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 0A1 / Noyau 0A1
Gatineau, Québec K1A 0S5
Bid Fax: (819) 997-9776

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

Title - Sujet ARMOUR TDP	
Solicitation No. - N° de l'invitation W7714-115274/E	**Date** 2013-02-18
Client Reference No. - N° de référence du client W7714-115274	
GETS Reference No. - N° de référence de SEAG PW-$$SV-051-25450	
File No. - N° de dossier 051sv.W7714-115274	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin at - à **02:00 PM** on - le **2013-04-30**	**Time Zone Fuseau horaire** Eastern Daylight Saving Time EDT

F.O.B. - F.A.B.
Plant-Usine: ☐ Destination: ☑ Other-Autre: ☐

Address Enquiries to: - Adresser toutes questions à: Peter Murray	**Buyer Id - Id de l'acheteur** 056sv
Telephone No. - N° de téléphone (819) 956-1387 ( )	**FAX No. - N° de FAX** (819) 997-2229

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

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	**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

Science Procurement Directorate/Direction de l'acquisition de travaux scientifiques
11C1, Phase III
Place du Portage
11 Laurier St. / 11, rue Laurier
Gatineau, Québec K1A 0S5

Canada

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

TABLE OF CONTENTS

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

9.   Applicable Laws
10.   Priority of Documents
11.   Defence Contract
12.   Foreign Nationals (Canadian Contractor) **OR**
        Foreign Nationals (Foreign Contractor)
13.   Insurance
14.   Controlled Goods Program
15.   Site Regulations

List of Attachments:

Attachment 1   Financial Bid Preparation Instructions
Attachment 2   Financial Bid Presentation Sheet
Attachment 3   Evaluation of Price
Attachment 4   Mandatory and Point Rated Technical Criteria
Attachment 5   Certifications Precedent to Contract Award
Attachment 6   Certifications Required with the Bid

List of Annexes:

Annex **A**   Statement of Work
        Appendix A   WORK Definitions
        Appendix B   Deliverables
        Appendix C   Optional Services Requirement
        Appendix D   Resource CATEGORY Requirements
        Appendix E   List of Abbreviations
Annex **B**   System Technical Specification and System Technical Specification Table
Annex **C**   Basis of Payment
Annex **D**   Security Requirements Check List
Annex **E**   DND 626, Task Authorization Form
Annex **F**   Intellectual Property Strategy
Annex **G**   Reference Terminology

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

PART 1 - GENERAL INFORMATION

1. Introduction

The bid solicitation document 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, if applicable, and the basis of selection;

Part 5   Certifications: includes the certifications to be provided;

Part 6   Security and Financial 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 annexes include the Statement of Work, System Technical Specification, the Basis of Payment, Security Requirements Check List, DND 626, Task Authorization Form, Intellectual Property Strategy and Reference Terminology.

2. Summary

The Defence Research and Development Canada (DRDC) has a requirement for design, development, demonstration and testing of automated computer network defence technology. This requirement of the Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) project contains two components: the Basic Requirement and the Optional Services Requirement. The Basic Requirement includes delivery of Research and Development (R&D) services and prototype systems to demonstrate computer network defence (CND) concepts on an operational segment of the Defence Research Establishment Network (DREnet) for potential future use by the Department of National Defence (DND). The Optional Services Requirement includes delivery of additional R&D services and supporting software to further develop the prototype system delivered under the Basic Requirement and may include integration of project results into an Initial Operational Capability.

The DRDC ARMOUR TD project has the following objectives:

1.   Demonstrate an Automated Computer Network Defence system that will:
   · Compute defensive courses of action in response to identified vulnerabilities and attacks.
   · Prioritize defensive courses of action to minimize impact to operations, and costs.
   · Proactively and reactively respond by effectuating courses of action in a semi-automated (requiring operator intervention) or fully-automated manner (not requiring any operator intervention).
   · Compute system security metrics over the enterprise wide system to enable comparison of previous and potential network states.

2.   Provide a software based Integration Framework that will:
   · Influence external CND programs and easily exploit innovations by providing a system for ongoing research and development that is shared with allies, research institutions, academia and commercial industry.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

The period of the contract is 42 months, or less than 42 months if proposed in the winning Bidder's Bid, to complete the Basic Requirement. The Optional Services Requirement may be exercised at any time after contract award and before contract expiry. If exercised, the Contractor grants to Canada the irrevocable option to extend the period of the Contract by 3 additional 2 year periods in accordance with the terms and conditions of the Contract for the Optional Services Requirement only.

There is a security requirement associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. Bidders should consult the "Security Requirements for PWGSC Bid Solicitations - Instructions for Bidders" (http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-eng.html#a31) document on the Departmental Standard Procurement Documents Web site.

Pursuant to section 01 of Standard Instructions 2003 and 2004, Bidders must submit a complete list of names of all individuals who are currently directors of the Bidder. Furthermore, as determined by the Special Investigations Directorate, Departmental Oversight Branch, each individual named on the list may be requested to complete a Consent to a Criminal Record Verification form.

The requirement is subject to the provisions of the Agreement on Internal Trade (AIT).

The requirement is subject to a preference for Canadian goods and/or services.

This procurement is subject to the Controlled Goods Program.

3. Debriefings

After contract award, 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 of receipt of the results of the bid solicitation process. The debriefing will be in writing.

4. Conflict of Interest

The Work described herein and the deliverable items under any resulting Contract specifically exclude the development of any statement of work, evaluation criteria or any document related to a bid solicitation. The Contractor, its subcontractor(s) or any of their agent(s) directly or indirectly involved in the performance of the Work and/or in the production of the deliverables under any resulting Contract will not be precluded from bidding on any potential future bid solicitation related to the production or exploitation of any concept or prototype developed or delivered under any resulting Contract.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

PART 2 - BIDDER INSTRUCTIONS

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* (http://sacc.pwgsc.gc.ca/sacc/index-e.jsp) Manual issued by Public Works and Government Services Canada.

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 (2012-11-19) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: sixty (60) days
Insert: one hundred eighty (180) days

2.   Submission of Bids

Bids must be submitted only to Public Works and Government Services Canada (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 to PWGSC will not be accepted.

3.   Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than ten (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 questions or may request that the Bidder do so, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all bidders. Enquiries not submitted in a form that can be distributed to all bidders may not be answered by Canada.

4.   Applicable Laws

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

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.

5.   Bidder's Conference

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

Canada is willing to host a Bidder's Conference in Ottawa the week of March 18, 2013, if there is sufficient demand from industry. Bidder's are requested to indicate their desire for a Bidder's Conference to the Contracting Authority on, or before March 6, 2013.

6.   DRDC Software Module Demonstration and Graph Processing

DRDC will be providing an in person demonstration of their supporting research and technology which may be used in the performance of the Work.

Demonstration of the software modules will be conducted in Ottawa on March 5, 2013.

Bidders who wish to attend the demonstration must communicate with the Contracting Authority no later than seven (7) calendar day(s) before the scheduled demonstration to confirm attendance and provide the name(s) of the person(s) who will attend. On confirmation of attendance, the Contracting Authority will provide the Bidder with the specific time and location of the demonstration. Bidders who do not confirm attendance and provide the name(s) of the person(s) who will attend as required will not be allowed access to the demonstration. Bidders will be requested to sign an attendance form. Bidders who do not attend the demonstration will not be precluded from submitting a bid.

Any clarifications or changes to the bid solicitation resulting from the demonstration will be included as an amendment to the bid solicitation.

Processing of Bidder provided graphs by AssetRank and COADS
The Bidder may submit an AND/OR graph to the DRDC ARMOUR TD team for processing by the DRDC developed processing modules AssetRank and COADS graph analysis systems. The ARMOUR TD team will make an effort to process and return the results of all graphs submitted in order of their submission to DRDC. Any Bidder who uses the results of any processed graph received from Canada to determine a technical solution does so at the Bidder's sole discretion. As a result, Canada is not responsible for any use of the results by the Bidder in the Bidder's developement of their proposal or any interpretations or assumptions made by the Bidder regarding the functionality, performance or capability of the analysis systems. Also, Canada will not extend the soliciation period for any purposes related to the of processing submitted graphs. The following list details the reasonable limits established for this effort:

- All submitted graphs must adhere to the described submission guidelines.
- Any single graph that exceeds a 24 hours processing time will be halted.
- Any reasonable number of graphs may be submitted at one time with a maximum of 100 graphs accepted.
- Graphs are to be submitted via email to ARMOUR_TDP@drdc-rddc.gc.ca
- Graphs must be submitted no later than 7 calendar days before date of bid closing

Any graphs submissions which fall outside these limitations will be returned with an explanation of the issue. Bidders may adjust and resubmit their graph if needed.

Submission Guidelines:

Each submitted graph must include:

   1) A Python application file (.py) intended to process the graph using the AssetRank and COADS library. The Python application should be based on the AssetRank and COADS samples.

      Bidders should review the AssetRank and COADS 0.3 API documentation and sample package for more information on how to load supported graph Comma Separated Value (CSV) files, implement graph ranking, course of action computation, export results, and visualize graph data:

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv

Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

https://partners.drdc-rddc.gc.ca/centres/Ottawa/NIO/ARMOUR_TD/rfp/Shared%20Documents/drdc_assetrank_and_coads_documentation_0.3.zip

The Python application source code and resulting output will be reviewed by the ARMOUR TD team and the submission will be rejected if any of the following criteria is violated:

a) Collection of system data other than CPU, memory, Python and loaded module versions;.

b) Modification of the test system environment;

c) Creation of files which are not graph related;

d) All logging must be to standard out;

e) Python modules which are not related to graph processing; or

f) Any other item contained in the source code or resulting output that is deemed, at DRDC's sole discretion, to be of harm to Canada or Canada's information systems; or not necessary for assessment of the analysis systems.

Each Python application will be executed using cProfile and the summary function call time will be used to determine overall processing time. The detailed function call names and timing will not be included.

2) AssetRank and COADS supported graph arcs and vertices in separate CSV (Comma Separated Value) format files.

Execution:

The Python application file will be executed and all output saved to an output.txt file in the same directory. If multiple Python application files are present for a single graph sub-directory, the output from each will be appended to the same output.txt file.

The ARMOUR TD team will make a best effort to ensure the Python application can execute successfully and reserve the right to modify the application code in order to do so. All execution results and necessary changes will be communicated to the submitter.

Packaging:

For each graph, the required files should be organized in their own sub-directory within a zip file. The zip filename must be prefixed with the submitter's name. The following is the organization of a sample submission:

```
companyA_graphs_2012-12-21.zip
    ./graph1a/
        ./VERTICES.CSV
        ./ARCS.CSV
        ./graph1a_budget10_BestFirstSearch.py
        ./graph1a_budget100_BestFirstSearch.py
    ./graph1b/

        ./VERTICES.CSV
        ./ARCS.CSV
```

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

./graph1b_budget1000_BestFirstSearch.py

The resulting processed package returned to submitter will be identical in organization, with the addition of the execution output file for each graph sub-directory.

7. Applicable and Reference Documentation

The following documents are available for download at the DRDC sharepoint site:

·   ARMOUR TD System Technical Specification v2.0, DRDC Ottawa, 18 January 2013 (Annex B)

·   ARMOUR TD System Technical Specification Table v2.0, DRDC Ottawa, 18 January 2013 (Annex B)

·   ARMOUR TD Supporting Research and Technology Presentation, DRDC Ottawa, November 2012

·   DRDC AssetRank and COADS Documentation, DRDC Ottawa

·   DRDC GENESIS Promotional Video, DRDC Ottawa

·   DRDC GENESIS Trend Micro Architecture, DRDC Ottawa

·   DRDC SPADE Technical Report Documents, DRDC Ottawa

·   Certification and Accreditation Guide v1.4, DND, December 2006

The DRDC sharepoint site is located at the following link: https://partners.drdc-rddc.gc.ca/centres/Ottawa/NIO/ARMOUR_TD/rfp/Shared%20Documents

Bidders are requested to contact the Contracting Authority for the required login credentials to access the DRDC sharepoint site.

8. Ownership of Intellectual Property

Defence Research and Development Canada has determined that any intellectual property rights arising from the performance of the Work under the resulting contract for the following items will belong to the Contractor:
·   Data source connectors
·   Effector connectors
·   Plugins to the Computational Services component (CND processing modules)
·   Plugins to the Database component (Database modules)
·   Plugins to the Data Presentation component (Data Presentation modules)

Any intellectual property rights arising from the performance of the Work under the resulting contract will belong to Canada, excluding the items listed above which belong to the Contractor.

The Department of National Defence has determined that any intellectual property rights arising from the performance of the Work under the resulting contract will belong to Canada, on the following grounds:

a.   the main purpose of the contract, or of the deliverables contracted for, is to generate knowledge and information for public dissemination; and

b.   to deliver a component or subsystem that will be incorporated into a complete system at a later date (not necessarily by the original Contractor), as a prerequisite to the planned transfer of the complete

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

system to the private sector (not necessarily to the original Contractor), through licensing or assignment of ownership, for the purposes of Commercial Exploitation.

Bidder's are advised that DRDC intends to distribute, via a Research License, the entire turnkey ARMOUR system, Code Repository, and access to the necessary Background Intellectual Propery to use the turnkey ARMOUR system delivered to DRDC under the Basic Requirement for non-operational research purposes only.

For greater certainty:

The ARMOUR system may be distributed via a Research License at no cost to the following entities, including but not limited to, industry, academia, research institutions and allies for research purposes only;

The turnkey ARMOUR system to be distributed by DRDC includes any of the delivered versions of the Software and Documentation in SD 007: System Hardware, Software and Documentation accepted by Canada. The delivered versions that may be distributed include any or all of the following: Initial Version, Final Version, and Iterations at the end of each phase;

The Research Licenses will also permit the Licensee access to DM 004: Code Repository;

The only source code distributed by DRDC will be the source code for Canada owned Foreground Intellectual Propetery contained in the turnkey ARMOUR System; and

All software components, including Contractor and third-party owned components, incorporated into the turnkey ARMOUR system, must maintain a functionality equivalent to the system delivered to DRDC for each entity testing the system under a Research License and for the duration of the Research License at no additional cost to DRDC or the Research Licensee.

9. Maximum Funding

9.1 Maximum Funding for Basic Requirement

The maximum funding available for the Basic Requirement of the contract resulting from the bid solicitation is $4,400,000.00 CAD, GST/HST extra. Bids with a Basic Requirement valued in excess of this amount will be considered non-responsive. This disclosure does not commit Canada to pay the maximum funding available.

9.2 Maximum Funding for the Optional Services Requirement

The maximum funding available for the Optional Services Requirement of the contract resulting from the bid solicitation is $9,550,000.00 CAD, GST/HST extra. Bids with a Optional Services Requirement valued in excess of this amount will be considered non-responsive. This disclosure does not commit Canada to pay the maximum funding available.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

PART 3 - BID PREPARATION INSTRUCTIONS

1.   Bid Preparation Instructions

Canada requests that bidders provide their bid in separately bound sections as follows:

Section I :   Technical Bid (4 hard copies) and one (1) soft copy on CD or DVD.

Section II :   Financial Bid (2 hard copies)

Section III :   Certifications (2 hard copies)

If there is a discrepancy between the wording of the soft copy and the hard copy, the wording of the hard copy will have priority over the wording of the soft copy.

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

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 (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, bidders are encouraged to:

(1)   use paper containing fibre certified as originating from a sustainably-managed forest and/or containing minimum 30% recycled content; and

(2)   use an environmentally-preferable format including black and white printing instead of colour prinnting, print double sided/duplex,using staples or clips instead of cerlox, duotangs 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 clearly address 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.

Section II : Financial Bid

1.1   The financial bid preparation instructions are included in Attachment 1, Financial Bid Preparation Instructions.

1.2   **SACC Manual Clauses**

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

C3011T (2010-01-11), Exchange Rate Fluctuation

Section III : Certifications

Bidders must submit the certifications required under Part 5.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv

Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

1.   Evaluation Procedures

(a)   Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria.

(b)   An evaluation team composed of representatives of Canada and AEPOS Technologies Inc. will evaluate the bids.

(c)   The evaluation team will determine first if there are three (3) or more bids with a valid Canadian Content certification. In that event, the evaluation process will be limited to the bids with the certification; otherwise, all bids will be evaluated. If some of the bids with a valid certification are declared non-responsive, or are withdrawn, and less than three responsive bids with a valid certification remain, the evaluation will continue among those bids with a valid certification. If all bids with a valid certification are subsequently declared non-responsive, or are withdrawn, then all the other bids received will be evaluated.

1.1   Technical Evaluation

Except where expressly provided otherwise, the experience described in the bid must be the experience of the Bidder itself (which includes the experience of any companies that formed the Bidder by way of a merger but does not include any experience acquired through a purchase of assets or an assignment of contract). The experience of the Bidder's affiliates (i.e. parent, subsidiary or sister corporations), subcontractors, or suppliers will not be considered.

