsequently appears on the list:

- The electronic copy of the bid submitted by using the epost Connect service provided by Canada Post Corporation;
- The electronic copy of the bid submitted to the PWGSC Bid Receiving Unit on a CD/DVD;
- The hard copies of the bid submitted to the PWGSC Bid Receiving Unit.

In accordance with the *Treasury Board Contracting Policy* and the *Accessible Canada Act*, federal departments and agencies must consider accessibility criteria and features when procuring goods or services. Therefore, bidders are encouraged to highlight all the accessibility features and components of their bid for the Statement of Work in Annex A. DAOD 5023-0, Universality of Service, specifies that members must be physically fit, employable and deployable to perform general military duties and common defence and security duties, not just the duties of their military occupation or occupational specification.

This bid solicitation uses Portable Document Format (PDF) technology. To access the PDF form, bidders must have a PDF reader installed. If bidders do not already have such a reader, there are several PDF readers available on the Internet. It is recommended to use the latest version of PDF reader to benefit all features of the interactive forms.

Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

If the Bidder chooses to submit its bid in hard copies, Canada requests that bidders follow the format instructions described below in the preparation of their bid:

a) Use 8.5 x 11 inch (216 mm x 279 mm) paper; and
b) Use a numbering system that corresponds to the bid solicitation.

In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process Policy on Green Procurement (https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/1/60/1).
To assist Canada in reaching its objectives, bidders should:

1. Use paper containing fiber certified as originating from a sustainably-managed forest and containing minimum 30% recycled content; and
2. Use an environmentally-preferable format including black and white printing instead of color printing, printing double sided/duplex, using staples or clips instead of cerlox, duo tangs or binders.

Section I: Technical Bid

In their technical bid, bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

Part 4, Evaluation Procedures, contains additional instructions that bidders should consider when preparing their technical bid.

Section II: Financial Bid

1. Bidders must submit their financial bid in Canadian funds and in accordance with the pricing schedule detailed in Attachment 1 to Part 3;

2. Bidders must submit their prices and rates FOB destination; Canadian customs duties and excise taxes included, as applicable; and Applicable Taxes excluded;

3. When preparing their financial bid, Bidders should review clause 4.1.2, Financial Evaluation, of Part 4 of the bid solicitation; and article 7.6, Payment, of Part 7 of the bid solicitation;

4. In their financial bids, bidders must provide a price breakdown for each firm lot price and each firm unit price quoted in response to the pricing schedule detailed in Attachment 1 to Part 3.

a) Estimated Cost of Professional Fees

For each labour category, bidders must provide the estimated cost of professional fees.

b) Estimated Cost of Information Technology Systems and Equipment

Bidders must identify each information technology system and equipment, and provide the estimated cost.

c) Estimated Cost of Materials and Supplies

Bidders must identify each category of materials and supplies to be purchased, and provide for each one, the estimated cost. Materials and supplies are items which will be consumed during the performance of any resulting contract.

d) Estimated Cost of Subcontracts

Bidders must identify any proposed subcontractors and provide a price breakdown submitted in accordance with paragraph 4 of this section of Part 3 of the bid solicitation for each one.

e) Estimated Cost of Other Direct Charges

Bidders must identify the categories of other direct charges anticipated (e.g. long distance communications, rental, transcript fee, etc.) and provide the estimated cost for each one.

f) Applicable Taxes

The price breakdown must not include the Applicable Taxes.

Section III: Certifications and Additional Information

In Section III of their bid, Bidders should provide the certifications required under Part 5 and, as applicable, any associated documentation and additional information.

a) Bidders must complete their Certifications and Additional Information by using the attached PDF fillable form, Attachment 2 to Part 3 - Certifications.pdf;

b) Bidders should complete the interactive form electronically before printing the document for submission. Bidders should note that simply printing the document prior to completing it electronically may omit certain fields that would appear when filling out the form electronically, resulting in incomplete Certifications; and

c) The form must be signed.

ATTACHMENT 1 to PART 3

PRICING SCHEDULE

The Bidder must complete this pricing schedule and include it in its financial bid.

The prices and fees for each period included in this pricing schedule includes the total estimated cost of any travel and living expenses that may need to be incurred described in Part 7 of the bid solicitation. Under any resulting contract, Canada will not accept travel and living expenses that may need to be incurred by the contractor for any relocation of resources required to satisfy its contractual obligations.

If the Bidder adds any conditions or makes changes to the pricing schedule, the Bidder’s financial bid will be declared non-responsive. Bidders can add additional lines, if required.

1. The Bidder must quote a firm lot price for a class size of 1-12 students.

Contract Period	Firm lot Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
Information technology (IT) support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Student email account for 1-12 students with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder’s student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each class during the Contract Period	$

Option Period 1	Firm Lot Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
IT support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Student email account for 1-12 students with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder's student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each class during Option Period 1	$

Option Period 2	Firm Lot Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
IT support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Student email account for 1-12 students with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder's student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each class during Option Period 2	$

Option Period 3	Firm Lot Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
IT support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Student email account for 1-12 students with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder's student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each class during Option Period 3	$

Option Period 4	Firm Lot Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
IT support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Student email account for 1-12 students with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder's student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each class during Option Period 4	$

Table 1		Firm Lot Price (in Cdn $)
		A
1	Contract Period	$
2	Option Period 1	$
3	Option Period 2	$
4	Option Period 3	$
5	Option Period 4	$
	Total (A1+A2+A3+A4+A5)	$

2. The Bidder must quote a firm unit price per student per semester for each additional student up to a maximum class size of 24 students.

Contract Period	Firm Unit Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
IT support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Individual student email account with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder's student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each semester during the Contract Period	$

Option Period 1	Firm Unit Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
IT support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Individual student email account with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder's student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each semester during Option Period 1	$

Option Period 2	Firm Unit Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
IT support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Individual student email account with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder's student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each semester during Option Period 2	$

Option Period 3	Firm Unit Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
IT support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Individual student email account with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder’s student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each semester during Option Period 3	$

Option Period 4	Firm Unit Price
Professional Fees	
Contract Supervisor	$
Program Coordinator	$
Faculty qualified professors	$
Instructors or teaching assistants	$
IT support	$
Other labour support (e.g. cleaners)	$
IT Systems and Equipment	
Hardware	$
Software	$
Individual student email account with 1 GB of mail storage, a web space account with 5 GB disk space and remote access to the Bidder’s student network	$
Bidder to identify other IT systems and equipment	$
Materials and Supplies	
Bidder to identify materials and supplies	$
Subcontracts	
Bidder to identify subcontracts	$
Other Direct Charges	
Bidder to identify other direct charges	$
Total for each semester during Option Period 4	$

Table 2		Firm Unit Price per Student per Semester (in Cdn $)	Number of Semesters	Estimated Number of Additional Students	Subtotal (in Cdn $)
		A	B	C	D = A x B x C
1	Contract Period	$	4	12	$
2	Option Period 1	$	4	12	$
3	Option Period 2	$	4	12	$
4	Option Period 3	$	4	12	$
5	Option Period 4	$	4	12	$
				Total (D1+D2+D3+D4+D5)	$

3. For a new or replacement textbook, the Bidder will be reimbursed at cost plus the administrative fee. The Bidder must quote an administrative fee. The estimated cost of the textbooks for each period in table 3 is for financial evaluation purposes only.

Table 3		Administrative Fee	Estimated Cost of Textbooks	Subtotal (in Cdn $)
		A	B	C = (A x B) + B
1	Contract Period	%	$24,000.00	$
2	Option Period 1	%	$24,000.00	$
3	Option Period 2	%	$24,000.00	$
4	Option Period 3	%	$24,000.00	$
5	Option Period 4	%	$24,000.00	$
			Total (C1+C2+C3+C4+C5)	$

Summary		A (in Cdn $)
1	Total from Table 1	$
2	Total from Table 2	$
3	Total from Table 3	$
	Total Evaluated Price (Applicable Taxes excluded) (A1+A2+A3)	$

ATTACHMENT 2 to PART 3
CERTIFICATIONS AND ADDITIONAL INFORMATION

See the attached PDF fillable form, Attachment 2 to Part 3 - Certifications.pdf

PART 4 – EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical evaluation criteria.

An evaluation team composed of representatives of Canada will evaluate the bids.

4.1.1 Technical Evaluation

4.1.1.1 Joint Venture Experience

a) Where the Bidder is a joint venture with existing experience as that joint venture, it may submit the experience that it has obtained as that joint venture.

Example: A bidder is a joint venture consisting of members L and O. A bid solicitation requires that the bidder demonstrate experience providing maintenance and help desk services for a period of 24 months to a customer with at least 10,000 users. As a joint venture (consisting of members L and O), the bidder has previously done the work. This bidder can use this experience to meet the requirement. If member L obtained this experience while in a joint venture with a third party N, however, that experience cannot be used because the third party N is not part of the joint venture that is bidding;

b) A joint venture bidder may rely on the experience of one of its members to meet any given technical criterion of this bid solicitation.

Example: A bidder is a joint venture consisting of members X, Y and Z. If a solicitation requires: (a) that the bidder have 3 years of experience providing maintenance service, and (b) that the bidder have 2 years of experience integrating hardware with complex networks, then each of these two requirements can be met by a different member of the joint venture. However, for a single criterion, such as the requirement for 3 years of experience providing maintenance services, the bidder cannot indicate that each of members X, Y and Z has one year of experience, totaling 3 years. Such a response would be declared non-responsive;

c) Joint venture members cannot pool their abilities with other joint venture members to satisfy a single technical criterion of this bid solicitation. However, a joint venture member can pool its individual experience with the experience of the joint venture itself. Wherever substantiation of a criterion is required, the Bidder is requested to indicate which joint venture member satisfies the requirement. If the Bidder has not identified which joint venture member satisfies the requirement, the Contracting Authority will provide an opportunity to the Bidder to submit this information during the evaluation period. If the Bidder does not submitted this information within the period set by the Contracting Authority, its bid will be declared non-responsive.

Example: A bidder is a joint venture consisting of members A and B. If a bid solicitation requires that the bidder demonstrate experience providing resources for a minimum number of 100 billable days, the bidder may demonstrate that experience by submitting either:

- Contracts all signed by A;
- Contracts all signed by B; or
- Contracts all signed by A and B in joint venture, or
- Contracts signed by A and contracts signed by A and B in joint venture, or
- Contracts signed by B and contracts signed by A and B in joint venture.

That show in total 100 billable days; and

d) Any Bidder with questions regarding the way in which a joint venture bid will be evaluated should raise such questions through the Enquiries process as early as possible during the bid solicitation period.

4.1.1.2 Mandatory Technical Criteria

Refer to Attachment 1 to Part 4.

4.1.1.3 Facility Assessment Visit

Canada may visit the facility proposed by the lowest evaluated price and technically responsive Bidder to confirm that the facility is as described in the Bid and that it meets the technical requirements described in the Bid Solicitation.

The Contracting Authority will give the bidder a minimum of 10 working days’ notice prior to the site visit to perform the validation. Canada will then visit the facility and perform the validation. The site visit validation will be completed within two working days. Canada will pay its own costs associated with the site visit validation.

The Bidder grants to Canada for the purpose of the validation, the right to access all sites and facility included in the Bid.

Canada will document the results of the site visit validation. If Canada determines that the Bidder does not meet all the mandatory requirements as outlined in Attachment 1 to Part 4 of the Bid Solicitation document, the Bidder will fail the validation and the Bid will be declared non-responsive. The Bidder will be provided an opportunity to respond and provide proof of how they meet the criteria indicated as non-responsive.

4.1.2 Financial Evaluation

For bid evaluation and Contractor selection purposes only, the evaluated price of a bid will be determined in accordance with the Pricing Schedule detailed in Attachment 1 to Part 3.

4.2 Basis of Selection - Lowest Evaluated Price

a) A bid must comply with the requirements of the bid solicitation and meet all mandatory evaluation criteria to be declared responsive; and

b) The responsive bid with the lowest evaluated price will be recommended for award of a contract.

ATTACHMENT 1 to PART 4
TECHNICAL CRITERIA

1.1 Mandatory Technical Criteria

a) The bid must meet the mandatory technical criteria specified in table below. The Bidder must provide the necessary documentation to support compliance;

b) Any bid which fails to meet the mandatory technical criteria will be declared non-responsive. Each mandatory technical criterion should be addressed separately;

c) In the case of a joint venture, at least one member of the joint venture must meet the mandatory technical criteria. The Bidder must indicate which member of the joint venture it uses for each mandatory technical criterion; and

d) In the case of a joint venture, the parties forming the joint venture cannot combine their experience in order to meet any one of the mandatory technical criteria.

Number	Mandatory Technical (MT) Criterion	Instructions to Bidders
MT1	The Bidder must have been in business for a minimum of three years prior to the bid solicitation publication date.	The Bidder must provide: A copy of business name registration certificate. OR A copy of provincial or territorial business corporation registration certificate. OR A copy of federal business incorporation registration certificate.
MT2	The Bidder must have a training site and facility located within the geographical boundaries of Kingston, Ontario or the National Capital Region.	The Bidder must provide the full address of the training site and facility (civic address, municipality/town, province and postal code).
MT3	The Bidder's training site and facility must include one classroom or computer laboratory that meets the following requirements: a) Must seat up to 24 students; b) Must be equipped with desks and chairs to accommodate up to 24 students; c) Must be equipped with a minimum of 24 computers or laptops. All computers or laptops must have: i. Internet connectivity and access; ii. The software identified in section 9.11 of the Statement of Work; d) A server and network infrastructure to support the training objectives; and e) Must have a photocopier.	The Bidder must provide a detailed description of the classroom or computer laboratory to demonstrate it meets the requirements.

Number	Mandatory Technical (MT) Criterion	Instructions to Bidders
MT4	The Bidder’s training site and facility must include one office space that meets the following requirements: a) Two single occupancy offices each with a desk, a chair, an individual telephone and access to a data communication line (e.g. internet, local area network); and b) One private room with one desk and two chairs.	The Bidder must provide a detailed description of the office space to demonstrate it meets the requirements.
MT5	The Bidder’s training site and facility must include one dining area that meets the following requirements: a) Must be separate from the classroom or computer laboratory; b) Must seat up to 24 students in order for the students to consume their meal as a group; c) Must have a fridge; and d) Must have a microwave.	The Bidder must provide a detailed description of the dining area to demonstrate it meets the requirements.
MT6	The Bidder’s cyber operator training program must be recognized by a Canadian provincially-recognized educational authority.	The Bidder must provide: a) Legal documents (e.g. certificate of accreditation, charter); b) Student assessment polices, grading procedures and grading rubrics; c) Tutorial assistance policies and procedures (draft is acceptable); d) Any guidelines, rules, and regulations that are provided to students including the course change policy; and e) A blank, unsigned copy of the diploma that would be provided to the student upon completion of the program.
MT7	The Bidder must provide a human resources plan to recruit and replace qualified resources to provide the services in the Statement of Work.	The Bidder must provide: a) The screening and selection process of faculty qualified professors and instructors/teaching assistants; b) The strategy and process to accommodate the student to professor/instructor/teaching assistant ratio of 12:1; and c) The strategy and process used to replace qualified resources in a timely manner that avoids disruption.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by bidders to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period. The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

Bidders must complete their certifications required under Part 5 by using the attached PDF fillable form, Attachment 2 to Part 3 - Certifications.pdf

PART 6 – SECURITY REQUIREMENTS

6.1 Security Requirement

6.1.1 Before award of a contract, the following conditions must be met:

a) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses; and

b) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites.

If the information is not provided in or with the bid, the Contracting Authority will so inform the Bidder and provide the Bidder with a time frame within which to meet the requirement. Failure to comply with the request of the Contracting Authority and meet the requirement within that time period will render the bid non-responsive.

6.1.2 Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

6.1.3 For additional information on security requirements, Bidders should refer to the Contract Security Program (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) of PWGSC.

PART 7 – RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

7.1 Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work in Annex A.

7.2 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions (SACC) Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada (PWGSC).

7.2.1 General Conditions

2035 (2018-06-21), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

Section 20 of 2035 General Conditions - Higher Complexity - Services, is deleted in its entirety.

7.2.2 Supplemental General Conditions

4006 (2010-08-16), Contractor to Own Intellectual Property Rights in Foreground Information, apply to and form part of the Contract.

7.2.3 Non-Disclosure Agreement

The Contractor must obtain from its employee(s) or subcontractor(s) the completed and signed non-disclosure agreement, attached at Annex C, and provide it to the Technical Authority before they are given access to information by or on behalf of Canada in connection with the Work.

7.3 Security Requirement

7.3.1 The following security requirement (security requirement check list (SRCL) and related clauses provided by the Contract Security Program (CSP) (https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) apply and form part of the Contract:

a) The Contractor must, at all times during the performance of the Contract, hold a valid Designated Organization Screening (DOS), issued by the CSP of the Industrial Security Sector (ISS) of PWGSC;

b) The Contractor's personnel requiring access to PROTECTED information, assets or sensitive work site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CSP/ISS/PWGSC;

c) The Contractor MUST NOT remove any PROTECTED information or assets from the identified work site(s), and the Contractor must ensure that its personnel are made aware of and comply with this restriction;

d) Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the CSP/ISS/PWGSC; and

e) The Contractor must comply with the provisions of the:

i. SRCL, attached at Annex B; and
ii. Industrial Security Manual (Latest Edition).

7.4 Term of Contract

7.4.1 Period of the Contract

The period of the Contract is from date of Contract to December 31, 2021 inclusive.

7.4.2 Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to four additional 17-month period(s) under the same conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least 90 calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

7.4.3 Termination on 120 Days Notice

Canada reserves the right to terminate the Contract at any time in whole or in part by giving 120 calendar days written notice to the Contractor.

In the event of such termination, Canada will only pay for costs incurred for services rendered and accepted by Canada up to the date of the termination. Despite any other provision of the Contract, there will be no other costs that will be paid to the Contractor as a result of the termination.

7.5 Authorities

7.5.1 Contracting Authority

The Contracting Authority for the Contract is:

Diane Reynolds
Supply Specialist
Public Works and Government Services Canada
Acquisitions Branch
Professional Services Procurement Directorate
Terrasses de la Chaudière
10 Wellington, 5th Floor
Gatineau, Quebec, K1A OS5
Telephone: 613-858-8571
Facsimile: 819-956-2675
Email: Diane.Reynolds@tpsgc-pwgsc.gc.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

7.5.2 Technical Authority

The Technical Authority for the Contract is:

To be identified at time of Contract award

The Technical Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

7.5.3 Contractor's Representative

To be identified at time of Contract award

7.6 Payment

7.6.1 Basis of Payment

7.6.1.1 Firm Lot Price

a) For the Work described in the Statement of Work in Annex A with the exception of additional students or a new or replacement textbook, the Contractor will be paid a firm lot price indicated below for a class size of 1-12 students. The firm lot price includes all of the costs associated with the delivery of the training, Customs duties are included and Applicable Taxes are extra.

Contract Period	Option Period 1	Option Period 2	Option Period 3	Option Period 4
$*To be identified at time of Contract award*	$*To be identified at time of Contract award*	$*To be identified at time of Contract award*	$*To be identified at time of Contract award*	$*To be identified at time of Contract award*

b) Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

7.6.1.2 Firm Unit Price

a) The Contractor will be paid a firm unit price per student per semester indicated below for each additional student up to a maximum class size of 24 students. The firm unit price per student per semester includes all of the costs associated with the delivery of the training for each semester for each additional student, Customs duties are included and Applicable Taxes are extra.

Contract Period	Option Period 1	Option Period 2	Option Period 3	Option Period 4
$*To be identified at time of Contract award*	$*To be identified at time of Contract award*	$*To be identified at time of Contract award*	$*To be identified at time of Contract award*	$*To be identified at time of Contract award*

b) Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

7.6.1.3 Administrative Fee

For a new or replacement textbook, the Contractor will be reimbursed at cost plus the administrative fee. The administrative fee includes all of the costs associated with providing the textbook to the client, Customs duties are included and Applicable Taxes are extra.

Administrative Fee: *To be identified at time of Contract award* %

7.6.2 Canada's Total Liability

a) Canada's total liability to the Contractor under the Contract must not exceed $*To be identified at time of Contract award.* Customs duties are included and Applicable Taxes are extra;

b) No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications or interpretations of the Work, will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Contracting Authority. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

i. When it is 75 percent committed, or
ii. Four months before the Contract expiry date, or
iii. As soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

Whichever comes first.

c) If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

7.6.3 Method of Payment

7.6.3.1 Milestone Payments

a) For the Work described in the Statement of Work in Annex A with the exception of additional students or a new or replacement textbook, Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Contract and the payment provisions of the Contract if:

i. An accurate and complete claim for payment using PWGSC-TPSGC 1111 (https://www.tpsgc-pwgsc.gc.ca/app-acq/forms/1111-eng.html), Claim for Progress Payment, and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
ii. All the certificates appearing on form PWGSC-TPSGC 1111 have been signed by the respective authorized representatives; and
iii. All work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada; and

b) The schedule of milestones for which payments will be made in accordance with the Contract is as follows:

Milestone Number	Description	Firm Amount
1	Completion of Semester 1	40% of firm lot price
2	Completion of Semester 2	20% of firm lot price
3	Completion of Semester 3	20% of firm lot price
4	Completion of Semester 4	20% of firm lot price

7.6.3.2 Single Payment

a) For each additional student, Canada will pay the Contractor upon completion of each semester in accordance with the payment provisions of the Contract if:

   i. An accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
   ii. All such documents have been verified by Canada;
   iii. The Work delivered has been accepted by Canada;

b) For a new or replacement textbook, Canada will pay the Contractor upon completion and delivery of the Work in accordance with the payment provisions of the Contract if:

   i. An accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
   ii. All such documents have been verified by Canada;
   iii. The Work delivered has been accepted by Canada;

7.6.4 SACC Manual Clauses

A9117C (2007-11-30), T1204 - Direct Request by Customer Department

7.6.5 Discretionary Audit

C0705C (2010-01-11), Discretionary Audit

7.6.6 Electronic Payment of Invoices – Contract (if applicable)

The Contractor accepts to be paid using any of the following Electronic Payment Instruments:

a) Visa Acquisition Card;
b) MasterCard Acquisition Card;
c) Direct Deposit (Domestic and International);
d) Electronic Data Interchange (EDI);
e) Wire Transfer (International Only);
f) Large Value Transfer System (LVTS) (Over $25M).

7.7 Invoicing Instructions

a) The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions. Invoices cannot be submitted until all work identified in the invoice is completed; and

b) Invoices must be distributed as follows:

   i. One soft copy must be forwarded to the following email address for certification and payment: STG-CFSTG-J3-Fin@forces.gc.ca. The contract number and Technical Authority must be entered in the subject line of the email; and
   ii. One soft copy must be forwarded by e-mail to the Contracting Authority identified under the section entitled "Authorities" of the Contract at the following email address: tpsgc.facturation-zh.zh-invoicing.pwgsc@tpsgc-pwgsc.gc.ca. The contract number and Contracting Authority must be entered in the subject line of the email.

7.8 Certifications and Additional Information

7.8.1 Compliance

Unless specified otherwise, the continuous compliance with the certifications provided by the Contractor in its bid or precedent to contract award, and the ongoing cooperation in providing additional information are conditions of the Contract and failure to comply will constitute the Contractor in default. Certifications are subject to verification by Canada during the entire period of the Contract.

7.8.2 Federal Contractors Program for Employment Equity - Default by the Contractor

The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC)-Labour, the AIEE must remain valid during the entire period of the Contract. If the AIEE becomes invalid, the name of the Contractor will be added to the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid List" available at the bottom of the page of the Employment and Social Development Canada (ESDC) - Labour's web site (https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html#s4). The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

7.9 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in the province of Ontario, Canada.

7.10 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list.

a) The Articles of Agreement;
b) The supplemental general conditions 4006 (2010-08-16), Contractor to Own Intellectual Property Rights in Foreground Information;
c) The general conditions 2035 (2018-06-21), General Conditions - Higher Complexity - Services;
d) Annex A, Statement of Work;
e) Annex B, SRCL;
f) Annex C, Non-disclosure Agreement; and
g) The Contractor's bid dated *To be identified at time of Contract award*.

7.11 Defence Contract

A9006C (2012-07-16), Defence Contract

7.12 Foreign Nationals

A2000C (2006-06-16), Foreign Nationals (Canadian Contractor) or
A2001C (2006-06-16), Foreign Nationals (Foreign Contractor)

7.13 Insurance

G1005C (2016-01-28), Insurance

7.14 Proactive Disclosure of Contracts with Former Public Servants (if applicable)

By providing information on its status, with respect to being a former public servant in receipt of a *Public Service Superannuation Act* (PSSA) (https://laws-lois.justice.gc.ca/eng/acts/P-36/FullText.html) pension, the Contractor has agreed that this information will be reported on departmental websites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 (https://www.canada.ca/en/treasury-board-secretariat/services/policy-notice/2012-2.html) of the Treasury Board Secretariat of Canada.

ANNEX A

STATEMENT OF WORK

1. TITLE

Cyber Operator Training

2. OBJECTIVE

The objective of this Statement of Work is for a Contractor to deliver a training program that will satisfy the occupation performance requirements for the Canadian Armed Forces (CAF) Cyber Operator (CYBER OP) Private Rank Qualification (Pte RQ) commencing in August 2020.