1.1.1   Mandatory Technical Criteria
Refer to Attachment 4, Mandatory and Point Rated Technical Criteria.

1.1.2   Point Rated Technical Criteria
Refer to Attachment 4, Mandatory and Point Rated Technical Criteria.

1.2   Evaluation of Price

The price of the bid will be evaluated in Canadian dollars, the Goods and Services Tax or the Harmonized Sales Tax excluded; FOB destination, Canadian customs duties and excise taxes included.

For evaluation purposes only, the price of the bid will be determined as detailed in Attachment 3 Evaluation of Price.

SACC Manual Clause A0222T (2010-01-11), Evaluation of Price

2.   Basis of Selection - Highest Total Point Score

1.   To be considered compliant a proposal must:

(a) comply with all the requirements of the bid solicitation;

(b) meet all Mandatory Evaluation Criteria;

(c) obtain the required minimum points for each criterion with a pass mark;

(d) obtain the required overall minimum points for the Point Rated Technical, Management and Corporate Experience Evaluation Criteria;

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

(e) be within the stipulated maximum budget for the Basic Requirement as stated in Attachment 3 Evaluation of Price, Item 1;

(f) be within the stipulated maximum budget for the firm per diem rates and mark-up on hardware and software as stated in Attachment 3 Evaluation of Price, Item 2 and

(g) obtain a point rated evaluation score for the Architectural Design Document (Section 1.0 of the Attachment 4 Point Rated Evaluation Criteria) within 6 points of the top ranked Architectural Design Document point rated evaluation score.

2. Bids not meeting (a) or (b) or (c) or (d) or (e) or (f) or (g) will be declared non-responsive.

3. The evaluation will be based on the highest total point score of technical merit, price and Canadian Content.

4. To establish the technical merit score, the overall technical score acheived for the Point Rated Technical, Management and Corporate Experience Evaluation Criteria will be the technical merit score.

5. To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and multiplied by a factor of 20.

6. To establish the Canadian Content score, each responsive bid will be assigned one score for goods and one score for services in accordance with Table 1 below. The sum of the score for goods and the score for services will be the Canadian Content score.

Table 1

Canadian Content	Certified Canadian Content	Points for Canadian Content
Goods	20.00% of Goods are Canadian Goods	0
	40.00% of Goods are Canadian Goods	1
	60.00% of Goods are Canadian Goods	2
	80.00% of Goods are Canadian Goods	3
	100.00% of Goods are Canadian Goods	4
Services	80.00% of Services are Canadian Services	0
	90.00% of Services are Canadian Services	5
	100.00% of Services are Canadian Services	10

7. For each responsive bid the technical merit score, the pricing score, and the Canadian Content score will be added to determine its Total Point Score.

8. Neither the responsive bid that receives the highest number of points for the Point Rated Evaluation Criteria, nor the one that proposed the lowest price will necessarily be accepted. Instead the bidder with the Highest Total Point Score will be recommended for award of a contract. In the event that two or more responsive bids achieve the same Highest Total Point Score, the responsive bid which obtained the highest number of points for the Architectural Design Document point rated evaluation criteria will be recommended for award of a contract.

Table, Example 1, below illustrates an example where all three bids are responsive and the selection of the contractor is determined by the Total Point Score. The total available technical merit point available equals 135 and the lowest evaluated price is $60,000.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

Example 1

		Bidder		
		Bidder 1	Bidder 2	Bidder 3
Overall Technical Score		130	125	110
Evaluated Bid Price		$77,000	$75,000	$60,000
Canadian Content Score	**Goods**	1	2	4
	Services	5	0	10
Calculations				
Pricing score		60/77 x 20 = 15.6	60/75 x 20 = 16	60/60 x 20 = 20
Total Point Score		130 + 15.6 + 1 + 5 = 151.6	125 + 16 + 2 + 0 = 143	110 + 20 + 4 + 10 = 144
Overall Ranking		**1 st**	**3 rd**	**2 nd**

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

PART 5 - CERTIFICATIONS

Bidders must provide the required certifications to be awarded a contract. Canada will declare a bid non-responsive if the required certifications are not completed and submitted as requested.

Compliance with the certifications bidders provide to Canada is subject to verification by Canada during the bid evaluation period (before award of a contract) and after award of a contract. The Contracting Authority will have the right to ask for additional information to verify the bidders' compliance with the certifications before award of a contract. The bid will be declared non-responsive if any certification made by the Bidder is untrue, whether made knowingly or unknowingly. Failure to comply with the certifications or to comply with the request of the Contracting Authority for additional information will also render the bid non-responsive.

1   Certifications Precedent to Contract Award and Certifications Required with the Bid

1.1   Certifications Precedent to Contract Award

The certifications in Attachment 5, Certifications Precedent to Contract Award, should be completed and submitted with the bid but may be submitted afterwards. If any of these required certifications is not completed and submitted as requested, 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.

1.2   Certifications Required with the Bid

Bidders must complete and submit the certifications in Attachment 6, Certifications Required with the Bid, as part of their bid.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

PART 6 - SECURITY AND FINANCIAL REQUIREMENTS

1.   Security Requirement

1.1   At the date of bid closing, the following conditions must be met:

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

     (b)   the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirement as indicated in Part 7 - Resulting Contract Clauses;

     (c)   the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites. This information must be submitted with the bid .

1.2   For additional information on security requirements, bidders should consult the "Security Requirements for PWGSC Bid Solicitations - Instructions for Bidders" document on the Departmental Standard Procurement Documents Web site. (http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-eng.html#a31)

2.   Financial Capability

SACC Manual clause A9033T (2012-07-16), Financial Capability

3.   Controlled Goods Requirement

SACC Manual clause A9130T (2011-05-16), Controlled Goods Program

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

PART 7 - RESULTING CONTRACT CLAUSES

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

1.   Requirement

This requirement consists of two (2) components: the Basic Requirement and the Optional Services Requirement.

1.1   Basic Requirement

1.1.1   Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work at Annex A, excluding Appendix C - Optional Services Requirement, to meet the specifications contained in the System Technical Specification and System Technical Specification Table at Annex B.

1.1.2   Work Authorization

Despite any other condition of the Contract, the Contractor is only authorized to perform the Work required to complete Phases 1 and 2 of the Contract. Upon completion of Phase 2, the Work will be reviewed before the Contractor is authorized to commence any Work for Phase 3. Depending on the results of the review and evaluation of the Work, Canada will decide at its discretion whether to continue with the Work.

If Canada decides to continue with Phase 3, the Contracting Authority will advise the Contractor in writing to commence work on Phase 3. The Contractor must immediately comply with the notice.

If Canada decides to continue with Phase 4, the Contracting Authority will advise the Contractor in writing to commence work on Phase 4. The Contractor must immediately comply with the notice.

If Canada decides to continue with Phase 5, the Contracting Authority will advise the Contractor in writing to commence work on Phase 5. The Contractor must immediately comply with the notice.

If Canada decides to continue with Phase 6, the Contracting Authority will advise the Contractor in writing to commence work on Phase 6. The Contractor must immediately comply with the notice.

If Canada decides not to proceed with any phase, the Contracting Authority will advise the Contractor in writing of the decision and the Contract will be considered completed at no further costs to Canada. In no event will the Contractor be paid for any cost incurred for unauthorized work.

1.2   Optional Services Requirement

The Contractor grants to Canada the irrevocable option to acquire the services described at Appendix C of the Annex A Statement of Work of the Contract, as and when requested by Canada, under the same conditions and at the prices and/or rates stated in the Contract. The option may only be exercised by the Contracting Authority and will be evidenced, for administrative purposes only, through a contract amendment.

lThe Contracting Authority may exercise the option at any time before the expiry of the Contract by sending a written notice to the Contractor.

1.2.1   Task Authorization

1.2.1.1   Task Authorization - Department of National Defence

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

The administration of the Task Authorization process will be carried out by Defence Research and Development Canada. This process includes monitoring, controlling and reporting on expenditures of the Contract with task authorizations to the Contracting Authority.

1.2.1.2   Task Authorization Process

Task Authorization:
The Work described at Appendix C of the Annex A Statement of Work to be performed under the Contract will be on an "as and when requested basis" using a Task Authorization (TA). The Work described in the TA must be in accordance with the scope of the Contract.

Task Authorization Process:

1. The Technical Authority will provide the Contractor with a description of the task using the "DND 626, Task Authorization Form" specified in Annex E.

2. The Task Authorization (TA) will contain the details of the activities to be performed, a description of the deliverables, and a schedule indicating completion dates for the major activities or submission dates for the deliverables. The TA will also include the applicable basis(bases) and methods of payment as specified in the Contract.

3. The Contractor must provide the Technical Authority, within seven (7) calendar days of its receipt, the proposed total estimated cost for performing the task and a breakdown of that cost, established in accordance with the Basis of Payment specified in the Contract.

4. The Contractor must not commence work until a TA authorized by the Technical Authority has been received by the Contractor. The Contractor acknowledges that any work performed before a TA has been received will be done at the Contractor's own risk.

1.2.1.3   Task Authorization Limit

The Technical Authority may authorize individual task authorizations up to a limit of $100,000.00, Goods and Services Tax or Harmonized Sales Tax included, inclusive of any revisions.

Any task authorization to be issued in excess of that limit must be authorized by the Technical Authority and Contracting Authority before issuance.

1.2.1.4 Periodic Usage Reports - Contracts with Task Authorizations

The Contractor must compile and maintain records on its provision of services to the federal government under authorized Task Authorizations issued under the Contract.

The Contractor must provide this data in accordance with the reporting requirements detailed below. If some data is not available, the reason must be indicated. If services are not provided during a given period, the Contractor must still provide a "NIL" report.

The data must be submitted on a quarterly basis to the Contracting Authority.

The quarterly periods are defined as follows:

1st quarter: April 1 to June 30;
2nd quarter: July 1 to September 30;
3rd quarter: October 1 to December 31; and

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

4th quarter: January 1 to March 31.

The data must be submitted to the Contracting Authority no later than 30 calendar days after the end of the reporting period.

Reporting Requirement - Details

A detailed and current record of all authorized tasks must be kept for each contract with a task authorization process. This record must contain:

For each authorized task:
(i)   the authorized task number or task revision number(s);
(ii)   a title or a brief description of each authorized task;
(iii)   the total estimated cost specified in the authorized Task Authorization (TA) of each task, GST or HST extra;
(iv)   the total amount, GST or HST extra, expended to date against each authorized task;
(v)   the start and completion date for each authorized task; and
(vi)   the active status of each authorized task, as applicable.

For all authorized tasks:

i.   the amount (GST or HST extra) specified in the contract as Canada's total liability to the contractor for all authorized TAs; and
ii. the total amount, GST or HST extra, expended to date against all authorized TAs.

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_ (http://ccua-sacc.tpsgc-pwgsc.gc.ca/pub/acho-eng.jsp) _Manual_ issued by Public Works and Government Services Canada.

2.1   General Conditions

2040 (2012-11-19), General Conditions - Research & Development, apply to and form part of the Contract.

The text under Subsection 1 of Section 29 Ownership of Intellectual Property Rights in Foreground Information of 2040 referenced above is replaced by the following:

Intellectual Property Rights in the Foreground Information for the following items belong to the Contractor as soon as the come into existence:
·   Data source connectors;
·   Effector connectors;
·   Plugins to the Computational Services component (CND processing modules);
·   Plugins to the Database component (Database modules); and
·   Plugins to the Data Presentation component (Data Presentation modules)

2.2   Supplemental General Conditions

The following supplemental general conditions apply to and form part of the Contract:

4001 (2010-08-16), Hardware Purchase, Lease or Maintenance
4002 (2010-08-16), Software Development or Modification Services

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

4003 (2010-08-16), Licensed Software
4004 (2010-08-16), Maintenance and Support Services for Licensed Software

2.3 SACC Manual Clauses

Not withstanding any other clause of the Contract, Canada will own all Intellectual Property Rights in Foreground Information in accordances with SACC Manual Clause K3410C (2008-12-12), Canada to Own Intellectual Property Rights in Foreground Information.

SACC Manual Clause K3415C (2008-05-12), Commerialization in Canada

2.4 Protection and Security of Data Stored in Databases

1   The Contractor must ensure that all the databases containing any information related to the Work are located in Canada or, if the Contracting Authority has first consented in writing, in another country where:

(a) equivalent protections are given to personal information as in Canada under legislation such as the Privacy Act, R.S. 1985, c. P-21, and the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, and under any applicable policies of the Government of Canada; and

(b) the laws do not allow the government of that country or any other entity or person to seek or obtain the right to view or copy any information relating to the Contract without first obtaining the Contracting Authority's written consent.

In connection with giving its consent to locating a database in another country, the Contracting Authority may, at its option, require the Contractor to provide a legal opinion (from a lawyer qualified in the foreign country) that the laws in that country meet the above requirements, or may require the Contractor to pay for Canada to obtain such a legal opinion. Canada has the right to reject any request to store Canada's data in a country other than Canada if there is any reason to be concerned about the security, privacy, or integrity of Canada's data. Canada may also require that any data sent or processed outside of Canada be encrypted with Canada-approved cryptography and that the private key required to decrypt the data be kept in Canada in accordance with key management and storage processes approved by Canada.

2   The Contractor must control access to all databases on which any data relating to the Contract is stored so that only individuals with the appropriate security clearance are able to access the database, either by using a password or other form of access control such as biometric controls.

3   The Contractor must ensure that all databases on which any data relating to the Contract is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases, unless those databases are located in Canada (or in an another country approved by the Contracting authority under subsection 1) and otherwise meet the requirements of this article.

4   The Contractor must ensure that all data relating to the Contract is processed only in Canada or in another country approved by the Contracting Authority under subsection 1.

5   The Contractor must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada, unless the Contracting Authority has first consented in writing to an alternate route. The Contracting Authority will only consider requests to route domestic traffic through another country that meets the requirements of subsection 1.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

6   Despite any section of the General Conditions relating to subcontracting, the Contractor must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the Contract unless the Contracting Authority first consents in writing.

3.   Security Requirement

1. The Contractor must, at all times during the performance of the Contract, hold a valid Facility Security Clearance at the level of SECRET, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).

2. This contract includes access to controlled goods. Prior to access, the contractor must be registered in the Controlled Goods Program of Public Works and Government Services Canada.

3. The Contractor personnel requiring access to PROTECTED/CLASSIFIED information, assets or sensitive work site(s) must EACH hold a valid personnel security screening at the level of RELIABILITY or SECRET, as required, granted or approved by CISD/PWGSC.

4. The Contractor MUST NOT remove any PROTECTED/CLASSIFIED information from the identified work site(s), and the Contractor must ensure that its personnel are made aware of and comply with this restriction.

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

6. The Contractor must comply with the provisions of the:

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

4.   Term of Contract

4.1   Period of Contract

The period of the Contract is (insert at contract award: 42 months **or** a period less than 42 months as stated in the Bidder's Proposal) from date of the Contract award, inclusive.

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 three (3) additional two (2) year period(s) under the same conditions for the Optional Services Requirement. 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 for the Optional Services Requirement.

Canada may exercise this option at any time by sending a written notice to the Contractor at least 30 calendar days prior to the Contract expiry date. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

5.   Authorities

5.1   Contracting Authority

The Contracting Authority for the Contract is:

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv

Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

Peter Murray
Public Works and Government Services Canada
Acquisitions Branch
Science Procurement Directorate
Place du Portage, Phase III, 11C1
11 Laurier Street
Gatineau, Quebec
K1A 0S5

Telephone: 819-956-1387
Facsimile: 819-997-2229
E-mail address: Peter.Murray@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.

5.2   Technical Authority

The Technical Authority for the Contract is:

Name : (TBD)
Title :   _____
Organization :   _____
Address :   _____

Telephone: ___ ___ _____
Facsimile: ___ ___ _____
E-mail address: _____

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.

5.3   Contractor's Representative
(TBD)

5.4   Procurement Authority

The Procurement Authority for the Contract is:

Name : (TBD)
Title :   _____
Organization :   _____
Address :   _____

Telephone: ___ ___ _____
Facsimile: ___ ___ _____
E-mail address: _____

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

The Procurement Authority is the representative of the department or agency for whom the Work is being carried out under the Contract. The Procurement Authority is responsible for the implementation of tools and processes required for the administration of the Contract. The Contractor may discuss administrative matters identified in the Contract with the Procurement Authority however the Procurement Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of Work can only be made through a contract amendment issued by the Contracting Authority.

6.   Payment

6.1   Basis of Payment (Basic Requirement)

For the Work described in Statement of Work in Annex A (excluding Appendix C):

In consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid a firm, all inclusive lot price, as specified in Section 1. Basic Requirement of the Basis of Payment in Annex C for a cost of $_____ (insert the amount at contract award). Customs duties are included and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

For the firm, all inclusive lot price portion of the Work only, 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.