3. BACKGROUND

3.1 In 2010, the Vice Chief of the Defence Staff endorsed the Cyber Task Force with a mandate to rapidly institutionalize and operationalize a new CAF cyber capability. This mandate was subsequently assumed by the Director Cyber Operations Force Development (FD). Integral to this mandate is the need to develop an institutionalized, specialized and dedicated workforce to conduct cyber operations, which was further endorsed by Canada's Defence Policy – Strong, Secure, Engaged (SSE) in June 2017. SSE provided the Department of National Defence (DND) and the CAF with a broad range of initiatives that will continue to evolve Canada's warfighting capabilities, including several directly related to warfare in the cyber domain such as growing and enhancing the CAF Cyber Force by creating a new CYBER OP occupation. This new occupation was created and endorsed in 2017.

3.2 CYBER OPs are members of the Communications and Electronics Branch of the CAF. They conduct defensive cyber operations, and when required and where feasible, active cyber operations. They liaise and work collaboratively with other government departments and agencies, as well as with Canada's allies, to enhance the DND's and the CAF's ability to provide a secure cyber environment. They monitor CAF communication networks to detect and respond to unauthorized network access attempts and provide cyber support to meet the operational requirements of the Navy, Army, Air Force, and joint enablers. A CYBER OP has the following responsibilities:

a. Collect, process and analyze network data;
b. Identify network vulnerabilities;
c. Manage a computer network environment;
d. Conduct defensive and active cyber operations;
e. Apply security and communications knowledge in the field of information technology; and
f. Use and maintain classified and unclassified records and publications.

3.3 A guiding principle underpinning the development of this new occupation is that cyber specialists require considerable training and education (T&E) to become effective. A significant component of this T&E is common to that required by non-military cyber specialists, with additional aspects being unique to DND/CAF networks and systems. The challenges associated with providing CYBER OPs with the T&E they require were highlighted during initial studies and persist today, including:

a. T&E specific to the CYBER OP occupation does not readily exist within the CAF;
b. The CAF currently does not have a full-time cadre of instructors with the level of education, training, and CAF-specific experience required to develop, deliver and maintain the full range of entry-level CYBER OP T&E; and
c. The infrastructure requirements associated with conducting all facets of the new CYBER OP training program exceed the capacity of the Canadian Forces School of Communications and Electronics (CFSCE).

3.4 Within the CAF, cyber operator training has been assigned to the following organizations:

a. CFSCE is responsible for training students and the management of individual students. The Technical Authority may designate a unit other than CFSCE at its discretion and will notify the Contractor in writing by email;

b. Military Personnel Generation Training Group (MPGTG) is responsible for the management and administration of training programs. The Technical Authority may designate a unit other than MPGTG at its discretion and will notify the Contractor in writing by email; and

c. Director General Cyber Force Development (DG Cyber FD) is the Technical Authority and the main point of contact for the Contractor. DG Cyber FD is responsible for advising CFSCE and MPGTG on all occupation and technical matters for the CYBER OP occupation.

3.5 The CYBER OP Pte RQ qualification standard and plan (QSP) was developed in 2017 with the challenges outlined in section 3.3. The performance objectives (POs) included in the QSP detail what the student must be capable of achieving on completion of the Pte RQ qualification, to include:

a. PO 001 – Maintaining network situational awareness;
b. PO 002 – Responding to a cyber event;
c. PO 003 – Producing a technical report;
d. PO 004 – Preparing an analysis environment;
e. PO 005 – Developing software tools;
f. PO 006 – Implementing cyber security orders and directives; and
g. PO 007 – Defending the DND/CAF cyber domain.

3.6 Non-military specific tasks common to the cyber defence and security workforce were deliberately grouped into POs 001 to 005, and tasks specific to DND/CAF were grouped into POs 006 and 007. This was done to facilitate delivery of POs 001 to 005 by the Contractor.

4. ACRONYMS AND APPLICABLE DOCUMENTS

4.1 Acronyms

The following acronyms are used in this Statement of Work:

CAF	Canadian Armed Forces
CFSCE	Canadian Forces School of Communications and Electronics
CYBER OP	Cyber Operator
DG	Director General
DND	Department of National Defence
FD	Force Development
IT	Information Technology
LIMDIS	Limited Distribution
MPGTG	Military Personnel Generation Training Group
NCR	National Capital Region
PO	Performance Objective
Pte RQ	Private Rank Qualification
QSP	Qualification Standard and Plan
SCCM	System Centre Configuration Management
SSE	Strong, Secure, Engaged
T&E	Training and Education

4.2 Applicable Documents

The following documents including any amendments, form part of this Statement of Work to the extent specified herein and are supportive of the Statement of Work:

a. Access to Information Act (https://laws.justice.gc.ca/eng/acts/A-1/index.html);
b. Accessible Canada Act (https://www.parl.ca/DocumentViewer/en/42-1/bill/C-81/third-reading);
c. Official Languages Act (https://laws.justice.gc.ca/eng/acts/O-3.01/page-9.html);
d. Privacy Act (https://laws.justice.gc.ca/eng/acts/P-21/index.html);
e. Treasury Board Contracting Policy (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14494);
f. Treasury Board Secretariat Guidelines to Ensuring Accessibility via Public Procurement (http://www.gcpedia.gc.ca/gcwiki/images/5/57/Accessibility_in_Procurement_Guidance_-_April_2019-V1%28EN%29.pdf);
g. Defence Learning Network Content Development Guide; https://www.canada.ca/en/department-national-defence/services/benefits-military/education-training/professional-development/defence-learning-network.html
h. Manual of Individual Training and Education, A-P9-050-000/PT001 publication series http://cda.mil.ca/pub/lib-bib/cfites-eng.asp
i. DAOD 5023-0, Universality of Service (https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/5000-series/5023/5023-0-universality-of-service.html);
j. DAOD 5039-0, Official Languages (https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/5000-series/5039/5039-0-official-languages.html);
k. DAOD 5039-4, Translation of Texts and Acquisition of Bilingual Documentation (https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/5000-series/5039/5039-4-translation-of-texts-and-acquisition-of-bilingual-documentation.html);
l. DAOD 5516-5, Learning Disability Accommodation during Recruiting, Training and Education (https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/5000-series/5516/5516-5-learning-disability-accommodation-during-recruiting-training-and-education.html);
m. National Defence Security Orders and Directives Chapter 6: Security Information (http://national.mil.ca/en/health-safety-security/security-policies-ndsod.page);
n. Appendix 1, Cyber Operator Private Rank Qualification;
o. Appendix 2, Performance Objectives and Enabling Objectives; and
p. Appendix 3, List of References.

5. SCOPE

5.1 The CYBER OP occupation requires an annual intake of at least 12 and up to 24 trained students per year in order to build the occupation and meet operational requirements. This contract is an initial two year contract with one program session to deliver a pilot CYBER OP course and four optional 17-month program sessions.

5.2 It is anticipated that the time required to deliver POs 001 to 005 will be approximately 15 months or four 15-week semesters. The required program sessions are as follows:

a. Contract Period: August 2020 – December 2021;
b. Option Period 1: August 2021 – December 2022;
c. Option Period 2: August 2022 – December 2023;
d. Option Period 3: August 2023 – December 2024;
e. Option Period 4: August 2024 – December 2025.

6. TRAINING REQUIREMENTS

6.1 The Contractor must demonstrate that their program is accredited by a Provincial government's higher education governing and accreditation organization in the field of cybersecurity analysis (civilian related careers) or cybersecurity operations[1]. The Contractor must:

a. Develop a training program that will satisfy the CYBER OP Pte RQ POs 001 to 005 occupational performance requirements identified in Appendix 1;

b. Have the course material (excluding lesson plans) assessed and approved by the CAF Accreditation, Certification, Equivalency (CAF-ACE) program office (http://www.caface-rfacace.forces.gc.ca/en/index); it can take up to three weeks for CAF-ACE to assess and approve the course material. In order to login, the Contractor must register to obtain an account from CAF-ACE. If the Contractor has any problems or issues, the Contractor must contact the CAF-ACE System Administrator;

c. Maintain the currency of a training program including all course material (lesson plans, textbooks, assessments and workbooks etc.) that will satisfy the CYBER OP Pte RQ POs 001 to 005 occupational performance requirements identified in Appendix 1 over the duration of the contract. Currency for this contract is the periodic review of all course material every two years, or the course material must be less than two years old to reflect best modern practices of cybersecurity; and

d. Submit all amendments to the course materials (excluding lesson plans) for assessment and approval by the CAF-ACE program office.

6.2 The Contractor must deliver 37.5 hours of teaching per week and ensure that the established hours of the standard training day are respected according to the agreed schedule. The weekly training schedule must include:

a. 27.5 hours of academics (programmed learning time);
b. Five one-hour lunch periods;
c. Three one-hour periods of time for physical fitness training (either at the start or the end of the training day); and
d. One two-hour period of personal administration time.

6.3 The Contractor must be recognized as a post-secondary diploma/degree granting institution by a Canadian provincially-recognized educational authority. The Contractor must maintain this recognition throughout the duration of the contract.

6.4 Upon completion of the CYBER OP Pte RQ training program, the Contractor must provide students with a provincially-recognized diploma in Cybersecurity Analysis or Network Defence Analysis.

6.5 The Contractor must provide a training site and facility which is within the geographical boundaries of Kingston, Ontario, or the National Capital Region (NCR).

6.6 Canada strives to ensure that the goods and services it procures are inclusive by design and accessible by default, in accordance with the *Accessible Canada Act*, its associated regulations and standards, and *Treasury Board Contracting Policy*. DAOD 5516-5, Learning Disability Accommodation during Recruiting, Training and Education specifies the learning disability accommodation for training and education if a student requires such accommodation.

[1] Cyber Operations include Defensive Cyber Operations, Offensive Cyber Operations and Support Cyber Operations in accordance with Canadian Armed Forces Joint Doctrine Note 2017-02.

7. TRAINING METHODOLOGY

7.1 The Contractor must deliver training and student evaluations that must focus on the knowledge and skills required to achieve POs 001 to 005 detailed in Appendix 1.

7.2 The Contractor must incorporate practical work sessions during the training to develop student skills for the commonly used network analyst operating systems and software applications in the public/private sectors and that are also common to CAF CYBER OPs. An example of the type of operating systems is Linux and Windows workstations and servers. Examples of user software include Apache, PHP, MySQL, Adobe, Microsoft Office and Wireshark. In addition to the operating systems listed above, the Contractor must also incorporate scripting software such as Python and Ruby, malware analysis tools such as Cuckoo Sandbox, and configuration software such as System Centre Configuration Management (SCCM) into the course material as detailed by CFSCE.

7.3 The Contractor must ensure all exams, materials and training are available in both of Canada's Official Languages and provided to students in the language of choice of the student.

7.4 The Contractor must deliver training consistent with the provincial community college practices and standards as determined by the provincially-recognized education approval authority (e.g. Counsel of Ontario Universities).

7.5 The Contractor must enforce provincially approved community college student academic assessment procedures, standards, and practices. The Contractor must notify the Technical Authority of any student at risk of not being able to progress in the program or succeed in/complete the program as soon as practicable but prior to course completion and prior to removal from the program. The Technical Authority will review the student’s academic situation and provide any necessary disposition to the Contractor by email. The Technical Authority may direct additional student assessments (e.g. request a second opinion and/or give the student another chance).

7.6 CFSCE may monitor any instructional and assessment sessions upon written notice to the Contractor. Feedback related to the monitoring of the sessions will be provided to the Contractor and the Technical Authority by email.

7.7 The Contractor must provide tutorial assistance as necessary and in accordance with the procedures agreed to with CFSCE in writing. These arrangements must be provided to CFSCE no less than 30 working days prior to the start of the program. The Contractor or CFSCE may modify these arrangements as long as it is in consultation with each other and with each other’s written consent by email.

7.8 The Contractor must provide a copy of all graded student material upon request of the Technical Authority. Academically sensitive materials must be protected in accordance with A2– A4 in Appendix 3.

7.9 The Contractor must provide the Technical Authority with a final transcript of each student within 30 working days of a student completing or departing the training program. Student transcripts must be protected in accordance with A2 – A4 in Appendix 3.

8. TRAINING SCHEDULE

8.1 The Contractor must provide a soft copy of the preliminary training schedule in Microsoft Word to the Technical Authority within 10 working days of Contract award. The Contractor must work with the Technical Authority to refine the proposed schedule, in order to define the course duration and the training day to satisfy the requirements of the POs and the needs of the CAF. The final schedule must be approved by the Technical Authority and published by the Contractor a minimum of 30 working days in advance of the start of training delivery.

8.2 The preliminary training schedule must clearly identify all practical and theory learning sessions. For initial planning purposes, the daily schedule should commence at 0800 hours and end at 1600 hours.

8.3 The CYBER OP training program must be completed within a 15-month period with no more than four semesters focused on academics. The semesters are defined as follows:

a. Semester One – September to December;
b. Semester Two – January to April;
c. Semester Three – May to July; and
d. Semester Four – September to December.

9. TRAINING SITE AND ADDITIONAL SUPPORT

9.1 The Contractor must provide a training site and facilities consistent with Ontario community college practices and standards for this type of learning program. The classroom or computer laboratory must accommodate all students, furniture, materials as well as all necessary information technology (IT) hardware and common software required to achieve POs 001 to 005.

9.2 The Contractor must provide access to the training site and facility as necessary for additional student support and student practice (supervised and/or unsupervised) outside of the standard training day.

9.3 The Contractor must develop and provide up to date course materials in soft copy and provide any textbooks in hard copy necessary to satisfy POs 001 to 005.

9.4 The Contractor must provide a single hard copy of any textbooks or instructional materials to each student and at least one hard copy to CFSCE. Textbooks purchased by DND will remain the property of DND.

9.5 The Contractor must provide any consumable instructional materials. This includes, but is not limited to, workbooks and handouts. This does not include individual student consumable learning supplies (i.e. materials that may be different for each student used by them to facilitate their learning; e.g. paper, pens, pencils, stationary, etc.).

9.6 The Contractor must provide access to the classroom or computer laboratory to all students with peripheral cyber operations hardware and an information support network configuration.

9.7 The Contractor must provide IT equipment, support resources and network that provides internet access, individual student email accounts with 1 GB (minimum) of mail storage, a web space account with 5 GB (minimum) disk space allocation and remote access to the Contractor’s student network. The classroom or computer laboratory must include all necessary IT hardware to achieve POs 001 to 005 of the CYBER OP training requirements and must include suitable networked backup systems to ensure the integrity of data and student work.

9.8 All hardware must be life-cycled on a maximum four-year plan at cost to the Contractor.

9.9 Any leased IT equipment (e.g. laptops, hard drives, etc.) must be scrubbed upon completion of the training program and/or return to a third party according to DND IT security policies A2– A4 in Appendix 3.

9.10 The Contractor must provide a server and network infrastructure to support the training objectives that comply with the Canadian requirements for processing and storing CAF member's personal information as described in the National Defence Security Orders and Directives, Chapter 6 Security of Information. The Contractor and/or the Contractor's resources requiring access to personal information must complete and sign the non-disclosure agreement.

9.11 The Contractor must provide the following suite of software for the classroom or computer laboratory:

a. Industry standard operating systems (LINUX/Windows client and server);
b. Industry standard user software (Apache, PHP, MySQL, Adobe, Microsoft Office and Wireshark);
c. Industry standard scripting software (Python and Ruby);
d. Industry standard malware analysis tools (Cuckoo, Sandbox and InetSim), and
e. Configuration software (SCCM).

9.12 The implementation of upgrades to software must be coordinated by the Contractor. The Contractor must determine the optimum timeframe for upgrades in order to minimize disruption to classes and to coordinate the lesson plans amendments to the available teaching material related to the latest version of the software. A software upgrade is where changes have been made to an existing software package and the release will follow the same version identification.

9.13 The Contractor must provide proof of software and/or hardware agreements and/or licenses to the Technical Authority by email within 60 calendar days prior to the training program start date.

9.14 The Contractor must provide office space suitable for CFSCE personnel visits, including single occupancy offices for two CFSCE personnel, plus one private room for counselling or interviews. The offices must be furnished consistent with the existing Ontario community college practices and standards for instructional staff. The offices must include a minimum of two individual telephone and access to data communication lines. Access to these facilities must be provided as necessary for additional student support and practice outside of the standard training day.

9.15 The Contractor must provide refrigeration for the safe storage of students' meals throughout the day. This capability must be able to store the meals of up to 24 students for two meals per day.

9.16 The Contractor must provide a microwave for the safe reheating of students' meals by the students.

9.17 The Contractor must provide a dining area (separate from the classroom and/or computer laboratory) for students to consume their meals as a group. The size of the area must be able to accommodate all students expected to eat at a single period (i.e. if only one lunch period, all students may be expected to eat at the same time).

9.18 The Contractor must provide a photocopier (including but not limited to various size paper, toner, ink cartridges), for the use by the students and at no cost to the students or Canada.

10. RESOURCE REQUIREMENTS

10.1 Resources

The Contractor must provide the following resources to deliver and fully support the requirements of the CYBER OP training program, including:

a. A Contract Supervisor for contract management and related issues;

b. A Program Coordinator for program delivery and supervision of contracted resources;

c. Faculty qualified professors, at a student to professor ratio of 12:1;

d. Instructors (or Teaching Assistants), at a student to instructor/teaching assistant ratio of 12:1;

e. IT technician(s) to ensure the serviceability of the IT support systems and technical support for students. Training time lost due to technical failures, IT system maintenance or any unforeseen circumstance must be provided by the Contractor at no additional cost to Canada in order to ensure the hours of student instruction per week is delivered as per section 6.2; and

f. Other resources as deemed necessary and appropriate to support other aspects of this contract (e.g. cleaning resources to maintain the hygiene of the dining areas).

10.2 Minimum Mandatory Qualifications

Resources must meet the minimum mandatory qualifications for the respective resource category:

a. Faculty qualified professors must have:
   i. A minimum of four years' experience; and
   ii. A Master's Degree in but not limited to Computer Science, or Computer Programming, Information Science or Computer Engineering from a recognized Canadian university, college or high school, or the equivalent as established by a recognized Canadian academic credentials assessment service (https://www.cicic.ca/2/home.canada), if obtained outside Canada;

b. Instructors or Teaching Assistants must have:
   i. A minimum of three years' experience instructing in the content area related to the POs and associated EOs in Appendix 1; and
   ii. A Bachelor's Degree in but not limited to Computer Science, or Computer Programming, Information Science or Computer Engineering from a recognized Canadian university, college or high school, or the equivalent as established by a recognized Canadian academic credentials assessment service (https://www.cicic.ca/2/home.canada), if obtained outside Canada.

11. LANGUAGE REQUIREMENTS

11.1 The Contractor and the Contractor's resources must be fluent (listening, speaking, reading and writing) in both or either of Canada's Official Languages (English or French); fluent is equivalent to a Level 8 of the Canadian Language Benchmarks for English and of the Niveaux de compétence linguistique canadiens for French: https://www.language.ca/overview-of-clb-and-nclc-competency-levels/.

11.2 The Contractor must have an established quality assurance process for English and French correspondence and deliverables, including proof reading all correspondence and deliverables.

11.3 Canada reserves the right to request the Contractor to evaluate the language proficiency of any of its resources throughout the period of the Contract, at no additional cost to Canada, through one of the approved language test by Immigration, Refugees and Citizenship Canada. Should the evaluation of a Contractor's resource determines that the resource does not meet the language requirement; the Contractor must immediately replace the resource at no additional cost to Canada.

12. MEETINGS

The Contractor and the Contractor's resources will not be reimbursed for any costs incurred by the Contractor and the Contractor's resources for meetings.

12.1 Kick off Meeting

a. A kick off meeting must be held within five working days from the contract award date. The kick-off meeting must be held within the NCR or by conference call. The exact time and location of the kick off meeting will be mutually agreed upon between the Contractor and the Technical Authority;

b. The purpose of the kick-off meeting is to:
   i. Review the contractual requirements; and
   ii. Review and clarify, if required, the respective roles and responsibilities of CFSCE, MPGTG, the Technical Authority and the Contractor to ensure common understanding.

12.2 Monthly Meetings

a. The Contractor's Contract Supervisor and Program Coordinator must participate in training steering meetings in Kingston or by conference call with CFSCE to review the status of the course and students’ progress. These training steering meetings will occur no more than once per calendar month, unless agreed upon by the Contractor and the TE. The date and time of the monthly will be mutually agreed upon between the Contractor and the Technical Authority; and

b. The Contractor is responsible for the preparation of agendas and records of decisions for all meetings. Agendas must be made available five working days before meetings and the draft record of decisions for meetings must be delivered to the Technical Authority for review within three working days after the meeting.

13. LIMITATIONS AND CONSTRAINTS

13.1 Decisions concerning revision or definition of policy, budgets, as well as contractual obligations and requirements, are excluded from the Contractor’s services. Contractor’s resource must limit themselves to provide comments and recommendations only to the Technical Authority on these issues.

13.2 Contractor’s resource providing the services will be independent of direct control by servants of Canada and are not in any respect employees or servants of Canada.

13.3 During the performance of the Contract, the Contractor or their resource must not direct any departmental organizations, or any personnel of any third parties with whom Canada has or intends to contract, to perform any action.

13.4 At all times during the provision of the required services, the Contractor’s resource are not to have access to any proprietary information including but not limited to financial information (including unit prices or rates) or technical information concerning any third parties with whom Canada has contracted or intends to contract, other than information that is in the public domain, (e.g. total value of contract(s) awarded). Proprietary information may be provided to Contractor’s resource in the performance of the services if the non-disclosure agreement is completed and signed by the Contractor’s resource.

13.5 All drawings, software codes, reports, data, documents, or materials, provided to the Contractor by Canada or produced by the Contractor’s resource in providing services under the Contract, must be used solely in support of this requirement. The Contractor must safeguard the preceding information and materials from unauthorized use and will not release them to any third party, person or organization external to DND without the express written permission of the respective organization (as identified under section 3.4) or Technical Authority. Such information and material must be returned to the respective organization or Technical Authority upon completion of the services or when requested by the Technical Authority.

13.6 All correspondence, either initiated by the Contractor's resource or by any section of DND, must be submitted to the respective organization (as identified under section 3.4) or Technical Authority. Correspondence is defined as records of conversation or decisions as well as any written correspondence in any format.

13.7 The Technical Authority or respective organization will have access at all times to the Work and to the facility where any part of the Work is being performed.

13.8 The Contractor must ensure that their resource does not use Government of Canada or DND designations, logos or insignia on any business cards, cubicle/office signs or written/electronic correspondence that in any manner lead others to perceive Contractor's resource as being an employee of Canada.

Appendix 1

Cyber Operator Private Rank Qualification

List of Abbreviations

CYBER OP	Cyber Operator
Pte RQ	Private Rank Qualification
PO	Performance Objective
EO	Enabling Objective
DND	Department of National Defence
CAF	Canadian Armed Forces
IT	Information Technology
IDS	Intrusion Detection System
IPS	Intrusion Protection System
IP	Internet Protocol
OS	Operating System
CIO	Chief Information Officer
ISSO	Information System Security Officer
CVE	Common Vulnerabilities and Exposures
IAW	In accordance with
Ref	Reference
PCAP	Packet Capture
DNS	Domain Name Server
DHCP	Dynamic Host Control Protocol
IIS	Information Internet Server
LAMP	Linux Apache MySQL and PHP

Outline of the training requirement: Cyber Operators (CYBER OP) conduct network and computer defensive operations and liaise with Canada's allies in order to enhance Department of National Defence (DND) and Canadian Armed Forces (CAF) abilities to provide a secure cyber environment. They monitor CAF communication networks to detect and respond to unauthorized network access attempts and provide cyber support to meet the operational requirements of the Navy, Army and Air Force. Offensive cyber activities and tasks, which include disrupting adversaries' actions in the cyber domain, also fall within their scope of work. The aim of this training is to prepare CYBER OPs to perform the entry level job of "CYBER OP". This job is performed in an operations centre in support of the Sea, Land and Air elements. The primary responsibility is to identify indicators of compromise through the analysis of DND/CAF networks. The main tasks include collecting, examining, and analyzing cyber alerts, and creating technical reports on cyber alerts.

Overview of the training strategy: This is a new training requirement (i.e., no CAF version of the course is currently being delivered). The training program is designed to have two main components:

Module 1 – Performance Objectives (POs) 001 to 005 (the focus of this Training Requirement, listed below): To be delivered by the Contractor.

Module 2 – POs 006 and 007 (not included in this Training Requirement): To be delivered by a CAF training establishment. The intent of these POs is to prepare the CYBER OP to apply the generic skills and network monitoring techniques developed in POs 001 to 005 in a CAF context.

POs and associated Enabling Objectives (EOs):

PO 001 – Maintain Network Situational Awareness: The intent of this PO is to prepare the CYBER OP to conduct activities to establish and maintain situational awareness of the structure, composition, traffic patterns and security posture of a network. This is achieved through use of automated tools, manual methods and various levels of analysis of the raw data. In enumerating the network, building the network map and benchmarking network traffic, the CYBER OP must be well-versed in network technologies, architecture, devices and communications. In conducting vulnerability assessments, they must be knowledgeable of common vulnerabilities, threats and attack vectors in order to analyze and advise on mitigations. Additionally, they must have a general understanding of various operating systems (PC and server), virtualization and various other areas of networking and information technology (IT), in order to identify and assess if any anomalies were detected during a network scan or in packet captures.