6.2   Basis of Payment (Optional Services Requirement APPENDIX C TO ANNEX A)

For the Work described in APPENDIX C of the Statement of Work in Annex A:

The following type of basis of payment will form part of the approved Task Authorization (TA). The task price must be determined in accordance with Section 2. Optional Service Requirement of the Basis of Payment in Annex C.

(a)   Firm Lot Price TA

In consideration of the Contractor satisfactorily completing all of its obligations under the authorized Task Authorization (TA), the Contractor will be paid the firm, all inclusive lot price of $ _____ in accordance with the Basis of Payment, in Annex C, as specified in the authorized TA. Customs duties are included and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

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

(b)   Ceiling Price TA

The Contractor will be reimbursed its costs reasonably and properly incurred in the performance of the Work, plus a fixed fee or a profit as determined in accordance with the Basis of Payment in Annex C, to the ceiling price specified in the approved TA. Customs duties are included and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

The ceiling price is subject to downward adjustment so as not to exceed the actual costs reasonably incurred in the performance of the Work and computed in accordance with the Basis of Payment.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

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 Technical Authority Contracting Authority as applicable before their incorporation into the Work.

(c)   TA subject to a Limitation of Expenditure

The Contractor will be reimbursed for the costs reasonably and properly incurred in the performance of the Work specified in the authorized Task Authorization (TA), as determined in accordance with the Basis of Payment Annex C, to the limitation of expenditure specified in the authorized TA.

Canada's liability to the Contractor under the authorized TA must not exceed the limitation of expenditure specified in the authorized TA. Customs duties are included and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

No increase in the liability of Canada or in the price of the Work specified in the authorized TA 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 authorized, in writing, by the Contracting Authority before their incorporation into the Work.

6.2.1   Canada's Obligation - Portion of the Work - Task Authorizations

Canada's obligation with respect to the portion of the Work under the Contract that is performed through task authorizations is limited to the total amount of the actual tasks performed by the Contractor.

6.2.2   Total Limitation of Expenditure - Cumulative Total of all Task Authorizations

1.   Canada's total liability to the Contractor under the Contract for all authorized Task Authorizations (TAs), inclusive of any revisions, must not exceed the sum of $ _____**(to be inserted at time option is exercised)**. Customs duties are included and the Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

2.   No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.

3.   The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:
      (a)   when it is 75 percent committed, or
      (b)   four (4) months before the contract expiry date, or
      (c)   as soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized TAs, inclusive of any revisions,

      whichever comes first.

4.   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.

6.3   Method of Payment (Basic Requirement)

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Contract and the payment provisions of the Contract if:

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

A.) an accurate and complete claim for payment using PWGSC-TPSGC 1111, 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;

B.) all the certificates appearing on form PWGSC-TPSGC 1111 have been signed by the respective authorized representatives;

C.) all work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada.

6.3.1   Schedule of Milestones

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

Milestone #	Project Phase	Milestone Description	% of Basic Requirement	$ Value
1	Phase 1	Preliminary Design Review Meeting (Phase 2 approval)	8%	
2	Phase 2	Critical Design Review Meeting	2%	
3	Phase 2	Readiness Review Meeting (Phase 3 approval)	14%	
4	Phase 3	Critical Design Review Meeting	5%	
5	Phase 3	First Demonstration Completion	10%	
6	Phase 3	Readiness Review Meeting	7%	
7	Phase 4	Critical Design Review Meeting	5%	
8	Phase 4	Second Demonstration Completion	10%	
9	Phase 4	Readiness Review Meeting	7%	
10	Phase 5	Critical Design Review Meeting	5%	
11	Phase 5	Third Demonstration Completion	10%	
12	Phase 5	Readiness Review Meeting	7%	
13	Phase 6	Final Review Meeting	10%	

6.4   Method of Payment (Optional Services Requirement)

6.4.1   Payments will be made not more frequently than once a month.

6.4.2   Depending on the method of payment specified in the applicable TA, one of the following method of payment clauses will apply.

6.4.2.1 Single Payment

Canada will pay the Contractor upon completion and delivery of the Work in accordance with the payment provisions of the Task Authorization and the Contract if:

(a)   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;

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

(b)   all such documents have been verified by Canada;

(c)   the Work delivered has been accepted by Canada.

6.4.2.2   Milestone Payments   (For a Firm Price TA)

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Task Authorization and the payment provisions of the Contract if:

(a)   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;

(b)   all work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada.

6.4.2.3   Monthly Payments   (For a TA subject to a Limitation of Expenditure or a Ceiling Price)

Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Task Authorization and the Contract if:

(a)   an accurate and complete invoice and any other documents required by the Task Authorization and the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

(b)   all such documents have been verified by Canada;

(c)   the Work performed has been accepted by Canada.

6.5   SACC Manual Clauses

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

C2000C (2007-11-30), Taxes - Foreign-based Contractor

C0305C (2008-05-12), Cost Submission

C2605C (2008-05-12), Canadian Customs Duties and Sales Tax - Foreign-based Contractor

6.6   Discretionary Audit

SACC Manual Clause C0705C (2010-01-11), Discretionary Audit

6.7   Time Verification

SACC Manual Clause C0711C (2008-05-12), Time Verification

7.   Invoicing Instructions

7.1   Basic Requirement.

1.   The Contractor must submit a claim for payment using form PWGSC-TPSGC 1111, Claim for Progress

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

Payment.

Each claim must show:
a.   All information required on form PWGSC-TPSGC 1111;
b.   All applicable information detailed under the section entitled "Invoice Submission" of the general conditions;
c.   The description and value of the milestone claimed as detailed in the Contract.

2.   Goods and Services Tax (GST) of Harmonized Sales Tax (HST), as applicable, must be calculated on the total amount of the claim.

3.   The Contractor must prepare and certify an original claim on form PWGSC-TPSGC 1111, and forward it to the Contracting Authority for certification in an electronic format to the electronic mail address identified under section entitled "Authorities" of the Contract. Adobe Reader (.pdf) format is acceptable. The Contracting Authority will then forward the certified claim, in an electronic format, to the Technical Authority for appropriate certification after inspection and acceptance of the Work takes place, and onward submission to the Payment Office for the remaining certification and payment.

4.   The Contractor must not submit claims until all work identified in the claim is completed.

7.2   Task Authorizations - Optional Services Requirement

1. The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions. The invoice must show the Task Authorization (TA) number and, as applicable, the description of the milestone invoiced. Invoices cannot be submitted until all work identified on the invoice is completed.

2.   For TAs subject to a Limitation of Expenditure or a Ceiling Price, each invoice must be supported by:

(a)   a list of all expenses, in accordance with the TA;
(b)   a copy of time sheets to support the time claimed;
(c)   a copy of the release document and any other document(s) as specified in the Contract;
(d)   a copy of the invoices, receipts, vouchers for all direct expenses, travel and living expenses;
(e)   a copy of the monthly progress report.

3.   Invoices must be distributed as follows:

(a)   the original and one (1) copy must be forwarded to the address shown on page 1 of the Contract for certification and payment; and

(b)   one (1) copy must be forwarded to the Contracting Authority.

8.   Certifications

8.1   Compliance with the certifications provided by the Contractor in its bid is a condition of the Contract and subject to verification by Canada during the entire contract period. If the Contractor does not comply with any certification or it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

8.2   SACC Manual Clauses

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

A3060C (2008-05-12), Canadian Content Certification

9. Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in _____ (to be inserted at contract award).

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)   4001 (2010-08-16), Hardware Purchase, Lease or Maintenance
(c)   4002 (2010-08-16), Software Development or Modification Services
(d)   4003 (2010-08-16), Licensed Software
(e)   4004 (2010-08-16), Maintenance and Support Services for Licensed Software
(f)   the General Conditions - Research & Development 2040 (2012-11-19),
(g)   Annex A, Statement of Work;
(h)   Annex B, System Technical Specifications and associated System Technical Specifications Table;
(i)   Annex C, Basis of Payment;
(j)   Annex D, Security Requirements Check List;
(k)   the signed Task Authorizations (including all of its annexes, if any);
(l)   the Contractor's bid dated _____   (If the bid was clarified or amended, insert at the time of contract award: "as clarified on _____".

11. Defence Contract

SACC Manual clause A9006C (2012-07-16), Defence Contract

12. Foreign Nationals (Canadian Contractor)

SACC Manual clause A2000C (2006-06-16), Foreign Nationals (Canadian Contractor)

OR

12. Foreign Nationals (Foreign Contractor)

SACC Manual clause A2001C (2006-06-16), Foreign Nationals (Foreign Contractor)

13. Insurance

SACC Manual clause G1005C (2008-05-12), Insurance

14. Controlled Goods Program

14.1   SACC Manual clause A9131C (2011-05-16), Controlled Goods Program
14.2   SACC Manual clause B4060C (2011-05-16), Controlled Goods

15. Site Regulations

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

The Contractor must comply with all standing orders or other regulations, instructions and directives in force on the site where the Work is performed.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

ATTACHMENT 1

FINANCIAL BID PREPARATION INSTRUCTIONS

1.1   Bidders must submit their financial bid in accordance with the following :

(a)   A Firm All Inclusive Lot Price in for the Basic Requirement, as described in Annex A, Statement of Work, excluding Appendix C, not exceeding $4,400,000.00 CAD, GST/HST excluded, FOB Destination (for goods), all applicable customs duty and excise taxes included.

The total amount of Goods and Services Tax or Harmonized Sales Tax is to be shown separately, if applicable.

(b)   Firm all-inclusive hourly rates for each category of resources listed in Attachment 2 FINANCIAL BID PRESENTATION SHEET for the Optional Services Requirement as outlined in Appenidx C of the Annex A, Statement of Work.

The Firm all-inclusive rates are subject to escalation in accordance with Section 2.1.1 of the Basis of Payment in Annex C.

(c)   Firm mark-up on hardware and software procured under the Optional Services Requirement as outlined in Appendix C of the Annex A, Statement of Work.

(d)   The total evaluated value of the Optional Services Requirement, labour and mark-up, must not exceed $9,550,000.00 CAD GST/HST excluded, FOB Destination (for goods), all applicable customs duty and excise taxes included.

(e)   The total amount of Goods and Services Tax or Harmonized Sales Tax is to be shown separately, if applicable.

(f)   For Canadian-based bidders, prices must be in Canadian funds, Canadian customs duties and excise taxes included, and Goods and Services Tax (GST) or Harmonized Sales Tax (HST) excluded.

For foreign-based bidders, prices must be in Canadian funds, Canadian customs duties and excise taxes and GST or HST excluded. Canadian customs duties and excise taxes payable by Canada will be added, for evaluation purposes only, to the prices submitted by foreign-based bidders.

For the purpose of the bid solicitation, bidders with an address in Canada are considered Canadian-based bidders and bidders with an address outside of Canada are considered foreign-based bidders.

1.1.1   Price Breakdown

Bidders are requested to detail the following elements for each phase of the Basic Requirement of the Work, as applicable:

(a)   Labour : For each individual and (or) labour category to be assigned to the Work, indicate: i) the hourly rate, inclusive of overhead and profit; and ii) the estimated number of hours.

The labour categories are expected to be common between the Basic Requirement and the Optional Services Requirement. The hourly rate, inclusive of overhead and profit, will be used to validate the rates

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

proposed for the labour categories listed in Attachment 2 FINANCIAL BID PRESENTATION SHEET for the Optional Services Requirement.

(b)   Equipment : Specify each item required to complete the Work and provide the pricing basis of each one, Canadian customs duty and excise taxes included, as applicable. These items will be deliverable to Canada upon completion of the contract.

(c)   Materials and Supplies : Identify each category of materials and supplies required to complete the Work and provide the pricing basis.

(d)   Travel and Living Expenses :   Indicate the number of trips and the number of days for each trip, the cost , destination and purpose of each journey, together with the basis of these costs.

(e)   Subcontracts : Identify any proposed subcontractor and provide for each one the same price breakdown information as contained in this article.

(f)   Other Direct Charges : Identify any other direct charges anticipated, such as long distance communications and rentals, and provide the pricing basis .

(g)   GST/HST : Identify any applicable GST or HST separately.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

ATTACHMENT 2
FINANCIAL BID PRESENTATION SHEET

1. Firm, all inclusive, lot price for the Basic Requirement

Table 1

Item	Firm All Inclusive Lot Price
Basic Requirement as described in Annex A (excluding Appendix C)	

Bidders may propose a Milestone Schedule for the Basic Requirement that reflects a neutral cashflow. The Bidder's proposed Milestone Schedule should be substantiated by their price breakdown for the Basic Requirement.

2. Firm, all inclusive, hourly rates for the Optional Services Requirement

Table 2

Labour Category	Total Estimated Level of Effort (sum of all years) Days, based on an 8 hour work day	Firm All Inclusive Hourly Rate
Project Management		
Project Manager (PM)	1060	
Project Communications Specialist (PCS)	1000	
Project Control Officer (PCO)	260	
Webmaster (WM)	120	
System Architecture and Design		
Lead System of Systems Architect (LSA)	260	
Software Solution Architect (SSA)	260	
System/Network Analyst (SNA)	600	
Technical Writer (TW)	260	
User Interface Analyst (UIA)	265	
Hardware Architect (HA)	140	
Data Warehouse Architect (DWA)	260	
Computer Network Defence Functional Analyst (CNDFA)	260	
Information Technology Security Analyst (ITSA)	200	
Information Technology Certification and Accreditation Specialist (CAS)	540	
System Programming		
Senior Programmer (SP)	400	
Intermediate Programmer (IP)	660	
Junior Programmer (JP)	1700	
Senior Web-Services Developer (SWD)	340	
System Engineering and Operations		
Operating Systems Administrator (OSA)	180	
Project Test Coordinator (PTC)	480	
Quality Assurance Specialist (QAS)	300	
Tester (TES)	560	
Total Estimated Cost		

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

The estimated level of effort specified is only an approximation of requirements given in good faith and is provided for financial bid evaluation purposes only. It does not represent a commitment by Canada.

3.   Mark up on Hardware and Software for the Optional Services Requirement

_____ %

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

ATTACHMENT 3

EVALUATION OF PRICE

For evaluation purposes only, the price of the bid will be determined as follows:

1. Basic Requirement: The firm all inclusive lot price for the Basic Requirement as detailed in Table 1 of Attachment 2, Financial Bid Presentation Sheet.

$_____   (GST/HST extra)

2. Labour Component: The firm all inclusive hourly rate will be multiplied by a factor of 8 (8 hours in a working day) against corresponding level of effort as detailed in Table 2 of Attachment 2, Financial Bid Presentation Sheet for each resource category. The sum across all labour categories and days in Table 2 will form the total estimated price for labour for evaluation purposes.

 $_____   (GST/HST extra)

Note: The estimated level of effort specified is only an approximation of requirements given in good faith and is provided for financial bid evaluation purposes only. It does not represent a commitment by Canada.

3. MARK-UP ON HARDWARE AND SOFTWARE COMPONENTS: Ceiling all-inclusive costs, GST/HST extra, F.O.B. Destination (for goods), in accordance with the following categories of technology, as per the ARMOUR System Technical Specification:

- · Data Sources;
- · Infrastructure Management Systems;
- · Data Source Connectors;
- · Database Modules;
- · Data Presentation:
- · Computational Services;
- · Integration Framework;
- · Effector Connectors; and
- · Effectors.

TOTAL ESTIMATED COST OF HARDWARE AND SOFTWARE COMPONENTS INCLUDING MARK-UP FOR EVALUATION PURPOSES:
$ 1,000,000.00   (GST/HST extra) * (1 + proposed Mark-up) = $_____   (GST/HST extra)

BID PRICE: TOTAL ESTIMATED COST FOR EVALUATION PURPOSES:
(Calculated as the sum of Items 1, 2 and 3 above) $ _____(GST/HST extra)

The estimated level of effort specified is only an approximation of requirements given in good faith and is provided for financial bid evaluation purposes only. It does not represent a commitment by Canada.

PRICING SCORE
The Pricing score will be determined based on a proportional formula relative to the lowest Bid Price, **to a maximum of 20 points for the lowest Bid Price**, as follows:

Points for Price   =   20 X   Lowest Bid Price of all compliant bidders
Bid Price of the Proposal Being Evaluated

Examples:

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

Bid Price	Calculation	Price Points
$8M (lowest Bid Price)	20 X 8/8	20 pts
$9M	20 X 8/9	17.7 pts
$9.5M	20 X 8/9.5	16.9 pts
$10M (highest Bid Price)	20 X 8/10	16 pts

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

ATTACHMENT 4

MANDATORY AND POINT RATED CRITERIA

EXPERIENCE

Except where expressly provided otherwise, the experience of the Bidder described in the bid must be the experience of the Bidder itself (which includes the experience of any companies that formed the Bidder by way of a merger but does not include any experience acquired through a purchase of assets or an assignment of contract). The experience of the Bidder's affiliates (i.e. parent, subsidiary or sister corporations), subcontractors, or suppliers will not be considered for criteria under section 3.1 Corporate Experience of Bidder (Prime) Only.

Listing experience without providing any supporting data to describe where and how such experience was obtained will result in the experience not being included for evaluation purposes.

In evaluating resource past performance experience, compliance should be demonstrated through brief past project descriptions, whereby such descriptions should include name of the project, resource position, contract start date, work competed date, brief description of the project and other relevant details that document how this experience has been acquired by the Bidder.

For the purposes of calculation of experience "12 months of experience" can be documented by the Bidder as per the following two examples:

1. One (1) project for 12 months = 12 months experience; or
2. two (2) projects for 6 months = 12 months.

This model shall be employed everywhere where 'months' of experience are employed.

The months where the projects overlap shall be counted only once.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv

Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

MANDATORY TECHNICAL EVALUATION CRITERIA

At bid closing time, the Bidder must comply with the following Mandatory Evaluation Criteria and provide documentation to support compliance for both the Basic Requirement and the Optional Requirement.

Any bid which fails to meet the following Mandatory Evaluation Criteria will be declared non-responsive.

Mandatory Criteria Number	Mandatory Criteria Description
M1.	The Bidder must submit a Draft Architectural Design Document.
M2.	The Bidder must submit a Draft Project Management Plan.
M3.	The Bidder must identify one individual for each Key Technical Personnel postion who meets the requirements defined in Appendix D of the Statement of Work in Annex A.
M4.	The Bidder must submit a Description of Corporate Experience demonstrating that the Bidder has the required minimum experience.

Each mandatory criteria should be addressed separately. Meeting the Mandatory Evaluation Criteria above is demonstrated as follows:

1. **ARCHITECTURAL DESIGN DOCUMENT**
The Bidder must submit a draft Architectural Design Document.

2. **PROJECT MANAGEMENT PLAN**
The Bidder must submit a draft Project Management Plan (PMP). The draft PMP will be used to evaluate the Bidder's response to the Management Evaluation Criteria of the Point Rated Evaluation Criteria and must include the following:

- Identification of the intended Requirements Management Tool. The proposed Requirements Management Tool must be compatible with the IBM Rational DOORS product line, though compatility can be through an import/export process (e.g., DOORS can import from many file formats including Microsoft Word and Excel); and

- A proposed schedule that does not exceed 42 months duration.

3. **KEY TECHNICAL PERSONNEL**

The Bidder must identify one individual for each of the following positions, collectively called the Key Technical Personnel and demonstrate that each identified individual meets the mandatory requirements that are applicable to the labour category of the proposed individual as defined in Minimum Resource Requirements Table found in Appendix "D" of Annex "A" – Statement of Work (SOW) :

- Key Technical Personnel must be proposed to fill the following positions:
- Project Manager (PM);
- Lead System Architect (LSA) - LSA may also fill the SSA position or vice versa;
- Software Solution Architect (SSA) – SSA may also fill the LSA position and vice versa;
- User Interface Analyst (UIA);
- Computer Network Defence Functional Analyst (CNDFA);
- Information Technology Security Analyst (ITSA) - ITSA may also fill the CAS position or vice versa;
- Information Technology Security Certification and Accreditation Specialist (CAS) – CAS may also fill the ITSA position and vice versa;
- Senior Programmer (SP); and

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

- Quality Assurance Specialist (QAS).

4.   CORPORATE EXPERIENCE

The Bidder must submit a Description of Corporate Experience relevant to the project and demonstrate that the experience of the Bidder includes at minimum the following:

- The Bidder has successfully completed at least two (2) IT or CND Software Development and Integration relevant projects. Relevant projects are defined as being similar to the ARMOUR project, including, team size, nature, complexity and software R&D projects related to Information Technology or Computer Network Defence (CND); and

- The Bidder or a member of the proposed team has successfully completed at least one (1) relevant projects in which they were required to setup an operational simulation environment for pre-deployment testing, including the creation of test data sets. Relevant projects are defined as being similar to the ARMOUR project, including, creation of a simulated network of similar size and scope including the simulation or use of network sensors and effectors related to Computer Network Defence (CND), including the creation of test data sets.

POINT RATED EVALUATION CRITERIA

Point Rated Evaluation Criteria Summary Table

Evaluation Criteria	Points	Min.
	130	**90**
Technical, Management and Corporate Experience Evaluation Criteria		
1.0 Architectural Design (Draft Architectural Design Document)	**60**	**40**
1.1 Understanding of the vision, objectives and scope	**10**	**6**
1.2 Adequacy of the technical soloution	**50**	**32**
a) How solution meets capability requirements stated in System Technical Specification	20	14
b) How solution meets performance requirements stated in System Technical Specification	3	0
c) How solution aligns with open standards	4	0
d) How solution aligns with identified security standards	4	0
e) Ability to meet technology challenges	10	5
f) Level of COTS incorporated into the proposed solution	5	0
g) Level of risk associated with technical aspects of the solution	4	0
2.0 Management Proposal	**40**	**30**
2.1 Project Management Plan	**18**	**12**
a) Development Approach and Risk Mitigation	5	0
b) Work plan and schedule	6	0
c) Quality Management System	4	0
d) Resource Allocation and Control	3	0
2.2 Personnel	**22**	**16**
2.2.1 Project Manager	**7**	**4**
a) Experience	3	0
b) Education and Credentials	2	0

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		051sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No/ N° VME
W7714-115274	051svW7714-115274	

Evaluation Criteria	Points	Min.
c) Technical Expertise	2	0
2.2.2 Key Technical Personnel	**15**	**10**
a) Relevant IT Security experience	3	0
b) Education and Credentials	2	0
c) Computer Network Defence Experience	4	0
d) Experience developing open architectures and using relevent technology standards	3	0
e) Experience using relevent security standards	3	0
3.0 Corporate Experience	**30**	**8**
3.1 Corporate Experience of the Bidder	**17**	0
3.1.1 Relevance of Bidder's core business lines	4	0
3.1.2 Establishing and managing integrated project teams involving subcontractors	4	0
3.1.3 Demonstrated Experience in IT or CND Software Development and Integration Projects	5	0
3.1.4 Demonstrated Experience in IT Project Deployment	4	0
3.2 Corporate Experience of Proposed Team	**13**	0
3.2.1 Test Environment Setup and Datat Population	5	0
3.2.2 Demonstrated Experience providing Certification and Accreditation Support Services	4	0
3.2.3 Demonstrated Experience providing Open Source Software Project or Open Architecture Promotion and Support	4	0
Canadian Content Evaluation Criteria	**14**	**0**
Goods	4	0
Services	10	0

The Technical, Management and Corporate Experience Bid will be evaluated and scored in accordance with the following evaluation criteria:

For the work to be performed as specified in **Annex "A"** - Statement of Work (SOW) the total Point Rated Evaluation will be calculated as shown in the following tables.

Solicitation No. - N° de l'invitation
W7714-115274/E

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur
056sv

Client Ref. No. - N° de réf. du client
W7714-115274

File No. - N° du dossier
056svW7714-115274

CCC No./N° CCC - FMS No./N° VME

1. TECHNICAL EVALUATION CRITERIA

The Bidder submitted draft Architecture Design Document will be used to evaluate the Bidder response to the Technical Evaluation Criteria. The draft Architectural Design Document will be used to evaluate the Bidder's response to the Technical Evaluation Criteria of the Point Rated Evaluation Criteria and should include the following:

- A completed matrix response to the System Technical Specification for Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) Version 2.0 (STS), Section 5, STS Table including the Technology Readiness Level (TRL)[1] at time of bid closing. The matrix response for each item should be the 'TRL rating' or, in the event that there is no TRL rating at time of bid closing, 'To be met through development.'

The draft Architectural Design Document should be structured in accordance with the Data Item Description (DID) SD002 as described in Annex "A" -Statement of Work (SOW). This document should be structured so as to facilitate evaluation of the point rated criteria. The draft Architectural Design Document should describe the proposed architecture and approach the Bidder intends to use to meet the System Technical Specification for Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) Version 2.0 (STS) (instructions for accessing the STS as a supporting project reference can be found in Annex "B") including:

- Proposed architecture including identification and described use of Commercial-off-the-shelf (COTS), Open Source Software (OSS), DRDC furnished software or other sources of software modules to be included in the solution;
- Identification of new software modules that will be developed completely within the ARMOUR TD to meet STS requirements;
- Identification of existing software modules (whether COTS, OSS, DRDC furnished or other sources) that will need to be enhanced within the ARMOUR TD to meet STS requirements;
- Proposed use of technology and security standards;
- Mapping of the proposed architecture to the STS Section 4, ARMOUR Conceptual Architecture;
- Description of the ability of the proposed architecture to meet the STS Section 6, Performance Targets and Metrics; and
- Description of the understanding and proposed approach to address the STS Section 7, Areas Requiring Further Investigation.

Technical Evaluation criteria	Scale	Maximum Points	Min.
1.0 Architectural Design (Draft Architectural Design Document - SD002)		60 (1.1 + 1.2)	40

[1] Technology Readiness Levels

https://buyandsell.gc.ca/initiatives-and-programs/canadian-innovation-commercialization-program-cicp/program-specifics/technology-readiness-levels

Solicitation No. - N° de l'invitation Amd. No. - N° de la modif. Buyer ID - Id de l'acheteur

W7714-115274/E 056sv

Client Ref. No. - N° de réf. du client File No. - N° du dossier CCC No./N° CCC - FMS No./N° VME

W7714-115274 056svW7714-115274

Technical Evaluation criteria	Scale	Maximum Points	Min.
1.1. Understanding of the vision, objectives and scope The Bidder should demonstrate their understanding of the vision, objectives and scope in their own words. Restating the description of these concepts from the Solicitation material will not be considered sufficient to demonstrate Bidder understanding.	**1 point per** criteria will be awarded for an accurate description of the Bidder understanding of the vision, objectives and scope across the following criteria: • Proactive operations based on identified security vulnerabilities • Reactive operations based on detection of security incidents • Capabilities supporting Semi-automated response • Capabilities supporting Fully-automated response; • Mission assurance concepts including the dynamic nature of mission priorities and their impact on Course of Action prioritization; • Degree of automated Course of Action calculation and prioritization; • Course of Action coverage involving multiple concurrent mitigations; • Enterprise-wide metrics coverage at the mission, service, and system levels; • Importance of an Integration Framework for the Computer Network Defence community; and • Degree of modularity in the proposed software architecture	10	6

Solicitation No. - N° de l'invitation   Amd. No. - N° de la modif.   Buyer ID - Id de l'acheteur
W7714-115274/E   056sv

Client Ref. No. - N° de réf. du client   File No. - N° du dossier   CCC No./N° CCC - FMS No./N° VME
W7714-115274   056svW7714-115274

Technical Evaluation criteria	Scale	Maximum Points	Min.
1.2. Adequacy of the technical solution	Given the requirements stated in the Solicitation, the adequacy of the technical solution proposed by the bidder will be evaluated as a whole across criteria a) to g).	**50 Total a) to g)**	**32**
a) How the solution meets the capability requirements as stated in the System Technical Specification for Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) Version 2.0, Sections: 4, 5, 6.	**20** The solution as described, at completion of the relevant demonstration phase(s), meets 100% of the stated requirements with TRL 7 (or higher level) technologies. **17** The solution as described, at completion of the relevant demonstration phase(s), meets 80% of the stated requirements with TRL 7 (or higher level) technologies and 95% of the stated requirements with TRL 6 (or higher level) technologies. **14** The solution as described, at completion of the relevant demonstration phase(s), meets 60% of the stated requirements with TRL 7 (or higher level) technologies and meets 80% of the stated requirements with TRL 6 (or higher level) technologies and 95% of the stated requirements with TRL 5 (or higher level) technologies. **0** The solution as described, at completion of the relevant demonstration phase(s), meets less than 60% of the stated requirements with TRL 7 (or higher level) technologies or meets less than 80% of the stated requirements with TRL 6 (or higher level) technologies or less than 95% of the stated requirements with TRL 5 (or higher level) technologies. **Summary of Technology Readiness Levels:** TRL 7: System prototype demonstration in an operational environment TRL 6: System/subsystem model or prototype demonstration in a relevant (simulated operational) environment TRL 5: Component validation in relevant (simulated) environment	20	14
b) How the solution meets the performance requirements as stated in System Technical Specification for Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) Version 2.0, Sec 6. Recognizing that the proposal includes an architectural level view, the bidder is expected to be able to provide an analytical justification of the proposed architectural ability to meet the performance targets.	**3** The solution, as described, presents an architecture that demonstrates the ability to meet both the Technology Demonstration (TD) and deployed system operational performance targets and metrics; **2** The solution, as described, presents an architecture that demonstrates the ability to meet the TD performance targets and metrics, but meets the deployed system operational performance targets and metrics with deficiencies; **1** The solution, as described, presents an architecture that demonstrates the ability to meet the Technology Demonstration (TD) performance targets and metrics with deficiencies; **0** The solution, as described, does not meet the TD performance targets and metrics.	3	0

Solicitation No. - N° de l'invitation
W7714-115274/E

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur
056sv

Client Ref. No. - N° de réf. du client
W7714-115274

File No. - N° du dossier
056svW7714-115274

CCC No./N° CCC - FMS No./N° VME

Technical Evaluation criteria	Scale	Maximum Points	Min.
c) How the solution aligns with open standards: Does the solution ensure that XML standards are identified and incorporated? Standards bodies are: OASIS or W3C. (The expected use of open standards is described in the System Technical Specification for Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD), Sections 4.1 and 5.)	**4** The solution, as described, uses standards based web services for more than 50% of the solution in all three architecture areas listed below; **3** The solution, as described, uses standards based web services for more than 50% of the solution in two of three architecture areas listed below; **2** The solution, as described, uses standards based web services for more than 50% of the solution in one of three architecture areas listed below; **0** The solution, as described, uses standards for 50% or less of the solution across the three architecture areas listed below. The three architecture areas are identified as follows: • Standards based web services are used for Data Source Connectors and Effector Connectors (e.g., interfaces to and from the ARMOUR system); • Standards based web services are used between architectural components (e.g., Database, Computational Services and Data Presentation components) • Standards based web services are used between processing modules (e.g., Correlation module, Fusion module, etc.)	4	0
d) How the solution aligns with identified security standards: Does the solution ensure that the Common Vulnerabilities and Exposures (CVE); Open Vulnerability and Assessment Language (OVAL); Common Vulnerability Scoring System (CVSS); Common Platform Enumeration (CPE); Malware Attribute Enumeration and Characterization (MAEC); and Common Attack Pattern Enumeration and Classification (CAPEC) or equivalent open standards are identified and incorporated where appropriate? (The expected use of security standards is described in the System Technical Specification for Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD), Section 5.) Where equivalent open standards are included, the bidder must demonstrate how they map to one or more of the six information domains represented by the standards named in this rating criteria. It is permissible to use fewer standards to cover the information domains.	**4** The solution, as described, aligns with all 6 identified security standards and ensures that information requirements are identified and incorporated into the solution; **3** The solution, as described, aligns with at least 3 of 6 identified security standards and ensures that information requirements are identified and incorporated into the solution; **2** The solution, as described, aligns with at least 2 of 6 identified security standards and ensures that information requirements are identified and incorporated into the solution; **1** The solution, as described, aligns with at least 1 of 6 identified security standards and ensures that information requirements are identified and incorporated into the solution; **0** The solution, as described, does not align with identified security standards.	4	0

Technical Evaluation criteria	Scale	Maximum Points	Min.
e) Ability to meet technology challenges: Does the Bidder demonstrate technical knowledge in understanding the areas requiring further investigation and present viable approaches to meet these challenges? (The technology challenges requiring further investigation are described in the System Technical Specification for Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD), Section 7.)	**10** The Bidder demonstrates clear understanding of all 7 areas requiring further investigation, has presented sound approaches to deal with them and has further identified additional areas requiring further investigation with sound approaches to dealing with them; **9** The Bidder demonstrates clear understanding of all 7 areas requiring further investigation and has presented sound approaches to deal with them; **8** The Bidder demonstrates clear understanding of at least 6 of 7 areas requiring further investigation and has presented sound approaches to deal with them; **7** The Bidder demonstrates clear understanding of at least 6 of 7 areas requiring further investigation and has presented sound approaches to deal with at least 4 of them; **6** The Bidder demonstrates clear understanding of 5 of 7 areas requiring further investigation and has presented sound approaches to deal with at least 3 of them; **5** The Bidder demonstrates clear understanding of 4 of 7 areas requiring further investigation and has presented sound approaches to deal with at least 3 of them; **0** The Bidder demonstrates clear understanding of less than 4 of 7 areas requiring further investigation or has not presented a sound approach to deal with at least 3 of them.	10	5
f) The level of COTS incorporated within the proposed solution to meet the architectural requirements will be reviewed. For the purposes of this criterion, Open Source Software for which a commercial license is available will be considered as COTS.	**5** The solution, as described at bid time, mostly (greater than 50%) incorporates COTS within all 5 of the 5 architectural components (Data Sources, Database, Computational Services, Data Presentation, Effectors). **4** The solution, as described at bid time, mostly (greater than 50%) incorporates COTS for at least 4 of the 5 architectural components. **3** The solution, as described at bid time, mostly (greater than 50%) incorporates COTS for 3 of the 5 architectural components. **2** The solution, as described at bid time, mostly (greater than 50%) incorporates COTS for 2 of the 5 architectural components. **1** The solution, as described at bid time, mostly (greater than 50%) incorporates COTS for 1 of the 5 architectural components. **0** The solution, as described at bid time, does not incorporate mostly (50% or less) COTS for at least 1 of the 5 architectural components.	5	0