EO 001.01 – Enumerate a network and system
EO 001.02 – Develop a logical network map
EO 001.03 – Identify network and system vulnerabilities
EO 001.04 – Characterize network traffic to establish normal patterns

PO 002 – Respond to a Cyber Event: The intent of this PO is to prepare the CYBER OP to investigate an event using data collected from a variety of cyber defence tools (e.g., intrusion detection system (IDS) alerts, firewalls, network traffic logs). The analyst will go through the steps to analyze the event that occurred within their environment for the purposes of mitigating threats through internal reporting.

EO 002.01 – Detect threat activity
EO 002.02 – Investigate cyber events
EO 002.03 – Produce internal reports
EO 002.04 – Safeguard cyber forensic evidence

PO 003 – Produce a Technical Report: The intent of this PO is to prepare the CYBER OP to produce a technical report using any and all raw available data, completed analyses and other relevant reports and cyber injects.

EO 003.01 – Collate relevant data in order to initiate a technical report
EO 003.02 – Draft a technical report
EO 003.03 – Produce a technical report for verbal or written dissemination

PO 004 – Prepare an Analysis Environment: The intent of this PO is to prepare the CYBER OP to configure hardware and software. The CYBER OP will be capable of installing, maintaining and removing cyber defence hardware and software and creating and removing intrusion detection system (IDS)/intrusion protection system (IPS) rules. The setup and configuration of various security devices in a small network environment will prepare the CYBER OP for custom applications and unique deployment requirements. In support of CAF forensics and malware analysis, the CYBER OP requires a hands-on understanding of virtualized platforms.

EO 004.01 – Install required hardware
EO 004.02 – Configure physical network security devices
EO 004.03 – Prepare and set up virtual operating systems
EO 004.04 – Configure software
EO 004.05 – Troubleshoot toolset hardware deficiencies
EO 004.06 – Troubleshoot toolset software deficiencies
EO 004.07 – Set up and maintain network sensors
EO 004.08 – Remove required software and hardware

PO 005 – Develop Software Tools: The intent of this PO is to prepare the CYBER OP to design, build, test, and maintain custom software tools. They will be able to determine deficiencies in existing tools in order to design and build tools to resolve those deficiencies. They will have competency in scripting and be able to write small programs for the purpose of building custom tools. This PO is not intended to make CYBER OPs expert at software development, but will give them basic scripting skills and provide foundational skills for other POs as well as future specialized job-based training.

EO 005.01 – Plan software tool development
EO 005.02 – Build software tools
EO 005.03 – Build software tools

Appendix 2

Performance Objectives and Enabling Objectives

See Appendix 3 for the list of references that are coded alphabetically/numerically (e.g., C1, C2, C3) for the EOs.

PO 001 - Maintain Network Situational Awareness

EO	EO content (what students must be able to do on completion of associated education & training)
EO 001.01 - Enumerate a network and system	(1) Prepare the network scanning tool, to include: (a) identifying targets and Internet Protocol (IP) space; (b) verifying targets and IP space as DND)/CAF-owned; and (c) configuring the network scanning tool, in accordance with (IAW) the tool documentation. (2) Test custom network assessment functionality, to include: (a) running the tool with current configurations on a test IP range; (b) validating the test output to ensure correct results; and (c) adjusting the scan configurations as required, to account for unforeseen issues with bandwidth usage, scan run time or other parameters. (3) Run a network scanning tool on target IP space, to include: (a) initiating and monitoring scan progress; (b) troubleshooting scan progress and reconfiguring scan, to include pausing, assessing results, modifying and resuming scan; (c) validating scan output to ensure correct results; and (d) processing the output, in order to achieve a readable or visual format. (4) Analyze scan results, to include: (a) identifying critical information, to include: i. identifying device applications and operating systems (OS); and ii. identifying other information, including device type, port status, IP, host name, etc.; (b) fingerprinting the device, to include: i. characterizing the device by merging identifying information; and ii. validating the fingerprint, if required, through confirmatory scans, secondary tools or other information sources; (c) determining the location of physical network assets, to include: i. identifying location using automated tools (e.g., IP Control) or other network monitoring tools; and ii. identifying location using alternative methods, such as checking the geolocation of other IPs in range, cross-referencing with historical scan data, and cross-referencing with other identified devices or information. (5) Update the network situational awareness database, in accordance with database usage and documentation.

EO	EO content (what students must be able to do on completion of associated education & training)
EO 001.02 - Develop a logical network map	(1) Collect network asset information, to include data from: (a) network traffic; (b) automated scanning; and (c) partner organizations. (2) Build a network map, to include using: (a) manual methods to build the map, (e.g., Microsoft Visio, Microsoft PowerPoint) or other means; and (b) automated methods to build the map, including automated tools (e.g., ZenMap, LanState Pro) and scripts. (3) Update the network situational awareness database, in accordance with database usage and documentation.
EO 001.03 - Identify network and system vulnerabilities	(1) Prepare vulnerability assessment tools and assessment methodology, to include: (a) assessing intake package and client documentation; (b) identifying targets, IP space and scope of scan; (c) verifying targets and IP space as DND/CAF-owned; (d) acquiring administrative credentials or equivalent to achieve scan results; and (e) configuring the vulnerability assessment tool, in accordance with the tool documentation. (2) Test custom network assessment functionality, to include: (a) running the tool with current configurations on a test IP range; (b) validating the test output to ensure correct results; and (c) adjusting the scan configurations as required, to account for unforeseen issues with bandwidth usage, scan run time or other parameters. (3) Conducting tool-based vulnerability assessment, to include: (a) initiating and monitoring scan progress; (b) troubleshooting scan progress and reconfiguring scan, to include pausing, assessing results, modifying and resuming scan; (c) validating scan output to ensure correct results; and (d) processing the output, in order to achieve a readable or visual format. (4) Conduct manual vulnerability assessment, to include: (a) liaising with subject matter experts, system administrators, system operators, technical resources, Chief Information Officers (CIO)/Information System Security Officers (ISSO) and others; (b) assessing network configuration and processes against industry best practices and standards; and (c) supporting the task lead in assessing security controls, including physical, procedural, personal and IT security of network or system. (5) Analyze the manual and automated vulnerability assessment results, to include: (a) reviewing the automated results' criticality score (e.g., Common Vulnerabilities and Exposures [CVE] scores); (b) conducting a combined assessment of the manual and automated results; and (c) assessing the impact and likelihood of exploitation of any vulnerabilities discovered. (6) Initiate reporting.

EO	EO content (what students must be able to do on completion of associated education & training)
	(7) Update the network situational awareness database, in accordance with database usage and documentation.
EO 001.04 - Characterize network traffic to establish normal patterns	(1) Prepare for traffic collection, to include: (a) identifying the network devices and security appliances; (b) identifying the whitelisted, blacklisted and authorized traffic, protocols, applications, etc., for routine and non-routine operations; (c) determining the period of time required to benchmark network activity; and (d) preparing tools and scripts for collection. (2) Collect network traffic, to include: (a) using automated tools to capture network data, to include: i. initiating and monitoring packet capture; ii. troubleshooting packet capture activities; and iii. validating output to ensure intended results; and (b) using other means to collect required network data, including scripts, commands, etc. (3) Analyze packet capture and ancillary data, to include: (a) identifying distinct sessions and source/destination hosts; (b) creating statistics; and (c) summarizing baseline activity/metrics, to include:i. peak times and low times; and ii. bandwidth usage and traffic volume by application, protocol, port, etc. (4) Initiate reporting and present statistics.

PO 002 - Respond to a Cyber Event

EO	EO content (what students must be able to do on completion of associated education & training)
EO 002.01 - Detect threat activity	(1) Receive and analyze IDS alerts from various sources IAW references (refs) C35 and C116, to include: (a) identifying traffic parameters IAW refs C57 and C59; (b) extracting network traffic IAW refs C77, C78, C95, C96 and C125; (c) extracting network indicators from IDS IAW refs C35 and C116; (d) determining validity of alert IAW refs C76, C99, C105, C106 and C107; and (e) logging false positives IAW ref C115. (2) Analyze network traffic IAW refs C14, C58, C65, C97, C116 and C118, to include: (a) analyzing anomalies in network traffic using metadata IAW refs C57 and C125; (b) identifying network mapping and operating system finger printing; (c) investigating traffic behavior IAW refs C78 and C125; (d) analyzing event logs from perimeter security appliances IAW refs C116 and C126; and (e) extracting network indicators from traffic IAW refs C74, C78, C96 and C125.

EO	EO content (what students must be able to do on completion of associated education & training)
EO 002.02 – Investigate cyber events	(1) Validate alerts/anomalous behavior through network analysis, to include: (a) collecting metadata, network traffic and logs, to include: i. identifying device applications and operating systems based on network traffic IAW refs C58, C78, C97, C116, C118 and C125; ii. identifying event timeline IAW refs C74, C116 and C125; iii. extracting network indicators from traffic IAW refs C74, C78, C96 and C125; and iv. determining location of physical network asset IAW refs C125, C127 and C128. (b) reconstructing malicious activity, to include: i. analyzing malicious activities IAW refs C74, C78 and C125; ii. collating traffic activity to determine the source of compromise IAW refs C78, C116 and C125; iii. identifying means of compromise, including command and control channels and exfiltration IAW refs C14, C70, C73, C108, C114, and C125; iv. identifying exploitation attempts IAW ref C109; and v. extracting packet capture for protocol analysis IAW refs C78, C114, and C125. (c) providing preliminary findings for additional analysis, to include indicators (i.e., IPs, hostnames, ports). (2) Conduct packet capture (PCAP) analysis, to include: (a) analyzing PCAPs IAW refs C57, C58, C74, and C79; (b) extracting artifacts IAW ref C74, C119 and C125; and (c) collecting artifacts IAW ref C74. (3) Perform malware analysis IAW refs C74, C77 and C95, to include: (a) analyzing artifacts IAW ref C120; (b) characterizing malware with automated tools IAW refs C74, C77, C95 and C121; and (c) escalating malware incident for additional analysis.
EO 002.03 – Produce internal reports	(1) Collate relevant data in order to initiate a technical report, to include: (a) identifying or acknowledging the event or issue; (b) creating a documented timeline of the incident; (c) identifying relevant findings and conclusions that must be communicated to the supervisor, external agency and/or client; and (d) determining suitable recommendations to mitigate or resolve the event or issue. (2) Draft the report, including the following elements as appropriate: (a) any necessary introductory remarks/background information; (b) observations/findings (e.g., risks and vulnerabilities, analysis findings, system and network/data facts); (c) conclusions based on the observations/findings; and (d) recommended mitigation measures to improve security and/or incident recovery measures.

EO	EO content (what students must be able to do on completion of associated education & training)
EO 002.04 – Safeguard cyber forensic evidence	(1) Create a working copy of the artifact; (2) Preserve the original artifact; (3) Document specifically what the artifact is; (4) Document how it was obtained; (5) Document when it was collected; (6) Document who handled it and what actions have been taken; and (7) Document where the artifact is stored.

PO 003 – Produce a Technical Report

EO	EO content (what students must be able to do on completion of associated education & training)
EO 003.01 - Collate relevant data in order to initiate a technical report	(1) Identify or acknowledge the event or issue; (2) Create a documented timeline of the event or issue; (3) Extract relevant details contained within document analysis notes; (4) Identify relevant findings and conclusions that must be communicated to the supervisor, external agency and/or client; and (5) Determine suitable recommendations to mitigate or resolve the event or issue.
EO 003.02 – Draft a technical report	Draft the report, including the following elements as appropriate: (1) Any necessary introductory remarks/background information; (2) Observations/findings (e.g., risks and vulnerabilities, analysis findings, system and network/data facts); (3) Conclusions based on the observations/findings; (4) Recommended mitigation measures to improve security and/or incident recovery measures; and (5) Any new information relevant to the event or issue that will increase the accuracy of the report.
EO 003.03 - Produce a technical report for verbal or written dissemination	Produce the report for verbal or written dissemination, taking into consideration the audience and use of appropriate technical language, employing the following principles: (1) Clarity (report is explicit, definite, complete, intelligible and unambiguous); (2) Accuracy (report is exact in detail and factual); (3) Relevance (report is free of irrelevant words, phrases and ideas); (4) Brevity (report is concise, ideas and facts are expressed as briefly as possible but not at the expense of clarity, accuracy or relevance); and (5) Timeliness (report is delivered in accordance with required timelines).

PO 004 - Prepare an Analysis Environment

EO	EO content (what students must be able to do on completion of associated education & training)
EO 004.01 - Install required hardware	Install required hardware, to include but not limited to: (1) Workstation, (2) Hard drive, and (3) Tap switch.

EO 004.02 - Configure physical network security devices	Configure physical network security devices, to include:
	(1) Routers;
	(2) Switches;
	(3) Firewalls;
	(4) Network taps; and
	(5) IDS and IPS.