Solicitation No. - N° de l'invitation
W7714-115274/E

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur
056sv

Client Ref. No. - N° de réf. du client
W7714-115274

File No. - N° du dossier
056svW7714-115274

CCC No./N° CCC - FMS No./N° VME

Technical Evaluation criteria	Scale	Maximum Points	Min.
g) Level of risk associated with technical aspects of the solution (Avoidance of unnecessary complexity, degree of integrated software and use of unproven technologies)	The solution, as described will be awarded points according to the following scales, by category. The sum of all three categories will create a composite level of risk score: **Avoidance of unnecessary complexity** **1.5 points** = Low Risk, Architecture maps closely to ARMOUR Conceptual Architecture **0.75 points** = Medium Risk, Architecture includes use of unnecessary or redundant software modules **0 points** = High Risk, Architecture includes additional software modules considered beyond scope of Basic Requirement **Degree of Integrated Software** **1.5 points** = Low Risk, More than 50% of software modules have existing standards based Application Programming Interfaces (APIs) **0.75 points** = Medium Risk, More than 50% of software modules have published (though proprietary) APIs **0 points** = High Risk, More than 50% of software modules have non-standard, unpublished, or non-existent APIs **Use of Unproven Technologies** **1 point** = Low Risk, 80% or more of the requirements are met with TRL 6 (or higher) level technologies at bid time. **0.5 points** = Medium Risk, 50% or more, but less than 80%, of the requirements are met with TRL 6 (or higher) level technologies at bid time. **0 points** = High Risk, Less than 50% of the requirements are met with TRL 6 (or higher) level technologies at bid time.	4	0
Summary of Technology Readiness Levels: TRL 6: System/subsystem model or prototype demonstration in a relevant (simulated operational) environment			

Solicitation No. - N° de l'invitation   Amd. No. - N° de la modif.   Buyer ID - Id de l'acheteur

W7714-115274/E   056sv

Client Ref. No. - N° de réf. du client   File No. - N° du dossier   CCC No./N° CCC - FMS No./N° VME

W7714-115274   056svW7714-115274

2. MANAGEMENT EVALUATION CRITERIA

The Bidder submitted draft Project Management Plan (PMP) will be used to evaluate the Bidder response to the Management Evaluation Criteria. The draft PMP should be structured in accordance with the DID PM001 as described in Annex "A" -Statement of Work (SOW). The draft PMP should demonstrate a thorough work plan and should include a comprehensive schedule with consideration to respond to unforeseen delays. The draft PMP should be structured so as to facilitate evaluation of the point rated criteria as follows:

- **Development Approach and Risk Mitigation Plan:** The draft PMP should include a description of the development approach and risk mitigation plan including the Bidder's approach to cyclical development that will accommodate the potential for evolving requirements resulting from each development phase. The development approach should include a brief description of the intended approach to Requirements Management, Configuration Management and Demonstration Management;

- **WBS and Schedule:** The draft PMP should include a resource loaded work breakdown structure (WBS) and schedule that clearly identifies significant milestones as indicated in the SOW. The Bidder is free to propose an alternate schedule for these milestones;

- **Quality Management System:** The draft PMP should include a description of the Quality Management System in use by the Bidder, including a description of any Quality Management Standards followed, or Quality Management Certifications held by the bidder. Copies of any Quality Management Certificates (e.g., an ISO/IEC 9001:2008 Certificate) claimed by the Bidder should be included in an Appendix to the draft PMP. Relevant quality management or software development process standards or certifications include ISO/IEC 9001:2008, ISO 12207, IEEE 829 or 830, CMMi, SEI-CMM or equivalent applicable documentation and process standards. For equivalent applicable documentation and process standards, Bidders should confirm equivalence by submitting a question prior to bid close. The approach to ensure the Bidder's Quality Management System encompasses the Bidder's proposed team members (e.g., sub-contractors) should be described;

- **Resource Plan:** The Resource Plan section of the draft PMP should describe the allocation of Key Technical Personnel, other labour and non-labour resources assigned to tasks and sub-tasks of the work plan; the organizational structure and reporting relationships; provide a Resource Assignment and Responsibility Matrix, and describe the control and quality assurance processes used by the Bidder to ensure effective management of all tasks throughout the duration of the Contract. The Resource Plan should describe the nature of any teaming or sub-contracting relationships between the Bidder and other members of the proposed team. The Resource Plan should describe the available personnel resource pool, alternate sources of personnel and recruiting mechanisms that may be used to ensure sufficient personnel resources are applied to meet the needs of the SOW. The Bidder should also Provide a Summary of Experience for all proposed individuals that are to be evaluated as Key Technical Personnel.

Solicitation No. - N° de l'invitation
W7714-115274/E

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur
056sv

Client Ref. No. - N° de réf. du client
W7714-115274

File No. - N° du dossier
056svW7714-115274

CCC No./N° CCC - FMS No./N° VME

Management Evaluation criteria	Scale	Maximum Points	Min.
2.0 Management Proposal		40 (2.1 + 2.2)	30
2.1. Project Management Plan (Draft PM001)		18 Total a) to d)	12
a) Development Approach and Risk Mitigation The proposed work plan will be evaluated for its completeness, clarity and achievability as demonstrated through: • The use of a development approach that can flexibly adapt to evolving requirements; and • The use of supporting requirements management and configuration management tools.	**5** Work plan includes a industry-based development approach that is well suited to cyclical software development in a complex environment and can adapt to evolving requirements, while effectively managing risk (examples of accepted industry-based development approaches include Unified Process, Scrum, Agile Software Development, including requirements management and configuration management tools) and has been used by the Bidder on at least one other project for at least 6 months; **4** Work plan includes an identified development approach that is well suited to cyclical software development in a complex environment and can adapt to evolving requirements, while effectively managing risk (examples of accepted development approaches would be those involving incremental development, rapid prototyping, spiral development, or rapid application development, including requirements management and configuration management tools); **3** Work plan includes an identified development approach that can effectively manage a complex software development project while effectively managing risk (examples would include non-cyclical development approaches like the waterfall method and incorporates requirements management and configuration management tools, including requirements management and configuration management tools); **2** Work plan includes an identified development approach that can manage common software development tasks and moderate risk levels (examples would include non-cyclical development approaches like the waterfall method but lacking either requirements management or configuration management tools); **1** Work plan includes an identified development approach that can manage simple software development tasks and low risk levels (examples would include non-cyclical development approaches like the waterfall method but lacking both requirements management and configuration management tools); **0** Work plan includes an identified development approach that would not adequately address software development tasks and low risk levels (examples would include use of a development approach that does not include at least Requirements Analysis, Design, Build, Test, and Demonstration stages, or does not account for rework following the Test phase).	5	0

Solicitation No. - N° de l'invitation
W7714-115274/E

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur
056sv

Client Ref. No. - N° de réf. du client
W7714-115274

File No. - N° du dossier
056svW7714-115274

CCC No./N° CCC - FMS No./N° VME

Management Evaluation criteria	Scale	Maximum Points	Min.
b) Work plan and schedule The proposed work plan will be evaluated for its completeness, clarity and achievability as demonstrated through: • The use of a work breakdown structure mapped to the Statement of Work for the Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD), Version 2.0, Section phase and work descriptions (Section 2 and Appendix A); • The ability to meet or accelerate the estimated schedule for delivery identified in the SOW for the ARMOUR TD, Appendix B, Table 1.	**4** The WBS of the proposed work plan identifies all the necessary management, administrative and engineering tasks and sub-tasks required for the successful completion of each Phase, and for each deliverable of each Phase of the Basic Requirement identified in the SOW at Annex A at a higher level of detail than described in the SOW. The identified tasks and sub-tasks provide a task duration granularity that does not exceed 42 months. All tasks and sub-tasks are reflected in a comprehensive schedule that also includes limiting activities, required inputs from Canada, identifies critical path activities and presents consideration to anticipate and avoid delays. An additional 2 points will be awarded if the schedule provides accelerated delivery of the Basic Requirement in less than 42 months. **2** The WBS of the proposed work plan identifies, at a minimum, all major management, administrative and engineering tasks required for successful completion of each Phase, and for each deliverable of each Phase of the Basic Requirement identified in the SOW at Annex A at the level of detail described in the SOW or higher. The identified tasks and sub-tasks provide a task duration granularity does not exceed 42 monthss. All tasks and sub-tasks are reflected in a comprehensive schedule that also includes limiting activities, required inputs from Canada, identifies critical path activities and presents consideration to anticipate and avoid delays. An additional 1 point will be awarded if the schedule provides accelerated delivery of the Basic Requirement in less than 42 months. **0** The WBS of the proposed work plan does not address all tasks identified in the SOW as Annex A; or the tasks identified in the WBS are not described at the level of detail provided in the SOW or higher. No task duration granularity is provided for the tasks identified or the task granularity exceeds 42 months. The tasks identified are not reflected in a comprehensive schedule; or the schedule does not identify: limiting activities, required inputs from Canada, the critical path activities or consideration for delays.	6	0

Solicitation No. - N° de l'invitation   Amd. No. - N° de la modif.   Buyer ID - Id de l'acheteur

W7714-115274/E   056sv

Client Ref. No. - N° de réf. du client   File No. - N° du dossier   CCC No./N° CCC - FMS No./N° VME

W7714-115274   056svW7714-115274

Management Evaluation criteria	Scale	Maximum Points	Min.
c) Quality Management System Conformance to quality management and software development process standards or certifications will be evaluated.	**4** The Bidder maintains both a relevant quality management system certification and software development process standards validated by an independent review or certification body; **3** The Bidder maintains either a relevant quality management system certification or software development process standard validated by an independent review or certification body; **2** The Bidder maintains either a relevant quality management system certification or software development process standard validated through an internal audit or review; **1** The Bidder maintains either a relevant quality management system or software development process according to a relevant standard, but has not had the system or processes validated by an audit or review; **0** The Bidder does not maintain either a relevant quality management or software development process standard. *Relevant quality management or software development process standards include ISO/IEC 9001:2008, ISO 12207, IEEE 829 or 830, CMMi, SEI-CMM or equivalent applicable documentation and process standards.*	4	0

Solicitation No. - N° de l'invitation
W7714-115274/E

Client Ref. No. - N° de réf. du client
W7714-115274

Amd. No. - N° de la modif.

File No. - N° du dossier
056svW7714-115274

Buyer ID - Id de l'acheteur
056sv

CCC No./N° CCC - FMS No./N° VME

Management Evaluation criteria	Scale	Maximum Points	Min.
d) Resources allocation and control The following will be evaluated: • The level of effort and commitment of the proposed personnel in all activities of the project; • An assessment of the team organizational structure, description of responsibilities, and description of reporting relationships including sub-contracting and partnering agreements; • An assessment of the available personnel resource pool and the ability to ensure qualified resources are available to meet project demands including alternate sources of personnel and recruiting mechanisms; and • The demonstrated means by which the Bidder will control the project resources and the quality assurance processes as applied to subcontracting and partnering agreements.	**3** The level of effort is identified for Key Technical Personnel and other labour resources for each task and sub-task of each phase identified in the proposed work plan and are commensurate with proposed scope of work of the task. The responsibilities of each identified resource are defined for each task and sub-task. The flow of information and communications is detailed in the reporting structure between Key Technical Personnel, other labour resources, and subcontractors. The reporting structure identifies relationship between resources and corporate level authorities; and demonstrates consideration of communication requirements with all other project stakeholders. Detailed processes and procedures address control and maintenance of the proposed resources. Detailed processes and procedures address control, maintenance and quality assurance of resources for all tasks and sub-tasks throughout the duration of the contract. **2** The level of effort is identified for Key Technical Personnel and other labour resources for the major tasks of each phase identified in the proposed work plan and are commensurate with proposed scope of work of the task. The responsibilities of each identified resource are defined for each task. The flow of information and communications is detailed in the reporting structure between Key Technical Personnel and subcontractors. The reporting structure identifies relationship between resources and corporate level authorities; and demonstrates consideration of communication requirements with the Technical Authority. High level concept of the processes and procedures addressing control, maintenance and quality assurance of resources for all tasks throughout the duration of the contract are presented at a high level. **1** The level of effort is identified for Key Technical Personnel and other labour resources for the major tasks of each phase identified in the proposed work plan and are commensurate with proposed scope of work of the task. The responsibilities of each identified resource are defined for the majority of tasks. The flow of information and communications is detailed in the reporting structure between Key Technical Personnel and demonstrates consideration of communication requirements with the Technical Authority. Presents a plan without processes or procedures for addressing control, maintenance and quality assurance of resources for all tasks throughout the duration of the contract. **0** The level of effort is not identified for all Key Technical Personnel and other labour resources for the major tasks of each phase identified in the proposed work plan; or the level of effort identified is not commensurate with the proposed scope of work for each task. The responsibilities of each identified resource are not defined for the majority of tasks. The flow of information and communications is demonstrated only for the Key Technical Personnel; or the reporting structure is not provided. Processes and Procedures for resource control, maintenance and quality assurance are not addressed.	3	0

Management Evaluation criteria	Scale	Maximum Points	Min.
2.2. Personnel		**22** **(2.2.1 + 2.2.2)**	**16**
2.2.1. Project Manager		**7** **Total a) to c)**	**4**
a) Experience, past projects and accomplishments of the Project Manager. Relevant projects are defined as being similar to the ARMOUR project, including, Team size, nature and complexity for software R&D projects.	**3** The Project Manager has at least twelve (12) years of project management experience relevant to this project; **2** The Project Manager has at least ten (10) years of project management experience relevant to this project; **1** The Project Manager has at least eight (8) years of project management experience relevant to this project. **0** The Project Manager has less than eight (8) years of project management experience relevant to this project.	3	0
b) Education and credentials of the Project Manager	**2** University Degree in relevant field, and Project Management credentials; **1** University Degree in relevant field or equivalent Project Management credentials; **0.5** College Diploma in a relevant field; **0** No applicable degree/diploma. *Relevant fields include scientific, engineering, mathematics or business.* *Credentials include recognized certifications from the Project Management Institute (PMI).*	2	0
c) Technical expertise of the Project Manager relevant to this project.	**2** The project Manager has at least four (4) years working experience in at least two of the technical fields relevant to this project **1** The Project Manager has at least four (4) years of working experience in at least one of the technical fields relevant to this project. **0.5** The Project Manager has at least two (2) years of working experience in at least one of the technical fields relevant to this project. **0** The Project Manager has less than two (2) years of working experience in a technical field relevant to this project. *Technical fields of IT Security, relevant to this project include: Computer Network Defence, Security Information and Event Management Systems, Intrusion Detection and Prevention Systems, Security Operations Centre, Vulnerability Management, Patch Management, Security Incident Analysis or Forensics.*	2	0

Solicitation No. - N° de l'invitation   Amd. No. - N° de la modif.   Buyer ID - Id de l'acheteur

W7714-115274/E   056sv

Client Ref. No. - N° de réf. du client   File No. - N° du dossier   CCC No./N° CCC - FMS No./N° VME

W7714-115274   056svW7714-115274

Management Evaluation criteria	Scale	Maximum Points	Min.
2.2.2. Key Technical Personnel Proposal Evaluation The experience and education of the project team members will be evaluated. This criterion will assess how suitable is the breath, or range, of expertise proposed as part of the team, as well as the depth, or level, of this expertise. The experience for each team member within the past ten (10) years on projects of similar nature, size and complexity will be evaluated according to the criteria defined from a) to e) below. The following resources will be evaluated to fill the roles of Key Technical Personnel: -Project Manager (PM); -Lead System Architect (LSA); -Software Solution Architect (SSA); -User Interface Analyst (UIA); -Computer Network Defence Functional Analyst (CNDFA); -Information Technology Security Analyst (ITSA); -Certification and Accreditation Specialist (CAS); -Senior Programmer (SP); and -Quality Assurance Specialist (QAS). Note: the following resources may fill multiple roles: -LSA may also fill the SSA position or vice versa; and -ITSA may also fill the CAS position or vice versa.		**15** **Total a) to e)**	**10**

Solicitation No. - N° de l'invitation
W7714-115274/E

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur
056sv

Client Ref. No. - N° de réf. du client
W7714-115274

File No. - N° du dossier
056svW7714-115274

CCC No./N° CCC - FMS No./N° VME

Management Evaluation criteria	Scale	Maximum Points	Min.
a) Relevant IT Security experience of key team members (excluding the Project Manager): Relevant areas of IT Security include: 1) Security Information and Event Management Systems; 2) Intrusion Detection Systems or Intrusion Prevention Systems; 3) Vulnerability, Patch Management; 4) Security Incident Analysis; 5) IT Security Forensics; 6) Information System Security Engineering (ISSE); and 7) Certification and accreditation in accordance with the Government of Canada (GC) Policy on Government Security (PGS) *The bidder should clearly identify the key team members to be evaluated for this criterion.*	**Excluding the Project Manager:** **3** At least five (5) of the key team members have at least five (5) years each of experience relevant to IT Security and the team has at least one (1) year of collective experience in all seven (7) IT Security areas. **0** Less than five (5) of the key team members have at least five (5) years each of experience relevant to IT Security or the team does not have at least one (1) year of collective experience in all seven (7) IT Security areas. *Years of experience include graduate work in this field.* *Collective experience is the combination of individual experience, not experience gained as a team.*	3	0
b) Education and credentials of key members of proposed team (excluding the Project Manager). *The bidder should clearly identify the key team members to be evaluated for this criterion.*	**Excluding the Project Manager:** **0.25** Points for each key team member with a natural science, engineering, or mathematics university degree; **0.25** Points for each key team member with an active IT Security certification. *IT Security certifications include Certified Information Systems Security Professional (CISSP), Global Information Assurance Certification (GIAC) and associated certifications.*	2	0
c) Computer Network Defence processes and systems experience of key members of proposed team (excluding the Project Manager and Computer Network Defence Functional Analyst). *The bidder should clearly identify the key team members to be evaluated for this criterion.*	**Excluding the Project Manager and the Computer Network Defence Functional Analyst:** **4** At least three (3) of the team key members have at least four (4) years of experience in Computer Network Defence processes and systems. **3** At least two (2) of the team key members have at least four (4) years of experience in Computer Network Defence processes and systems. **0** Less than two (2) team key members have less than four (4) years of experience in Computer Network Defence processes and systems.	4	0

Solicitation No. - N° de l'invitation
W7714-115274/E

Client Ref. No. - N° de réf. du client
W7714-115274

Amd. No. - N° de la modif.

File No. - N° du dossier
056svW7714-115274

Buyer ID - Id de l'acheteur
056sv

CCC No./N° CCC - FMS No./N° VME

Management Evaluation criteria	Scale	Maximum Points	Min.
d) Experience of proposed key team members in developing open architectures and using relevant technology standards in a software development environment. Relevant technology standards include: 1) Web-services standards from W3C; 2) SOA architecture standards from OASIS; 3) XML Standards from W3C or XML.org *The bidder should clearly identify the key team members to be evaluated for this criterion.*	**3** At least three (3) of the key team members have at least four (4) years each demonstrating open architectures development and relevant experience; **2** At least two (2) of the key team members have at least four (4) years each demonstrating open architectures development and relevant experience; **0** Less than two (2) of the key team members have at least four (4) years each demonstrating open architectures development and relevant experience.	3	0
e) Experience of proposed key team members using relevant security standards and methods: 1) Common Vulnerabilities and Exposures (CVE) 2) Open Vulnerability and Assessment Language (OVAL) 3) Common Vulnerability Scoring System (CVSS) 4) Malware Attribute Enumeration and Characterization (MEAC) 5) Common Attack Pattern Enumeration and Classification (CAPEC) *The bidder should clearly identify the key team members to be evaluated for this criterion.*	**3** At least three (3) of the key team members have at least four (4) years each of combined relevant experience. **2** At least two (2) of the key team members have at least three (3) years each of combined relevant experience. **0** Less than two (2) of the key team members have at least three (3) years each of combined relevant experience. *Combined experience refers to a combination of experience across all five relevant security standards and methods.*	3	0

Solicitation No. - N° de l'invitation
W7714-115274/E

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur
056sv

Client Ref. No. - N° de réf. du client
W7714-115274

File No. - N° du dossier
056svW7714-115274

CCC No./N° CCC - FMS No./N° VME

3. CORPORATE EXPERIENCE EVALUATION CRITERIA

The Bidder submitted Description of Corporate Experience will be used to evaluate the Bidder response to the Corporate Experience Evaluation Criteria. The Description of Corporate Experience may be presented in the Bidders format, but must include the following:

• **Corporate Capabilities and Experience:** A general description of corporate capabilities and experience applicable to the scope of the ARMOUR TD project including a description of COTS product business lines and Software Integration Services business lines. This section must also include a description of the approach that will be used through the delivery of the Basic Requirement to ensure the Bidder can effectively leverage the corporate experience included in the bid response;

• **Summary of Corporate Experience Presentation Sheets:** A completed Summary of Corporate Experience Presentation Sheet (see Appendix 1 of Attachment 4) for each project to be evaluated. Note that Bidders must certify successful completion of the projects included for evaluation by certifying client acceptance of the project as outlined in Attachment 5 (Certifications Required With The Bid). The Corporate Experience Presentation Sheets must clearly demonstrate that the experience of the Bidder includes at minimum the following:

• The Bidder has successfully completed at least two (2) IT or CND Software Development and Integration relevant projects and has adequately demonstrated a mechanism to leverage the experience into the ARMOUR TD project. Relevant projects are defined as being similar to the ARMOUR project, including, team size, nature, complexity and software R&D projects related to Information Technology or Computer Network Defence (CND);

• The Proposed Team has successfully completed at least two (2) relevant projects in which they were required to setup an operational simulation environment for pre-deployment testing, including the creation of test data sets and has adequately demonstrated a mechanism to leverage the experience into the ARMOUR TD project. Relevant projects are defined as being similar to the ARMOUR project, including, the creation of a simulated network of similar size and scope including the simulation or use of network sensors and effectors related to Computer Network Defence (CND), including the creation of test data sets; and

• **Client References:** For at least two (2) of the projects included for evaluation in the **Summary of Corporate Experience Presentation Sheets**, provide client contact information (Client Organization, Client Name, Contact Phone Number, Contact Email Address, and Mailing Address) such that the evaluation team may contact the identified clients to verify the successful completion of the included projects.

Bidders are encouraged to include in the bid package a **Corporate Project Evaluation Matrix.** If included, the Corporate Project Evaluation Matrix should provide a cross referenced matrix mapping the projects used to demonstrate corporate experience against the Corporate Experience Point Rated Evaluation Criteria in a format similar to what is shown in the Table below. References should be provided between the relevant Corporate Experience Point Rated Evaluation Criteria indicated and the Summary of Corporate Experience Presentation Sheet paragraph number providing evidence related to the evaluation criteria.

| Project Reference | | Relevant Corporate Experience Point Rated Evaluation Criteria | | | | | | |
Proj.No.	Project Name	3.1.1	3.1.2	3.1.3	3.1.4	3.2.1	3.2.2	3.2.4
1	*Project Example*	Ref X	Ref X				Ref X	
2	*Project Example*		Ref X	Ref X	Ref X			
3	*Project Example*			Ref X	Ref X	Ref X		Ref X
4	*Project Example*				Ref X		Ref X	
	Total Relevant Projects Per Evaluation Criteria	1	2	2	3	1	2	1

Solicitation No. - N° de l'invitation
W7714-115274/E

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur
056sv

Client Ref. No. - N° de réf. du client
W7714-115274

File No. - N° du dossier
056svW7714-115274

CCC No./N° CCC - FMS No./N° VME

Corporate Experience Evaluation criteria	Scale	Maximum Points	Min.
3.0 Corporate Experience		**30 (3.1 + 3.2)**	**8**
3.1 Corporate Experience of Bidder (Prime) Only	For the purposes of section 3.1, the experience of the Bidder described in the bid must be the experience of the Bidder itself (which includes the experience of any companies that formed the Bidder by way of a merger but does not include any experience acquired through a purchase of assets or an assignment of contract). The experience of the Bidder's affiliates (i.e. parent, subsidiary or sister corporations), subcontractors, or suppliers will not be considered.		
3.1.1 Relevance of Prime Bidder core business lines Relevant applications and products are part of the core business of the Prime Bidder, including delivery of turn-key integration services.	**4** The Bidder sells COTS products for at least two (2) relevant applications and products or sells turn-key solutions that incorporate at least three (3) relevant applications or products. **3** The Bidder sells COTS products for at least one (1) relevant application or product or sells turn-key integrated solutions that incorporate at least three (3) relevant applications or products. **2** The Bidder sells turn-key integrated solutions that incorporate at least two (2) relevant applications or products. **0** The Bidder does not sell COTS products for at least one (1) relevant application or product and does not provide turn-key solutions that incorporate at least two (2) relevant applications or products. *Relevant applications and products include: Integrated Computer Network Defence Systems, Security Information and Event Management Systems, Intrusion Detection and Prevention Systems, Vulnerability and Patch Management Systems, Security Incident Analysis or Forensics Systems.*	4	0
3.1.2 Establishing and managing integrated project teams involving subcontractors The number, scope and relevance of past projects in which the Bidder was required to setup an integrated project team involving use of multiple sub-contractor companies will be evaluated considering whether they were successfully completed as demonstrated by client certification of acceptance.	**1 point per** successfully completed relevant project involving the use of sub-contractor companies and including an adequately demonstrated mechanism to leverage the experience into the ARMOUR TD project. *Relevant projects are defined as being similar to the ARMOUR project, including, software development and integration activities using a team size of at least 8 people, involving at least two (2) sub-contract companies and where the sub-contractors are demonstrated to have done at least 20% of the level of effort.* *Adequately demonstrated mechanisms to leverage the reference project experience into the ARMOUR TD project would include, for example, use of management personnel that were on the reference project teams, use of pre-existing processes for tracking lessons learned and making them available for reference during the project, including tasks in the WBS to formalize knowledge transfer from one project team to another, or Bidder equivalent processes.*	4	0

Solicitation No. - N° de l'invitation
W7714-115274/E

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur
056sv

Client Ref. No. - N° de réf. du client
W7714-115274

File No. - N° du dossier
056svW7714-115274

CCC No./N° CCC - FMS No./N° VME

Corporate Experience Evaluation criteria	Scale	Maximum Points	Min.
3.1.3 Demonstrated Experience in IT or CND Software Development and Integration Projects The number, scope and relevance of past software development and integration projects will be evaluated considering whether they were successfully completed as demonstrated by certification of client acceptance.	**5** The Bidder has successfully completed at least four (4) relevant projects, at least two of which are CND related and has adequately demonstrated a mechanism to leverage the experience into the ARMOUR TD project; **4** The Bidder has successfully completed at least three (3) relevant projects and has adequately demonstrated a mechanism to leverage the experience into the ARMOUR TD project; **0** The Bidder has successfully completed less than three (3) relevant projects or has not adequately demonstrated a mechanism to leverage the experience into the ARMOUR TD project. *Relevant projects are defined as being similar to the ARMOUR project, including, team size, nature, complexity and software R&D projects related to Information Technology or CND.* *Adequately demonstrated mechanisms to leverage the reference project experience into the ARMOUR TD project would include, for example, use of management personnel that were on the reference project teams, use of pre-existing processes for tracking lessons learned and making them available for reference during the project, including tasks in the WBS to formalize knowledge transfer from one project team to another, or Bidder equivalent processes.*	5	0
3.1.4 Demonstrated Experience in IT Project Deployment The number, scope and relevance of past projects involving IT solution deployment on a production (operational) network will be evaluated considering whether they were successfully completed as demonstrated by client certification of acceptance.	**1 point per** successfully completed relevant IT solution deployment projects on a production (operational) network and including an adequately demonstrated mechanism to leverage the experience into the ARMOUR TD project. *Relevant projects are defined as being IT related solutions involving both distributed network management systems and centralized network management applications deployed on a production (operational) network of at least 5,000 hosts.* *Adequately demonstrated mechanisms to leverage the reference project experience into the ARMOUR TD project would include, for example, use of management personnel that were on the reference project teams, use of pre-existing processes for tracking lessons learned and making them available for reference during the project, including tasks in the WBS to formalize knowledge transfer from one project team to another, or Bidder equivalent processes.*	4	0

Solicitation No. - N° de l'invitation
W7714-115274/E

Client Ref. No. - N° de réf. du client
W7714-115274

Amd. No. - N° de la modif.

File No. - N° du dossier
056svW7714-115274

Buyer ID - Id de l'acheteur
056sv

CCC No./N° CCC - FMS No./N° VME

Corporate Experience Evaluation criteria	Scale	Maximum Points	Min.
3.2 Corporate Experience of Proposed Team	For the purposes of section 3.2, the experience of the Bidder described in the bid may include the experience of any combination of the Bidder, its affiliates (i.e. parent, subsidiary or sister corporations) or subcontractors. The experience of the Bidder's hardware, software or other equipment suppliers will only be considered where it is demonstrated that the hardware, software or other equipment supplier is included as part of the Bidder's integrated project team (e.g., deployment experience of a server product supplier will not be considered if the server product supplier is not also part of the deployment team).		
3.2.1 Test Environment Setup and Data Population The number, scope and relevance of past projects in which the Bidder was required to setup an operational simulation environment for pre-deployment testing, including the creation of test data sets will be evaluated considering whether they were successfully completed as demonstrated by certification of client acceptance.	**5** The Bidder has successfully completed at least four (4) relevant projects and has adequately demonstrated a mechanism to leverage the experience into the ARMOUR TD project; **4** The Bidder has successfully completed at least three (3) relevant projects and has adequately demonstrated a mechanism to leverage the experience into the ARMOUR TD project; **0** The Bidder has completed less than three (3) relevant projects or has not adequately demonstrated a mechanism to leverage the experience into the ARMOUR TD project. *Relevant projects are defined as being similar to the ARMOUR project, including, creation of a simulated network of similar size and scope including the simulation or use of network sensors and effectors related to Computer Network Defence (CND), including the creation of test data sets.* *Adequately demonstrated mechanisms to leverage the reference project experience into the ARMOUR TD project would include, for example, use of management personnel that were on the reference project teams, use of pre-existing processes for tracking lessons learned and making them available for reference during the project, including tasks in the WBS to formalize knowledge transfer from one project team to another, or Bidder equivalent processes.*	5	0
3.2.2 Demonstrated Experience providing Certification and Accreditation (C&A) Support Services The number, scope and relevance of past projects involving Certification and Accreditation (C&A) Support Services will be evaluated considering whether they were successfully completed as demonstrated by certification of client acceptance.	**1 point per** successfully completed project providing C&A Support Services and including an adequately demonstrated mechanism to leverage the experience into the ARMOUR TD project. *C&A Support Services include working with system owners and departmental C&A authorities to develop Statements of Sensitivity, Threat and Risk Assessments, Security Architecture or System Descriptions, Security Plans or C&A Plans and resolving identified issues leading to interim authority to process (IAP) or Approval to Operate.* *Adequately demonstrated mechanisms to leverage the reference project experience into the ARMOUR TD project would include, for example, use of management personnel that were on the reference project teams, use of pre-existing processes for tracking lessons learned and making them available for reference during the project, including tasks in the WBS to formalize knowledge transfer from one project team to another, or Bidder equivalent processes.*	4	0

Solicitation No. - N° de l'invitation   Amd. No. - N° de la modif.   Buyer ID - Id de l'acheteur

W7714-115274/E   056sv

Client Ref. No. - N° de réf. du client   File No. - N° du dossier   CCC No./N° CCC - FMS No./N° VME

W7714-115274   056svW7714-115274

Corporate Experience Evaluation criteria	Scale	Maximum Points	Min.
3.2.3 Demonstrated Experience providing Open Source Software Project or Open Architecture Promotion and Support The number of projects, scope and duration of experience in providing Open Source Software Project or Open Architecture promotion and support will be evaluated.	**4** The Bidder has participated in at least two (2) Open Source Software or Open Architecture projects in either a board level or promotional role for a period of at least two (2) years per project; **3** The Bidder has participated in at least two (2) Open Source Software or Open Architecture projects in either a board level or promotional role for a total period of at least three (3) years; **2** The Bidder has participated in at least two (2) Open Source Software or Open Architecture projects in either a board level or promotional role for a total period of at least two (2) years; **1** The Bidder has participated in at least one (1) Open Source Software or Open Architecture projects in either a board level or promotional role for a period of at least two (2) years; **0** The Bidder has not participated in at least one (1) Open Source Software or Open Architecture projects in either a board level or promotional role for a period of at least two (2) years.	4	0

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

APPENDIX 1 TO ATTACHMENT 4

SUMMARY OF CORPORATE EXPERIENCE PRESENTATION SHEET

The description for each reference project demonstrating corporate experience should include the following information (2-pages maximum per reference description):

a. identification of the Bidder;
b. identification of the reference project;
c. identification of the client organization for whom the project was executed including contact information;
d. total duration of the project or initiative, in months;
e. total dollar value of the project or initiative;
f. total number of personnel resources applied to the work;
g. highest simultaneous number of personnel resources applied to the work; and
h. description of the relevant project work, including scope and results achieved, as per the point-rated evaluation criteria indicated in Attachment 4.