EO	EO content (what students must be able to do on completion of associated education & training)
EO 004.03 - Prepare and set up virtual operating systems	(1) Install a virtual server (e.g., enterprise plus type 1 [ESXI]) IAW ref C43, to include: (a) installing virtual Windows user workstation IAW refs C27 and C43; (b) installing various workstation virtual images IAW refs C32 and C43; (c) installing various mobile virtual images IAW ref C129; and (d) setting up Windows servers, to include: i. domain controller IAW refs C28, C29 and C30; ii. file and print server IAW refs C28, C29 and C30; iii. Domain Name Server (DNS) IAW refs C28, C29, C30, C46 and C47; iv. Dynamic Host Control Protocol (DHCP) server IAW refs C28, C29 and C30; v. exchange server IAW refs C28, C29, C30 and C48; vi. Information Internet Server (IIS) Microsoft web server IAW refs C28, C29 and C30; and vii. MySQL server IAW refs C28, C29 and C30. (2) Set up security group policies, to include configuring IAW refs C27, C28, C29 and C30. (3) Set up a Linux virtual workstation and server, to include: (a) setting up Linux web server (e.g., Linux Apache MySQL and PHP [LAMP] web server) IAW ref C45; (b) installing web application firewall (e.g., mod-security for Apache); and (c) installing a Linux workstation IAW ref C31. (4) Set up and configuring virtual networking systems, to include: (a) routers IAW refs C23, C26 and C49; (b) switches IAW refs C23, C26 and C49; (c) network taps; (d) IPS; and (e) firewalls IAW refs C49 and C56. (5) Manage snapshots of virtual images IAW ref C43, to include: (a) taking virtual snapshots; (b) reverting to old snapshots; (c) reverting to new snapshots; and (d) deleting snapshots. (6) Install local virtual workstation environment (e.g., Virtual Box or VMware workstation), to include setting up a virtual operating system image (e.g., in .iso format) IAW ref C43.
EO 004.04 – Configure software	(1) Install software, to include: (a) User software (e.g., Adobe, Office, Wireshark); (b) Scripting software (e.g., Python, Ruby); and (c) Malware analysis tools (e.g., ApateDNS, InetSim). (2) Configure software (e.g., packet sniffing software).
EO 004.05 - Troubleshoot toolset hardware deficiencies	(1) Replace hardware. (2) Configure physical networks.

EO	EO content (what students must be able to do on completion of associated education & training)
EO 004.06 - Troubleshoot toolset software deficiencies	(1) Resolve dependencies for software. (2) Uninstall and install applications. (3) Install and remove patches.
EO 004.07 - Set up and maintain network sensors	(1) Set up a network tap inline and out of band IAW ref C130, to include: (a) installing a hardware tap; and (b) mirroring a switch port (e.g., Hewlett Packard, CISCO). (2) Confirm network sensor functionality, to include: (a) verifying full packet capture, to include full packet capture retention and when packets will roll over; (b) verifying metadata retention; and (c) conducting sensor checks and reporting outages, to include informing supervisor of functionality. (3) Develop network sensor rules, to include: (a) writing a network sensor rule; (b) testing network sensor rule functionality; (c) recommending deployment of network sensor rules; (d) loading network sensor rules to sensors; (e) confirming validity of network sensor alerts against network traffic; and (f) recommending deactivation of network sensor rules.
EO 004.08 – Remove required software and hardware	(1) Remove required software, to include: (a) removing software from add-remove programs through Windows; (b) removing software from Linux command line (e.g., with “apt-get and yum remove”); and (c) formatting computer (e.g., with a kill disk). (2) Remove required hardware (e.g., switch, router, tap, USB, hard drive).

PO 005 - Develop Software Tools

EO	EO content (what students must be able to do on completion of associated education & training)
EO 005.01 - Plan software tool development	(1) Determine software deficiencies IAW ref C17 (Chapters 1, 2, 5, 6, and18). (2) Translate security requirements into application design elements, to include: (a) documenting the elements of software attack surfaces; and (b) identifying security implications on the network IAW refs C16 (Chapter 8). (3) Prepare work flow charts, to include: (a) implementing security into the software development cycle IAW ref C17 (Chapters 3–5); and (b) producing programming flow chart IAW refs C12, C14 (Chapter 12), and C15 (Chapters 13, 14 and 22).

EO	EO content (what students must be able to do on completion of associated education & training)
EO 005.02 – Build software tools	(1) Write software documentation IAW ref C15 (Chapters 3–5) and C17. (2) Program custom algorithms, to include: (a) designing algorithms, to include: i. identifying basic coding flaws, to include applying coding and testing standards IAW refs C14 (Chapter 12) and C16 (Chapter 1); and ii. applying security and programming best practices, to include programming scripts and programs, IAW refs C5, C7, C8, C11, C12 and C15; and (b) applying code and testing standards, to include testing tools and conducting trial runs of programs, to include: i. debugging software and designing unit tests IAW refs C15 (Chapter 6) and C17; and ii. correcting program errors, by making appropriate changes and rechecking to program to ensure desired results, IAW refs C15 and C17.
EO 005.03 – Build software tools	(1) Determine appropriate software patches, to include documenting software patches IAW ref C41. (2) Modify existing software IAW refs C14 (Chapters 17 and 18), C41, and C42 (Chapter 54), to include: (a) correcting errors; (b) ugrading interfaces; and (c) improving performance. (3) Perform risk analysis when an application has a major change IAW refs C14, C41, and C42 (Chapter 54).

Appendix 3

List of References

Those references in Appendix 2 for the EOs are highlighted in yellow.

Reference	Publication
A	**Canadian Military References**
A1	A-P2-002-NDA/PG-B01 CFSE Network Defence Analyst QS/TP
A2	NDSOD Ch 6 & 7 National Defence Security Orders and Directives (http://intranet.mil.ca/en/health-safety-security/security-policies-ndsod.page)
A3	NDSOD Ch 5,6 and 7 National Defence Security Orders and Directives (http://intranet.mil.ca/en/health-safety-security/security-policies-ndsod.page)
A4	ADM(IM) IT Security Policies and Standards (http://admim-smagi.mil.ca/en/security/policies-standards/index.page)
A5	A-SJ-100-002/AS-001 Information System Security – Operational Security Standard for Information Systems (OSSIS) (http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6003-0.page)
A6	CAF Cyber Operations Primer, February 2014, Chief of Force Development
A7	JDN 2017-02, CAF Joint Doctrine Note - Cyber Operations.
A8	DAOD 6002-2 (http://intranet.mil.ca/en/defence-admin-orders-directives/6000/6002-2.page)
B	**Allied Military References**
B1	TSG 158-0020 Conduct A Military Briefing (USAF) (http://tsg3.us/tnsg_lib/pldc_school/off_advanced/tnsg_158_0020_conduct_briefing/tnsg_158_0020.pdf) (http://tsg3.us/tnsg_lib/pldc_school/off_advanced/tnsg_158_0020_conduct_briefing/tnsg_158_0020_exam.pdf)
B2	CIICS User Guide
C	**Commercial References**
C1	ISBN 978-1-59327-509-9, The practice of Network Security Monitoring: Understanding Incidence Detection and Response.
C2	ISBN 978-0-471-66186-3, Computer Networking – Internet Protocols in Action
C3	ISBN 978-1587202834, Top-Down Network Design
C4	ISBN 978-1593275679, How Linux Works: What Every Superuser Should Know
C5	ISBN 978-1-59327-192-3, Gray Hat Python - Python Programming for Hackers and Reverse Engineers
C6	ISBN 978-1-118-10679-2, Linux Essentials
C7	ISBN 0070131511, Introduction to Algorithms, Second Edition
C8	ISBN 0470383267, Data Structures and Algorithms in Java
C9	ISBN 0534491324, Computer Science: A structured programming approach using C
C10	ISBN 9780133591620, Modern Operating Systems
C11	ISBN 0132143011, Distributed Systems: Concepts and Design
C12	ISBN 0596007124, Head First Design Patterns
C13	ISBN 9780134101613, Computer Organization and Architecture (9th Edition)
C14	ISBN 9780321247445, Introduction to computer security
C15	ISBN: 9781593271190, Code Craft: The Practice of Writing Excellent Code
C16	ISBN: 781593274245, Think Like a Programmer: An Introduction to Creative Problem Solving
C17	ISBN: 9780471793717, Software Testing: Testing Across the Entire Software Development Life Cycle
C18	Center for Internet Security (CIS) Top 20 Controls (https://www.cisecurity.org/critical-controls/Library.cfm)
C19	Common Vulnerability Scoring System v3.0 (https://www.first.org/cvss)
C20	Using Wireshark to Create Network-Usage Baselines (https://wiki.wireshark.org/KnownBugs/OutOfMemory?action=AttachFile&do=get&target=Using+Wireshark+to+Create+Network-Usage+Baselines.pdf)

Reference	Publication
C21	ISBN: 9781259589515, CompTIA A+ Certification All-in-One Exam Guide, Ninth Edition (Exams 220-901 & 220-902)
C22	ISBN: 9780071848220, CompTIA Network+ All-In-One Exam Guide, Sixth Edition (Exam N10-006)
C23	ISBN: 9781119288282, CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125
C24	ISBN: 9780071841245, Security + Certifications
C25	ISBN: 9781119155034, SSFIPS Security Cisco Networks with Sourcefire intrusion Prevention System Study Guide
C26	ISBN: 9781587144349, CCNP Routing and Switching Portable Command Guide
C27	ISBN: 9781597495615, Microsoft Windows 7 Administrator's Reference: Upgrading, Deploying, Managing, and Securing Windows 7
C28	ISBN: 9780470532867, Mastering Windows Server 2008 R2
C29	ISBN: 9781118289426, Mastering Windows Server 2012 R2
C30	ISBN: 9781785888908, Mastering Windows Server 2016
C31	ISBN: 780072193688, All-In-One Linux+ Certification Exam Guide
C32	ISBN: 9780071668972, MAC OSX System Administration
C33	ISBN: 9780071849272, CISSP Exam study Guide
C34	ISBN: 9781593275099, The practice of Network Security Monitoring: understanding Incident Detection and Response
C35	ISBN: 9781597490993, Snort IDS and IPS Toolkit
C36	ISBN: 9781118987056, The Network Security Test Lab a Step by Step Guide
C37	ISBN: 9781783985982, Kali Linux CTF BluePrints
C38	ISBN: 9781785883491, Building Virtual Pentesting Labs for Advanced Penetration Testing – Second Edition
C39	ISBN: 9780132564717, Network Forensics Tracking Hackers Through Cyberspace
C40	ISBN: 9781593272906 Practical Malware Analysis: The Hands on Guide to Dissecting Malicious Software
C41	Best Practices for Applying Service Packs, Hotfixes and Security Patches by Rick Rosato, Technical Account Manager, Microsoft Corporation (https://msdn.microsoft.com/en-us/library/cc750077.aspx)
C42	ISBN: 9781118127063, Computer Security Handbook, Set, 6th Edition
C43	ISBN: 9781118925157, Mastering VMware vSphere 6
C44	ISBN: 9781508532323, Information Assurance Directorate: Spotting the Adversary with Windows Event Log Monitoring
C45	ISBN: 9781539050261, Modern Web Server Administration using Linux and Wordpress
C46	ISBN: 9784873113906, DNS & BIND : Help for system administrators
C47	ISBN: 9780128033067, DNS Security: Defending the Domain Name System
C48	ISBN: 9781118556832, Mastering Microsoft Exchange Server 2013
C49	ISBN: 9781587142727, Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide (2nd Edition) (Foundation Learning Guides)
C50	ISBN: 9781587052460, Network Security Technologies and Solutions (CCIE Professional Development Series)
C51	ISBN: 9780470527665, CCNA Voice Study Guide: Exam 640-460
C52	ISBN: 9780470527658, CCNA Wireless Study Guide: IUWNE Exam 640-721
C53	ISBN: 9788126543311, CCNA Data Center: Introducing Cisco Data Center Networking Study Guide, Exam 640-911
C54	Cisco Network-Based Intrusion Detection—Functionalities and Configuration (http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/8_NIDS.pdf)
C55	Kerberos Golden Ticket Protection Mitigating Pass-the-Ticket on Active Directory (http://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf)