(a) Bidder:	(b) Identification of Reference Project:
(c) Client Organization and Contact Information:	
(d) Project Duration:	
(e) Project Value:	
(f) Total Personnel:	(g) Highest Simultaneous Number of Personnel Assigned:
(h) Description of the Work:	

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

ATTACHMENT 5

CERTIFICATIONS PRECEDENT TO CONTRACT AWARD

1.   Federal Contractors Program for Employment Equity - Certification

1.1   Federal Contractors Program - $200,000 or more

1.   The Federal Contractors Program (FCP) requires that some suppliers, including a supplier who is a member of a joint venture, bidding for federal government contracts, valued at $200,000 or more (including all applicable taxes), make a formal commitment to implement employment equity. This is a condition precedent to contract award. If the Bidder, or, if the Bidder is a joint venture and if any member of the joint venture, is subject to the FCP, evidence of its commitment must be provided before the award of the Contract.

Suppliers who have been declared ineligible contractors by Human Resources and Skills Development Canada (HRSDC) are no longer eligible to receive government contracts over the threshold for solicitation of bids as set out in the *Government Contracts Regulations*. Suppliers may be declared ineligible contractors either as a result of a finding of non-compliance by HRSDC, or following their voluntary withdrawal from the FCP for a reason other than the reduction of their workforce to less than 100 employees. Any bids from ineligible contractors, including a bid from a joint venture that has a member who is an ineligible contractor, will be declared non-responsive.

2.   If the Bidder does not fall within the exceptions enumerated in 3.(a) or (b) below, or does not have a valid certificate number confirming its adherence to the FCP, the Bidder must fax (819-953-8768) a copy of the signed form LAB 1168, Certificate of Commitment to Implement Employment Equity, to the Labour Branch of HRSDC.

3.   The Bidder, or, if the Bidder is a joint venture the member of the joint venture, certifies its status with the FCP, as follows:

The Bidder or the member of the joint venture

(a)   ( )   is not subject to the FCP, having a workforce of less than 100 full-time or part-time permanent employees, and/or temporary employees having worked 12 weeks or more in Canada;

(b)   ( )   is not subject to the FCP, being a regulated employer under the *Employment Equity Act*, S.C. 1995, c. 44**;**

(c)   ( )   is subject to the requirements of the FCP, having a workforce of 100 or more full-time or part-time permanent employees, and/or temporary employees having worked 12 weeks or more in Canada, but has not previously obtained a certificate number from HRSDC (having not bid on requirements of $200,000 or more), in which case a duly signed certificate of commitment is attached;

(d)   ( )   is subject to the FCP, and has a valid certificate number as follows: _____ (e.g. has not been declared an ineligible contractor by HRSDC.)

Further information on the FCP is available on the HRSDC Web site (http://www.hrsdc.gc.ca/eng/labour/equality/fcp/index.shtml).

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

2. **Former Public Servant Certification**

Contracts with 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 the spending of public funds. In order to comply with Treasury Board policies and directives on contracts with FPS, bidders must provide the information required below.

Definitions
For the purposes of this clause,"former public servant" is any former member of a department as defined in the Financial Administration Act, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

    a.an individual;
    b.an individual who has incorporated;
    c.a partnership made of former public servants; or
    d.a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means, a pension or annual allowance paid under the Public Service Superannuation Act (PSSA), R.S., 1985, c.P-36, and any increases paid pursuant to the Supplementary Retirement Benefits Act, R.S., 1985, c.S-24 as it affects the PSSA. It does not include pensions payable pursuant to the Canadian Forces Superannuation Act, R.S., 1985, c.C-17, the Defence Services Pension Continuation Act, 1970, c.D-3, the Royal Canadian Mounted Police Pension Continuation Act , 1970, c.R-10, and the Royal Canadian Mounted Police Superannuation Act, R.S., 1985, c.R-11, the Members of Parliament Retiring Allowances Act , R.S., 1985, c.M-5, and that portion of pension payable to the Canada Pension Plan Act, R.S., 1985, c.C-8.

Former Public Servant in Receipt of a Pension
As per the above definitions, is the Bidder a FPS in receipt of a pension? Yes ( ) No ( )

If so, the Bidder must provide the following information, for all FPS in receipt of a pension, as applicable:

        a.name of former public servant;
        b.date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

Work Force Reduction Program
Is the Bidder a FPS who received a lump sum payment pursuant to the terms of a work force reduction program?
        Yes ( ) No ( )

If so, the Bidder must provide the following information:

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

a. name of former public servant;
b. conditions of the lump sum payment incentive;
c. date of termination of employment;
d. amount of lump sum payment;
e. rate of pay on which lump sum payment is based;
f. period of lump sum payment including start date, end date and number of weeks;
g. number and amount (professional fees) of other contracts subject to the restrictions of a work force reduction program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including the Goods and Services Tax or Harmonized Sales Tax.

3.   Status and Availability of Resources

The Bidder certifies that, should it be awarded a contract as a result of the bid solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the bid solicitation or agreed to with Canada's representatives. If for reasons beyond its control, the Bidder is unable to provide the services of an individual named in its bid, the Bidder may propose a substitute with similar qualifications and experience. The Bidder must advise the Contracting Authority of the reason for the substitution and provide the name, qualifications and experience of the proposed replacement. For the purposes of this clause, only the following reasons will be considered as beyond the control of the Bidder: death, sickness, maternity and parental leave, retirement, resignation, dismissal for cause or termination of an agreement for default.

If the Bidder has proposed any individual who is not an employee of the Bidder, the Bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Bidder and of his/her availability. Failure to comply with the request may result in the bid being declared non-responsive.

4.   Education and Experience

The Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.

5.   Language Capability

The Bidder certifies that it has the language capability required to perform the Work, as stipulated in the Statement of Work.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

ATTACHMENT 6

CERTIFICATIONS REQUIRED WITH THE BID

1. Canadian Content Certification

This procurement is conditionally limited to Canadian goods and Canadian services.

Subject to the evaluation procedures contained in the bid solicitation, bidders acknowledge that only bids with a certification that the goods and services offered are Canadian goods and Canadian services, as defined in clause A3050T, may be considered.

Failure to provide this certification completed with the bid will result in the goods and services offered being treated as non-Canadian goods and non-Canadian services.

The Bidder certifies that:

( )   a minimum of 80 percent of the services delievered under the contract consist of Canadian services as defined in paragraph 5 of clause A3050T.

( )   a minimum of 90 percent of the services delievered under the contract consist of Canadian services as defined in paragraph 5 of clause A3050T.

( )   100 percent of the services delievered under the contract consist of Canadian services as defined in paragraph 5 of clause A3050T.

For more information on how to determine the Canadian content for a mix of goods, a mix of services or a mix of goods and services, consult Annex 3.6.(9), Example 2, of the Supply Manual.

(http://www.tpsgc-pwgsc.gc.ca/app-acq/ga-sm/chapitre03-chapter03-eng.html)

The Bidder certifies that:

( )   a minimum of 20 percent of the goods delievered under the contract consist of Canadian goods as defined in paragraph 5 of clause A3050T.

( )   a minimum of 40 percent of the goods delievered under the contract consist of Canadian goods as defined in paragraph 5 of clause A3050T.

( )   a minimum of 60 percent of the goods delievered under the contract consist of Canadian goods as defined in paragraph 5 of clause A3050T.

( )   a minimum of 80 percent of the goods delievered under the contract consist of Canadian goods as defined in paragraph 5 of clause A3050T.

( )   100 percent of the goods delievered under the contract consist of Canadian goods as defined in paragraph 5 of clause A3050T.

For more information on how to determine the Canadian content for a mix of goods, a mix of services or a mix of goods and services, consult Annex 3.6.(9), Example 2, of the Supply Manual.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

(http://www.tpsgc-pwgsc.gc.ca/app-acq/ga-sm/chapitre03-chapter03-eng.html)

1.1   SACC Manual clause A3050T (2010-01-11), Canadian Content Definition

2.   Certification of Summary of Corporate Experience Presentation Sheets

This procurement includes an evaluation of demonstration of successful client acceptance of previously completed projects.

The Bidder certifies that:

( ) all projects included for the purpose of evaluating past project experience through completion of Summary of Corporate Experience Presentation Sheets, have been successfully completed as evidenced by client acceptance of project deliverables.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

ANNEX A

STATEMENT OF WORK

The Statement of Work (Annex A) appended to the bid solicitation is to be inserted at this point and forms part of this document.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

ANNEX B

SYSTEM TECHNICAL SPECIFICATION

The System Technical Specification (Annex B) and System Technical Specification Table are available at the following link is to be inserted at this point and forms part of this document:
https://partners.drdc-rddc.gc.ca/centres/Ottawa/NIO/ARMOUR_TD/rfp/Shared%20Documents

To access Annex B please refer to the instructions in Section 6. Applicable and Reference Documentation of Part 2 - Bidder Instructions of the Solicitation.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

ANNEX C

BASIS OF PAYMENT

1.   Basic Requirement

A Firm All Inclusive Lot Price in for the Basic Requirement, as described in Annex A (excluding Appendix C - Optional Services Requirement), Statement of Work:

Table C-1

Item	All Inclusive Firm Lot Price
Basic Requirement as described in Annex A (excluding Appendix C)	

2.   Optional Services Requirement

For the Optional Services Requirement described in Appendix C to the Statement of Work in Annex A:

2.1   Labour: at the following Firm All Inclusive Hourly Rates

Table C-2

Labour Category	Firm All Inclusive Hourly Rates					
	Interim Labour Rates subject to escalation in accordance with 2.1 Escalation of Labour Rates of this Annex					
	Year 1*	Year 2	Year 3	Year 4	Year 5	Year 6
Project Management						
Project Manager (PM)						
Project Communications Specialist (PCS)						
Project Control Officer (PCO)						
Webmaster (WM)						
System Architecture and Design						
Lead System of Systems Architect (LSA)						
Software Solution Architect (SSA)						
System/Network Analyst (SNA)						
Technical Writer (TW)						
User Interface Analyst (UIA)						
Hardware Architect (HA)						

Solicitation No. - N° de l'invitation | Amd. No. - N° de la modif. | Buyer ID - Id de l'acheteur
W7714-115274/E | | 056sv
Client Ref. No. - N° de réf. du client | File No. - N° du dossier | CCC No./N° CCC - FMS No./N° VME
W7714-115274 | 056svW7714-115274 |

Data Warehouse Architect (DWA)						
Computer Network Defence Functional Analyst (CNDFA)						
Information Technology Security Analyst (ITSA)						
Information Technology Certification and Accreditation Specialist (CAS)						
System Programming						
Senior Programmer (SP)						
Intermediate Programmer (IP)						
Junior Programmer (JP)						
Senior Web-Services Developer (SWD)						
System Engineering and Operations						
Operating Systems Administrator (OSA)						
Project Test Coordinator (PTC)						
Quality Assurance Specialist (QAS)						
Tester (TES)						

* Year 1 of the Optional Services Requirement option period, if exercised, will begin no later than completion of the Basic Requirement work and end 12 months after completion of the Basic Requirement.

2.1.1 Escalation of Labour Rates

For each subsequent option year after the first option year, the labour rates will be subject to adjustment equivalent to the annual percent change in the Consumer Price Index, "All Items", (Not Seasonally Adjusted) for Ottawa-Gatineau, Statistics Canada Table 11, for the eleventh (11th) month of the previous option period or, in the case of the Year 2 option period, the eleventh (11th) month after completion of the Basic Requirement, as published by Statistics Canada if the annual percent change is greater than 2%.

2.2   HARDWARE AND SOFTWARE: at actual cost without markup   Est.: $ _____

For the following categories of technology as per the ARMOUR System Technical Specification:

· Data Sources;
· Infrastructure Management Systems;
· Data Source Connectors;
· Database Modules;
· Data Presentation:
· Computational Services;
· Integration Framework;

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

·   Effector Connectors; and
·   Effectors.

All licenses are to be perpetual licenses for the latest software version at the time of purchase.

2.3   **MARK-UP ON HARDWARE AND SOFTWARE:**
     Estimate Based on $100,000.00 (GST/HST extra for 2.2 Hardware and Software

             Est.: $ _____

2.4   **TRAVEL AND LIVING EXPENSES:**   Est.: $ _____

Travel required for project management and other tasks within the NCR will not be reimbursed.

It is anticipated that limited travel outside of the NCR, but within Canada, will be required in support of some Work performed under the Optional Services Requirement. For travel outside the NCR the Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal, private vehicle and incidental expenses provided in Appendices B, C and D of the Treasury Board Travel Directive and with the other provisions of the directive referring to "travellers", rather than those referring to "employees" are applicable. All travel must have prior authorization of the Technical Authority. All payments are subject to government audit. Travel outside the NCR will be specified for each individual task using DND form 626.
(http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_113/td-dv_e.asp)

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

Annex D

Security Requirements Check List

The Security Requirements Check List (SRCL) (Annex D) appended to the bid solicitation package is to be inserted at this point and forms part of this document.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

Annex E

DND 626, Task Authorization Form

DEPARTMENT OF NATIONAL DEFENCE
TASK AUTHORIZATION

MINISTERE DE LA DEFENSE NATIONAL
AUTORISATION DES TÂCHES

ALL INVOICES, SHIPPING BILLS, AND PACKING SLIPS MUST SHOW THE FOLLOWING AGREEMENT, REFERENCE NUMBERS:
TOUTES LES FACTURES, TOUS LES CONNAISSEMENTS ET BORDEREAUX D'EMBALLAGE DOIVENT INDIQUER LES NUMEROS SUIVANTS RELATIFS AU CONTRAT:

*Agreement/Contract No.
*No de la convention ou du contrat

Cost Centre	Organisation Code Code d'organisation	COB/FEE/ FMAS	S.A. Sous Rep	WBS/Internal Order	G/L Account	Amount Montant
9-15	22-27	28-34	35-36	37-41	42-46	47-56
						$ (Including GST)

Reqn. No. - No de la demande

TASK No.

TO – A

Company Name and Address:

ATTN: Company Contract Manager Name

DELIVER TO - EXPEDIEZ A

DELIVERY DATE – DATE DE LIVRAISON

TO THE CONTRACTOR

You are requested to supply the following materiel/services in accordance with the terms of the above reference contract. Only materiel/services included in the contract shall be supplied against this task.
Each delivery shall be accompanied by a packing note or delivery slip.
Please advise the undersigned if the delivery date cannot be met. Invoices shall be prepared in accordance with the instructions set out in the contract.

A L'ENTREPENEUR

Vous êtes prié de fournir le matériel ou les services suivants en conformité des termes du contrat mentionné ci-dessus. Seuls le matériel ou les services mentionnés dans le contrat doivent être fournis à l'appui de cette demande. Chaque livraison doit être accompagnée d'un bordereau d'emballage ou de livraison. Prière d'aviser le signataire si la livraison ne peut se faire dans les délais prescrits. Les factures doivent être établies selon les instructions énoncées dans le contrat.

Date — for Department of National Defence
Pour le Ministère de la Défense Nationale

Date — for DRDC Procurement Authority
Pour l'autorité d'approvisionnement du RDDC

Contract Items No. No d'article du contrat	Materiel/Services Matériel/Services	Cost Prix
	GST/HST TPS/TVH	
	Total	

APPLICABLE ONLY TO PWGSC CONTRACTS: The Contract Authority signature is required when the total value of the DND 626 exceeds the threshold specified in the contract.

NE S'APPLIQUE QU'AUX CONTRATS DE TPSGC : La signature de l'autorité contractante est requise lorsque la valeur totale du formulaire DND 626 est supérieure au seuil précisé dans le contrat.

for the Department of Public Works and Government Services
pour le ministère des Travaux publics et services gouvernementaux

DND 626 (01-85)

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

Instructions for completing DND 626 - Task Authorization

Contract no.
Enter the PWGSC contract number in full.

Task no.
Enter the sequential Task number.

Amendment no.
Enter the amendment number.when the original Task is amended to change the scope or the value.

Increase/Decrease
Enter the increase or decrease total dollar amount including taxes.

Previous value
Enter the previous total dollar amount including taxes.