Reference	Publication
C56	ISBN: 9781587143076, Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services, 3rd Edition
C57	ISBN: 9781593275099, The practice of Network Security Monitoring: Understanding Incidence Detection and Response
C58	ISDB: 9780471661863, Computer Networking – Internet Protocols in Action
C59	ISBN: 9780735712652, Network Intrusion Detection – Third Edition
C60	ISBN: 9781587202834, Top-Down Network Design
C61	ISBN: 9781449319212, IPv6 Essentials, 3rd Edition – Integrating IPv6 into your IPv4 Network
C62	ISBN: 9781593275679, How Linux Works: What Every Superuser Should Know
C63	ISBN: 9781593271923, Gray Hat Python - Python Programming for Hackers and Reverse Engineers
C64	ISBN: 9780735611313, The Hidden Language of Computer Hardware and Software
C65	ISBN: 9780071497282, CCNA Study Guide 640-802
C66	ISBN: 9780321336316, TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition)
C67	ISBN: 9781118106792, Linux Essentials ISDN
C68	An Introduction to Attack Patterns as A Software Assurance Knowledge Resource – OMG Software Assurance Workshop 2007 (https://capec.mitre.org/documents/An_Introduction_to_Attack_Patterns_as_a_Software_Assurance_Knowledge_Resource.pdf)
C69	Intrusion Detection Systems: A survey of Taxonomy (https://pdfs.semanticscholar.org/7D28/948bdcb530e2c1deedd8d22dd9b54788a634.pdf)
C70	ISBN: 9780071780285, Hacking Exposed 7: Network Security Secrets and Solutions
C71	DNS Sinkhole whitepaper - SANS Institute InfoSec Reading Room (https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523)
C72	ISBN: 9780596007911, Snort Cookbook
C73	ISBN: 9780128006047, Targeted Cyber Attacks
C74	Wireshark Network Protocol Analyzer: (http://www.wiresharktraining.com)
C75	Validate the legitimacy of an Alert Network tools, including traceroute, nslookup, dig, whois, ping (http://centralops.net)
C76	Validate the legitimacy of an Alert Analyze IPs with multiple IP blacklists and DNS blacklists (http://ipvoid.com)
C77	Tcpdump/libcap (http://www.tcpdump.org)
C78	Cheat Sheets (Headers, ports, and protocols) (http://packetlife.net/library/cheat-sheets/)
C79	RFC 1700 (Port Numbers) (https://www.ietf.org/rfc/rfc1700.txt)
C80	IANA (https://www.iana.org/)
C81	All TCP/UDP ports (http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)
C82	CCNA Routing and Switching: Introduction to Networks (https://www.netacad.com)
C83	IP Addresses Authority (https://www.iana.org/)
C84	Other Cisco Learning Games (https://learningnetwork.cisco.com/community/learning_center/games)
C85	IP Addressing Guide (http://www.tcpipguide.com/free/t_IPAddressing.htm)
C86	Online Subnet Calculator (http://www.subnet-calculator.com/)
C87	Cisco Subnet Game (https://learningnetwork.cisco.com/docs/DOC-1802)
C88	Cisco IP address and Subnet Introduction (In Depth) (http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html)
C89	IPv6 Primers (https://ipv6.he.net/certification/primer.php) (http://en.wikipedia.org/wiki/IPv6)
C90	IPv6 Certification (https://ipv6.he.net/certification/)
C91	Regex (https://support.sas.com/rnd/base/datastep/perl_regexp/regexp-tip-sheet.pdf)
C92	Common Attack Pattern Enumeration and Classification (CAPEC) (https://capec.mitre.org/index.html)
C93	The TCP/IP Guide (http://www.tcpipguide.com/free/index.htm)
C94	RFC SourceBook (http://www.networksorcery.com/enp/default.htm)

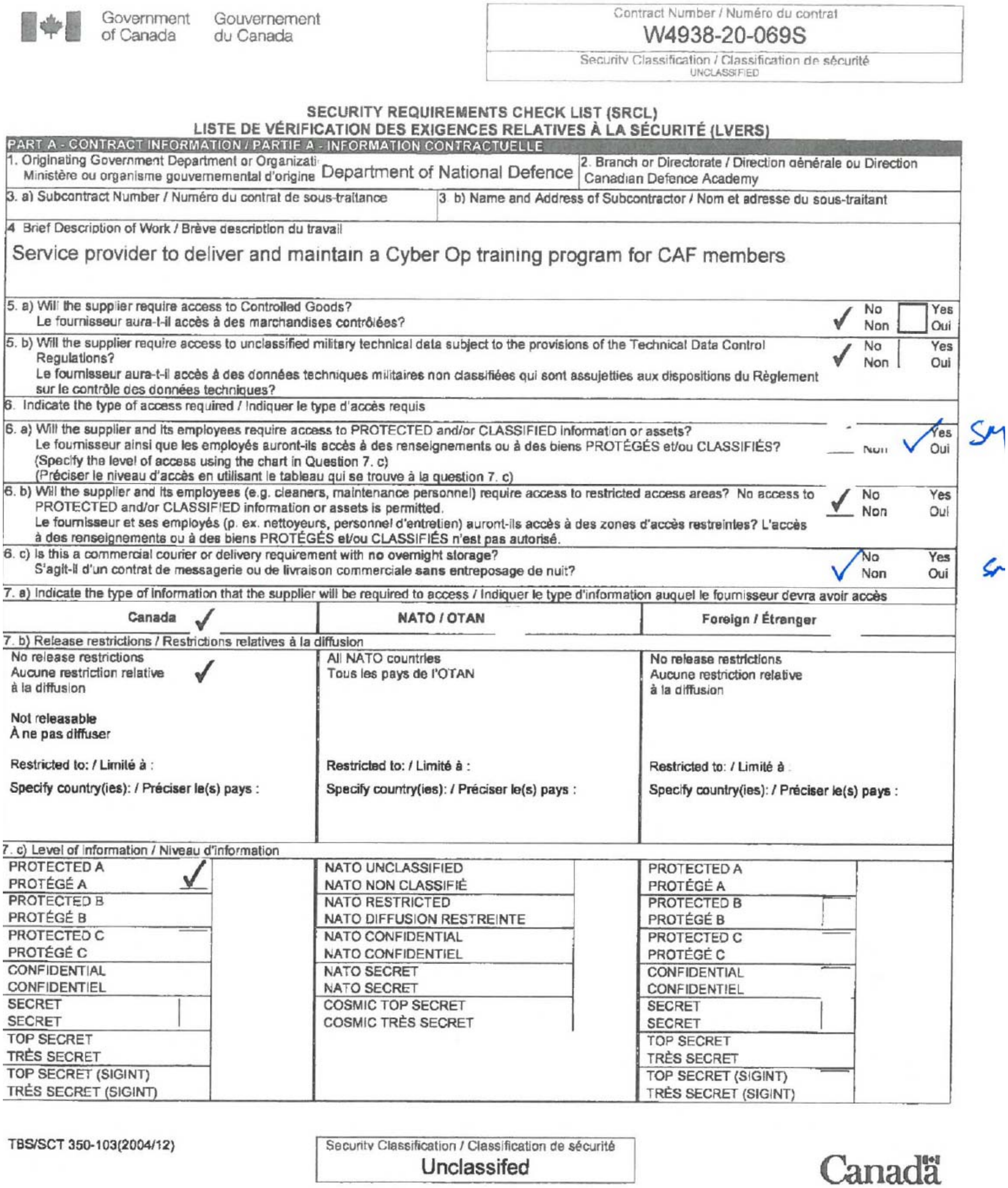
Reference	Publication
C95	Ngrep (https://www.freebsd.org/cgi/man.cgi?query=ngrep&sektion=8&manpath=FreeBSD+10.1-RELEASE+and+Ports)
C96	Google search operators (https://support.google.com/websearch/answer/2466433)
C97	Common Vulnerability Database (https://cve.mitre.org/)
C98	Validate the legitimacy of an Alert, Scan websites with multiple reputation engines & blacklists (http://urlvoid.com)
C99	Validate the legitimacy of an Alert, American Registry for Internet Numbers (http://arin.net)
C100	Validate the legitimacy of an Alert, Hurricane Electric Border Gateway Protocol (BGP) Toolkit (http://bgp.he.net)
C101	Validate the legitimacy of an Alert, Robtex Swiss Army Knife Internet Tool (http://www.robtex.com)
C102	Validate the legitimacy of an Alert, Alert Signature Websites, Cisco Intrusion Prevention System Signatures (http://tools.cisco.com/security/center/search.x?search=Signature)
C103	Validate the legitimacy of an Alert, Alert Signature Websites, Emerging Threats Snort Rule Database (http://doc.emergingthreats.net/)
C105	Validate the legitimacy of an Alert, Alert Signature Websites, Snort Rules Website and Rule Lookup (https://snort.org/downloads/#rule-downloads)
C106	Alert Signature Websites (http://manual-snort-org.s3-website-us-east-1.amazonaws.com/)
C107	nmap (https://nmap.org/)
C108	Penetration Testing Execution Standard – Exploitation (http://www.pentest-standard.org/index.php/Exploitation)
C109	Honeypots (https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9)
C110	Know Your Enemy; Honey Net (http://old.honeynet.org/papers/honeynet).
C111	Intrusion Detection FAQ (https://www.sans.org/security-resources/idfaq/are-there-limitations-of-intrusion-signatures/1/21)
C112	Suricata Rule guide (https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_Rules)
C113	PCAP-FILTER man page (http://www.tcpdump.org/manpages/pcap-filter.7.html)
C114	Strategies to Reduce False Positives and False Negatives in NIDS (http://www.symantec.com/connect/articles/strategies-reduce-false-positives-and-false-negatives-nids)
C115	Base64 (https://www.base64decode.org/)
C116	Arcsight (SIEM) (http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/)
C117	History of Encryption (SANS) (https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730)
C118	SANS Glossary of terms (www.sans.org/security-resources/glossary-of-terms)
C119	PCAP man page (http://www.tcpdump.org/manpages/pcap.3pcap.html)
C120	Cuckoo Sandbox Book (https://downloads.cuckoosandbox.org/docs/)
C121	NetWitness Investigator User Guide 9.8 (https://community.rsa.com/docs/DOC-36525)
C122	Sericata User Guide (http://suricata.readthedocs.io/en/latest)
C123	Yara Documentation (http://yara.readthedocs.io/en/v3.4.0/index.html)
C124	Stix Documentation (http://stixproject.github.io/documentation/)
C125	RSA NetWitness (https://sadocs.emc.com/0_en-us)
C126	Sourcefire 3D System (http://www.cisco.com/c/dam/en/us/td/docs/security/sourcefire/3d-system/53/Sourcefire_3D_System_User_Guide_v53.pdf)
C127	IP Address Geolocation (http://www.ipfingerprints.com/)
C128	IP Address Geolocation (http://www.ip-tracker.org/locator/ip-lookup.php)
C129	ISBN 9781516945863, Intermediate Security Testing with Kali Linux 2
C130	Out of Band Network Tap (https://www.ixiacom.com/company/blog/nsa-does-not-want-you know-about-taps-network-security)

Reference	Publication
C131	ISBN: 0470613033 - Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code
C132	ISBN: 1118825098 – The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory.
C133	ISBN: 1118787315 – Practical Reverse Engineering
C134	ISBN: 978-1-59327-716-1 – Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats.
C135	ISBN: 978-1-59327-793-2 – Practical Forensic Imaging: Securing Digital Evidence with Linux Tools
C136	ISBN: 978-1449626365 – The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System (2nd Edition)
C137	ISBN 978-0071832380 – Grey Hat Hacking: The Ethical Hacker's Handbook (Fourth Edition)
C138	ISBN 978-1491934944 – Intelligence-Driven Incident Response: Outwitting the Adversary
C139	ISBN 978-1500734756 – Blue Team Handbook: Incident Response Edition: A Condensed field guide for the Cyber Security Incident Responder.
C140	ISBN 978-0071798686 – Incident Response & Computer Forensics (Third Edition)
C141	ISBN 978-1118026472 – The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2nd Edition)
C142	ISBN 978-8126558766 – The Antivirus Hackers' Handbook
D	**Other**
D1	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF), NIST 800-181 (US Gov) (http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf)
D2	ITSG-38: Information Technology Security Guideline Network Security Zoning, Design Considerations for Placement of Services within Zones (CSE) (https://www.cse-cst.gc.ca/en/publication/itsg-38)
D3	ITSG-33: IT Security Risk Management: A Lifecycle Approach (CSE) (https://www.cse-cst.gc.ca/en/publication/itsg-33)
D4	Canada Evidence Act (http://laws-lois.justice.gc.ca/eng/acts/C-5/FullText.html)
D5	DRDC CORA TM 2013-XXX, Military Activities and Cyber Effects (MACE) Taxonomy, December 2013 (http://cradpdf.drdc-rddc.gc.ca/PDFS/unc218/p803340_A1b.pdf)
D6	ITSB-120 Cross Domain Security Primer (https://www.cse-cst.gc.ca/en/publication/list/Network-Security)
D7	ITSB-49 Security Bulletin - Keyloggers and Spyware (https://www.cse-cst.gc.ca/en/publication/list/Network-Security)
D8	ITSG-41 Security Requirements for Wireless Local Area Networks (https://www.cse-cst.gc.ca/en/publication/itsg-41)
D9	ITSB-96 Security Vulnerabilities and Patches Explained - IT Security Bulletin for the Government of Canada (https://www.cse-cst.gc.ca/en/publication/itsb-96)
D10	ITSB-100 Spotting Malicious E-mail Messages – Guidance for the Government of Canada (https://www.cse-cst.gc.ca/en/publication/itsb-100)
D11	ITSB-89 v3 Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information (https://www.cse-cst.gc.ca/en/publication/list/Security-Protocols)
D12	ITSG-31 User Authentication Guidance for IT Systems (https://www.cse-cst.gc.ca/en/publication/itsg-31)
D13	Security of Information Act (R.S.C., 1985, c. O-5) (http://laws-lois.justice.gc.ca/eng/acts/O-5/)
D14	Criminal Code R.S.C., 1985, c. C-46 Section 184 – Interception of Communications (http://laws-lois.justice.gc.ca/eng/acts/C-46/page-41.html?txthl=communications+communication+interception+intercepted+intercept#s-184.2)

Reference	Publication
D15	Criminal Code R.S.C., 1985, c. C-46 Section 342.1 – Unauthorized Use of Computer (http://laws-lois.justice.gc.ca/eng/acts/C-46/page-76.html?txthl=unauthorized+computer+use#s-342.1)
D16	Criminal Code R.S.C., 1985, c. C-46 SectSection 430(1.1) – Mischief in Relation to Computer Data (http://laws-lois.justice.gc.ca/eng/acts/C-46/page-89.html?txthl=relation+relating+mischief+computer+data#s-430)
D17	CSE OPS-1 (CLASSIFIED document)
D18	CSE OPS 5-15 (CLASSIFIED document)
D19	CSE CSOI 4-1 (CLASSIFIED document)
D20	Canadian SIGINT Security Standards (CLASSIFIED document)
D21	CFNOC SOP Physical Media Analysis - Forensics Tasking's
D22	CFNOC CND Tp SOP Annex H Network Defence Report
D23	DIME1 2 DSB G2 –Trends in vectors, payloads, behaviours, and effects
D24	CFNOC Ops Reference Guide
D25	CFNOC Surveillance Analyst Working Aide
D26	CFNOC Surveillance Report Template
D27	Short Course in Network Security (SCINS) course notes, Computer Network lectures 1-5
D28	SCINS course notes, Internet Protocols lectures 1-5
D29	SCINS course notes, Security Architecture lectures 1
D30	SCINS course notes, Operating Systems lectures 1-5
D31	CFCOSO lecture – tech day 3 (Reconnaissance, Maintaining Access, Gaining Access)
D32	CFCOSO 1501 lecture – Network Defence

ANNEX B

SECURITY REQUIREMENTS CHECK LIST



Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W4938-20-069S

Security Classification / Classification de sécurité
UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organizati / Ministère ou organisme gouvernemental d'origine: Department of National Defence

2. Branch or Directorate / Direction générale ou Direction: Canadian Defence Academy

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

Service provider to deliver and maintain a Cyber Op training program for CAF members

5. a) Will the supplier require access to Controlled Goods?
Le fournisseur aura-t-il accès à des marchandises contrôlées?
✓ No Non □ Yes Oui

5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations?
Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?
✓ No Non Yes Oui

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?
Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS?
(Specify the level of access using the chart in Question 7. c)
(Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)
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 ✓	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 :	Restricted to: / Limité à :	Restricted to: / Limité à :
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

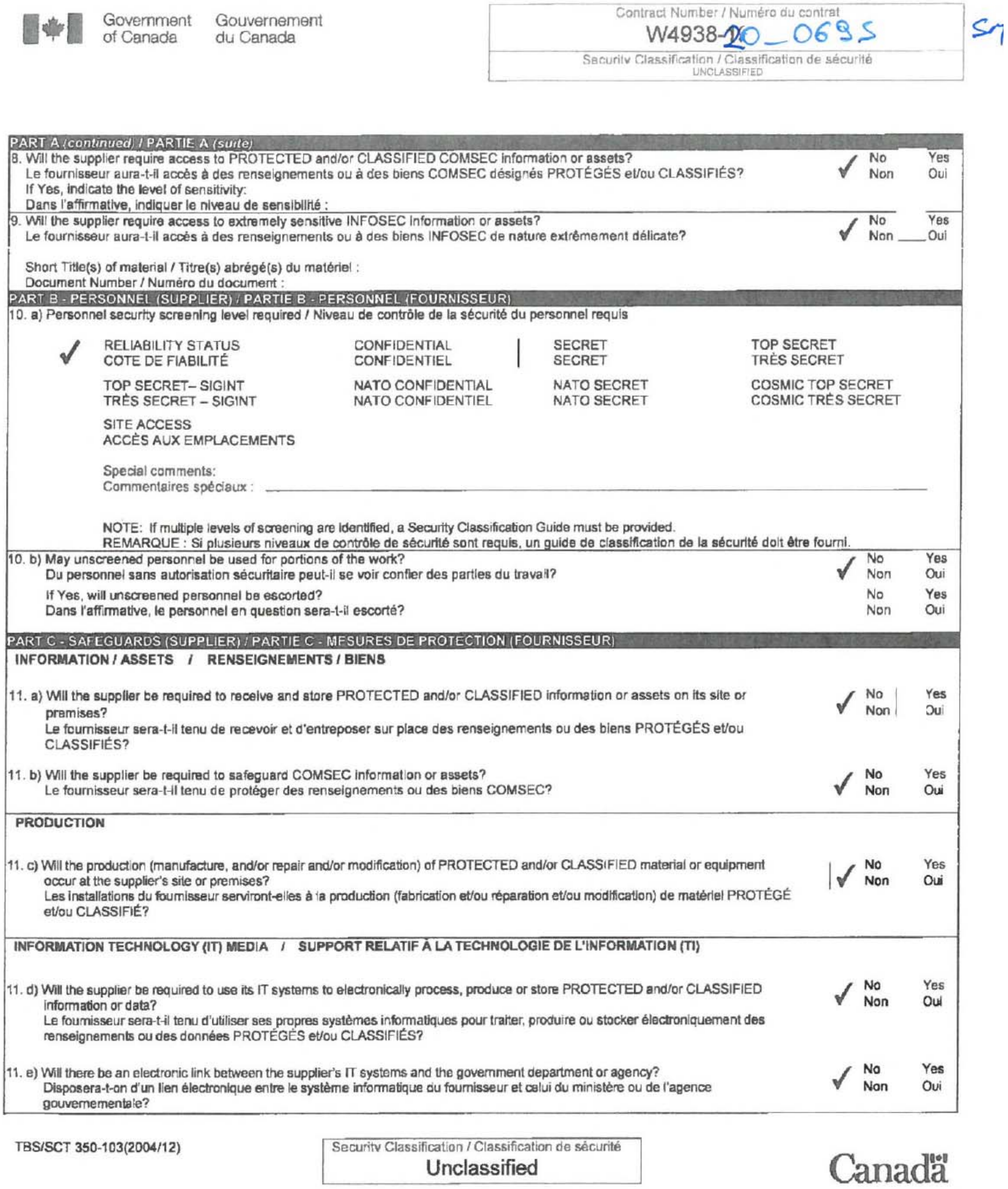
7. c) Level of information / Niveau d'information

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)

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
Unclassifed

Canada



Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W4938-20_069S

Sm

Security Classification / Classification de sécurité
UNCLASSIFIED

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?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :
✓ No / Non — Yes / Oui

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

✓ 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)

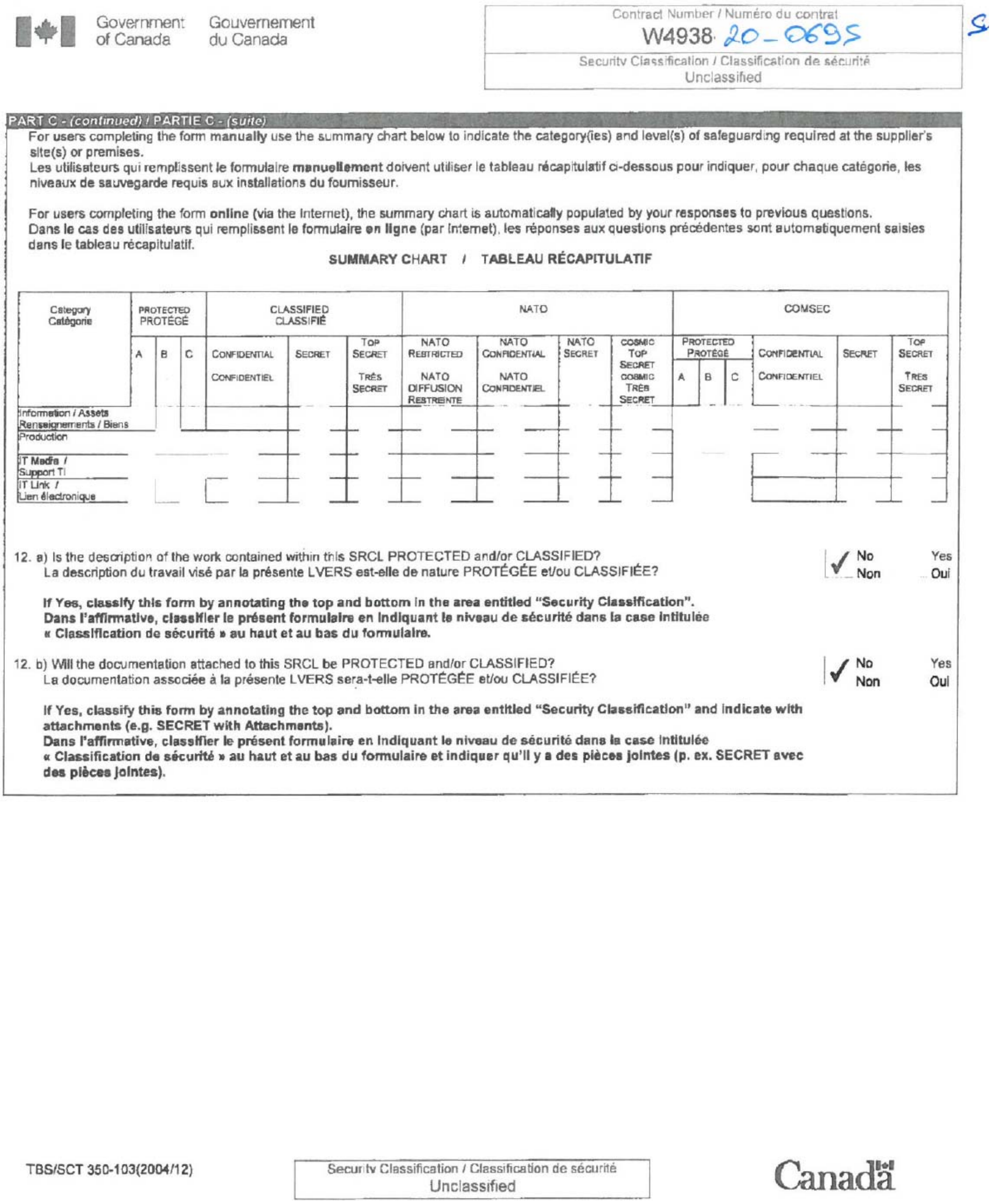
11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou 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

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
Unclassified

Canada



Government of Canada Gouvernement du Canada

Contract Number / Numéro du contrat
W4938 20-0695 S

Security Classification / Classification de sécurité
Unclassified

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

[✓ No / Non] Yes / Oui

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

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

[✓ No / Non] Yes / Oui

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

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
Unclassified

Canadä

ANNEX C

NON-DISCLOSURE AGREEMENT

I, ________________________________ , recognize that in the course of my work as an employee or subcontractor of _________________________ , I may be given access to information by or on behalf of Canada in connection with the Work, pursuant to Contract Serial No. W4938-20069Sé001/ZH between Her Majesty the Queen in right of Canada, represented by the Minister of Public Works and Government Services and the Department of National Defence, including any information that is confidential or proprietary to third parties, and information conceived, developed or produced by the Contractor as part of the Work. For the purposes of this agreement, information includes but not limited to: any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form, recorded electronically, or otherwise and whether or not labeled as proprietary or sensitive, that is disclosed to a person or that a person becomes aware of during the performance of the Contract.

I agree that I will not reproduce, copy, use, divulge, release or disclose, in whole or in part, in whatever way or form any information described above to any person other than a person employed by Canada on a need to know basis. I undertake to safeguard the same and take all necessary and appropriate measures, including those set out in any written or oral instructions issued by Canada, to prevent the disclosure of or access to such information in contravention of this agreement.

I also acknowledge that any information provided to the Contractor by or on behalf of Canada must be used solely for the purpose of the Contract and must remain the property of Canada or a third party, as the case may be.

I agree that the obligation of this agreement will survive the completion of the Contract Serial No.: W4938-20069S/001/ZH.

____
Signature

____
Date