To
Name of the contractor.

Delivery location
Location where the work will be completed, if other than the contractor's location.

Delivery/Completion date
Completion date for the task.

for the Department of National Defence
Signature of the DND person who has delegated Authority for signing DND 626 (level of authority based on the dollar value of the task and the equivalent signing authority in the delegation of financial authorities).
Note: the person signing in this block ensures that the work is within the scope of the contract, that sufficient funds remain in the contract to cover this task and that the task is affordable within the Project/Unit budget.

Materiel/Services
Define the requirement briefly (attach the SOW) and identify the cost of the task using the contractor's quote on the level of effort. The Task must use the basis of payment stipulated in the contract. If there are several basis of payment then list here the one(s) that will apply to the task quote (e.g. milestone payments; per diem rates/labour category hourly rates; travel and living rates; firm price/ceiling price, etc.). All the terms and conditions of the contract apply to this Task Authorization and cannot be ignored or amended for this task. Therefore it is not necessary to restate these general contract terms and conditions on the DND 626 Task form.

Cost
The cost of the Task broken out into the individual costed items in Services.

GST/HST
The GST/HST cost as appropriate.

Total
The total cost of the task. The contractor may not exceed this amount without the approval of DND indicated on an amended DND 626. The amendment value may not exceed 50% (or the percentage for amendments established in the contract) of the original value of the task authorization. The total cost of a DND 626, including all amendments, may not exceed the funding limit identified in the contract.

Applicable only to PWGSC contracts
This block only applies to those Task Authorization contracts awarded by PWGSC. The contract will include a specified threshold for DND sole approval of the DND 626 and a percentage for DND to approve amendments to the original DND 626. Tasks that will exceed these thresholds must be passed to the PWGSC Contracting Authority for review and signature prior to authorizing the contractor to begin work.

Note:
Work on the task may not commence prior to the date this form is signed by the DA Authority - for tasks within the DND threshold; and by both DND and PWGSC for those tasks over the DND threshold.

Instructions pour compléter le formulaire DND 626 - Autorisation des tâches

N° du contrat
Inscrivez le numéro du contrat de TPSGC en entier.

N° de la tâche
Inscrivez le numéro de tâche séquentiel.

N° de la modification
Inscrivez le numéro de modification lorsque la tâche originale est modifiée pour en changer la portée.

Augmentation/Réduction
Inscrivez le montant total de l'augmentation ou de la diminution, y compris les taxes.

Valeur précédente
Inscrivez le montant total précédent, y compris les taxes.

A
Nom de l'entrepreneur.

Expédiez à
Endroit où le travail sera effectué, si celui-ci diffère du lieu d'affaires de l'entrepreneur.

Date de livraison/d'achèvement
Date d'achèvement de la tâche.

pour le ministère de la Défense nationale
Signature du représentant du MDN auquel on a délégué le pouvoir d'approbation en ce qui a trait à la signature du formulaire DND 626 (niveau d'autorité basé sur la valeur de la tâche et le signataire autorisé équivalent mentionné dans les délégations des pouvoirs financiers).
Nota : la personne qui signe cette attache de signature confirme que les travaux respectent la portée du contrat, que suffisamment de fonds sont prévus au contrat pour couvrir cette tâche et que le budget alloué à l'unité ou pour le projet le permet.

Matériel/Services
Définissez brièvement le besoin (joignez l'ET) et établissez le coût de la tâche à l'aide de la soumission de l'entrepreneur selon le niveau de difficulté de celle-ci. Les modalités de paiement stipulées dans le contrat s'appliquent à la tâche. Si plusieurs d'entre elles sont prévues, énumérez ici celle/celles qui s'appliquera/ront à la soumission pour la tâche à accomplir (p.ex. acompte fondé sur les étapes franchies; taux quotidien ou taux horaire établi selon la catégorie de main-d'oeuvre; frais de déplacement et de séjour; prix fixe ou prix plafond; etc.). Toutes les modalités du contrat s'appliquent à cette autorisation de tâche et ne peuvent être négligées ou modifiées quant à la tâche en question. Il n'est donc pas nécessaire de répéter ces modalités générales afférentes au contrat sur le formulaire DND 626.

Prix
Mentionnez le coût de la tâche en le répartissant selon les frais afférents à chaque item mentionné dans la rubrique **Services**.

TPS/TVH
Mentionnez le montant de la TPS/TVH, s'il y lieu.

Total
Mentionnez le coût total de la tâche. L'entrepreneur ne peut dépasser ce montant sans l'approbation du MDN, formulaire DND 626 modifié à l'appui. Le coût de la modification ne peut pas être supérieur à 50 p. 100 du montant initial prévu dans l'autorisation de tâche (ou au pourcentage prévu dans le contrat pour les modifications). Le coût total spécifié dans le formulaire DND 626, y compris toutes les modifications, ne peut dépasser le plafond de financement mentionné dans le contrat.

Ne s'applique qu'aux contrats de TPSGC
Le présent paragraphe s'applique uniquement aux autorisations de tâche accordées par TPSGC. On inscrira dans le formulaire DND 626 un plafond précis qui ne pourra être approuvé que par le MDN et un pourcentage selon lequel le MDN pourra approuver des modifications au formulaire DND 626 original. Les tâches dont le coût dépasse ces plafonds doivent être soumises à l'autorité contractante de TPSGC pour examen et signature avant qu'on autorise l'entrepreneur à débuter les travaux.

Nota :
Les travaux ne peuvent commencer avant la date de signature de ce formulaire par le responsable du MDN, pour les tâches dont le coût est inférieur au plafond établi par le MDN, et par le MDN et TPSGC pour les tâches dont le coût dépasse le plafond établi par le MDN.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

ANNEX F

ARMOUR TD PROJECT INTELLECTUAL PROPERTY STRATEGY

The Intellectual Property Strategy (Annex F) appended to the bid solicitation package is to be inserted at this point and forms part of this document.

Solicitation No. - N° de l'invitation	Amd. No. - N° de la modif.	Buyer ID - Id de l'acheteur
W7714-115274/E		056sv
Client Ref. No. - N° de réf. du client	File No. - N° du dossier	CCC No./N° CCC - FMS No./N° VME
W7714-115274	056svW7714-115274	

ANNEX G

ARMOUR TD PROJECT REFERENCE TERMINOLOGY

The Reference Terminology (Annex G) appended to the bid solicitation package is to be inserted at this point and forms part of this document.

ANNEX A

Statement of Work

for the

Automated Computer Network Defence
(ARMOUR)

Technology Demonstration
(TD)

Version

2.0

Date

18 January 2013

Table of Contents

Table of Figures

List of Tables

1.   INTRODUCTION

SCOPE

DRDC has a requirement to design, build and test a system to meet the Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) project objectives and to demonstrate the system on an operational subset of the DRDC Defence Research Establishment Network (DREnet).

1.1   Purpose

The purpose of this SOW is to define the ARMOUR TD Research and Development (R&D) activities to be undertaken by the Contractor delivering the ARMOUR TD project.

1.2   Objectives

The ARMOUR TD project has the following objectives:

1.   Demonstrate an Automated Computer Network Defence system that will:
- **Compute** defensive **courses of action** in response to identified *vulnerabilities* and *attacks*.
- **Prioritize** defensive **courses of action** to *minimize* impact to operations, and costs.
- **Proactively and reactively respond** by effectuating courses of action in a *semi-automated* (requiring operator intervention) or *fully-automated manner* (not requiring any operator intervention).
- **Compute** system **security metrics** over the *enterprise wide system* to enable comparison of *previous* and *potential* network states.

2.   Provide a framework that will:
- **Influence external Computer Network Defence (CND) programs** and easily exploit innovations by providing a system for ongoing R&D that is shared with allies, research institutions, academia and commercial industry.

1.3   Background

All modern militaries are heavily reliant upon computer networks at every stage of their missions. The network plays a crucial role in all phases, from strategic intelligence gathering and dissemination, to operational planning, logistics and command, and finally, to time-critical tactical sensing and decision making in the field. Reliance on network enabled capabilities has increased the importance of networks as part of critical service delivery. Supporting processes and technology in the area of automated CND are required to maintain the security, including confidentiality, integrity and availability, of these services. The ARMOUR TD project intends to demonstrate automated CND capabilities based on the Observe, Orient, Decide and Act (OODA) loop. The ARMOUR TD project intends to deliver an integrated and automated system that will demonstrate the capabilities required to automate the OODA loop as applied to CND.

As applied to automated CND, the Observe phase of the OODA loop represents the phase where mission priority, infrastructure and security related information is collected, correlated and stored for analysis in later phases. Generally, the state of industry capabilities to collect infrastructure and security related information are considered mature as there are many products available to collect network and host related data as well as security vulnerability information. The DRDC Joint Network Defence and Management System (JNDMS) TD project (2004 – 2010) demonstrated capabilities for collection of not only network infrastructure and security related data, but also information related to operational mission priorities and criticality of services and equipment. Areas where additional development will be performed by the ARMOUR TD project include methods to cross-correlate information from multiple sources to uniquely identify hosts and software and also to reduce the false positive rate of incidents and alarms.

The Orient phase of the OODA loop represents the phase where the data collected in the Observe phase is initially analyzed to compute the operational priority of assets, potential cyber attack paths from selected sources to high priority operational assets, and to identify attack assets that are critical to the success of an attack path. Industry capabilities in this area are maturing, but are not considered mature today. Some products are available to predict attack paths, but these do not consider the operational priority of assets in relation to mission priorities. Similarly, the mitigations are localized and do not adequately identify the key attack assets that can minimize the attack paths. Defence Research and Development Canada – Ottawa (DRDC Ottawa) Cyber Operations Section has developed prototypes for computing attack paths that leverage related academic-partner technologies. DRDC Ottawa Cyber Operations Section has also developed the AssetRank algorithm, which is designed to generate an understanding of asset values in a system by assigning a rank based on dependencies (e.g., the value of infrastructure assets based on mission priorities, and the value of assets to attackers).

The Decide phase of the OODA loop represents the phase where defensive courses of action are identified, prioritized and optimized to mitigate the attack paths identified in the Orient Phase. Examples of defensive actions may include removing a network route, shutting down a service, or applying a patch. Industry capabilities in this area are considered immature. While some commercial tools can adequately identify the many instances of vulnerabilities that need to be addressed on a network, they are incapable of identifying the optimal set of actions that would minimize attack capability while also minimizing the impact to operations. DRDC Ottawa Cyber Operations Section has developed the Course of Action Decision Support (COADS) algorithm, which is designed to generate course of action recommendations that optimize the spending of limited resources in order to minimize attackers' freedom to move toward defence goals while also minimizing the impact to operational capabilities.

The Act phase of the OODA loop represents the phase where defensive courses of action are implemented on the network. These actions may be implemented in a semi-automated manner involving human intervention to effectuate the course of action, or in a fully automated manner where actions are taken up to a previously accepted level of operational impact. Industry capabilities in this area are considered mature. There are several tools on the market to reconfigure assets, deploy patches, change network routes and block connections.

As an automated CND system, the intent of the ARMOUR TD project is to demonstrate automation in all phases of the OODA loop on an enterprise-wide basis. As such, collection of data is fully-automated to the maximum extent possible during the Observe Phase (mission priority information may be an exception to the automated data collection), fully-automated identification of attack sources, evaluation of attack paths, priority goals to protect and estimation of the overall defensive posture is fully-automated during the Orient Phase, and the generation and calculation of optimized and prioritized courses of action are fully-automated in the Decide Phase. It is only in the Act phase where some semi-automatic effectuation of the courses of action will require manual intervention. This is limited to the selection of courses of action, where these courses of action are outside pre-configured parameters that would allow fully-automated selection of courses of action. After selection, the effectuation of these courses of action are again fully-automated in most cases (deployment of a patch or similar actions may include non-automated actions). In the case where the courses of action are within pre-configured parameters allowing fully-automated selection of courses of action, the courses of action are both selected and effectuated in a fully-automated manner.

In addition to the automated and semi-automated natures of the ARMOUR solution described above, ARMOUR will also provide both a proactive and a reactive capability. In the proactive case, the ARMOUR system will respond to hypothetical attack sources identified by the operator and propose courses of action to mitigate potential attack paths between these hypothetical sources and high priority operational goals to protect. In the reactive case, real-time data collected from intrusion detection systems and similar security products will identify hosts and host services with a high likelihood of compromise. These hosts with a high likelihood of compromise will then be used by the ARMOUR solution as attack sources. The ARMOUR system will respond to this automated identification of attack sources and will propose courses of action to mitigate the real attack paths between the attack source and high priority operational goals to protect.

1.4 Applicable Documents

The following references should be read in conjunction with this SOW:

- *ARMOUR TD Reference Terminology v2.0*, DRDC Ottawa, 18 January 2013, included as part of the bid package;

- *ARMOUR TD System Technical Specification v2.0*, DRDC Ottawa, 18 January 2013, access instructions included in the bid package Annex "B";

- *Technology Demonstration Program Guidebook, V2.2, January 2005; Technology Demonstration Program Exploitation Guidebook, 2005, http://www.drdc-rddc.gc.ca/sciences/guide-eng.pdf*

The following references contain information that may assist bidders in understanding the ARMOUR solution, AssetRank, and COADS.

- Sawilla, R. (2011), *Ranks and Partial Cuts in Forward Hypergraphs (Doctoral dissertation)*, https://qspace.library.queensu.ca/jspui/bitstream/1974/6484/1/Sawilla_Reginald_E_201104_PhD.pdf

1.5 Basic Requirement

The Contractor will:

a) Refine the system requirements;

b) Design the system;

c) Develop, integrate and test the system;

d) Prepare Certification and Accreditation (C&A) Documents and Evidence;

e) Perform demonstrations of the developed system, including plans, reports and demonstration instance.

f) Produce documentation relating to project management, system design, development and testing, system usage and support.

1.6 Approach

The ARMOUR TD project approach is based on the use of Commercial off-the-shelf (COTS) and Open Source software (OSS), where available, with an effort to mature and deliver Research and Development (R&D) products when mature products do not exist. A detailed description of the Intellectual Property approach is provided in the ARMOUR RFP bid package, Annex F – Intellectual Property Strategy.

The design of the ARMOUR TD project solution must be based on an Integration Framework allowing plug and play compatibility between system components. The Integration Framework will be an XML-based Service Oriented Architecture (SOA).

The ARMOUR TD project will follow a phased incremental development and demonstration approach. During each phase the Contractor will develop and demonstrate the solution or part of the solution using scenarios based on stakeholder input and requirements. Stakeholder reactions to, and lessons learned from, the demonstration of each phase will be used as input to determine the objectives and required improvements for the next phase.

One laboratory demonstration and three operational demonstrations are to be planned. The laboratory demonstration will be used to demonstrate the workings of the Integration Framework and Graphical User Interface (GUI). The first operational demonstration will include the "Proactive Observe and Orient" functions. This will include the capabilities to identify attacks that are possible before they occur. The second operational demonstration will include the "Proactive Decide and Act" functions. This will include the capabilities to prioritize courses of action and allow them to be implemented with operator approval. The third operational demonstration will include the capabilities for "Reactive Response" to detected

cyber attacks on the infrastructure. In all demonstrations, the target operational network to be used will be an operational subnet of the Defence Research Establishment network (DREnet).

DRDC intends to license a research and development version and a commercial version of the ARMOUR solution, as described in the ARMOUR RFP bid package, Annex F – Intellectual Property Strategy.

An introduction to the software components is provided in Section1.8. For a complete description of the software components, please refer to the ARMOUR TD project System Technical Specification (STS).

1.7   Stakeholders

The Contractor must consult with various DND Information Management and Information Technology (IM/IT) stakeholders to get familiarized with the operational concepts and corporate IT environment to be supported by the ARMOUR TD project delivered capabilities. These stakeholders include but are not limited to:

- Director General Cyber (DG Cyber)

- Canadian Forces Information Operations Group (CFIOG)

- Canadian Forces Network Operations Centre (CFNOC);

- Network Command and Control Integrated Situation Awareness Capability (NetC2 ISAC) project;

- Director Information Management Engineering and Integration (DIMEI);

- Director Information Management Security (DIM Secur); and

- Director Information Management Technologies, Products and Services (DIMTPS).

1.8   ARMOUR SYSTEM CONCEPTUAL ARCHITECTURE

The development scope of the ARMOUR TD project Basic Requirement includes the delivery of the technology components supporting the Observe, Orient, Decide and Act (OODA) loop functions as applied to automated Computer Network Defence (CND). The Contractor must include in their solution such components as are necessary to meet the ARMOUR TD project requirements. To the maximum extent possible, the Contractor must use a modular design approach to integrate available technologies (e.g., COTS or Open Source Software products). The technology components required in the ARMOUR TD project solution are illustrated in Figure 1 and are briefly described in this section. Additional details are provided in the System Technical Specification (STS).
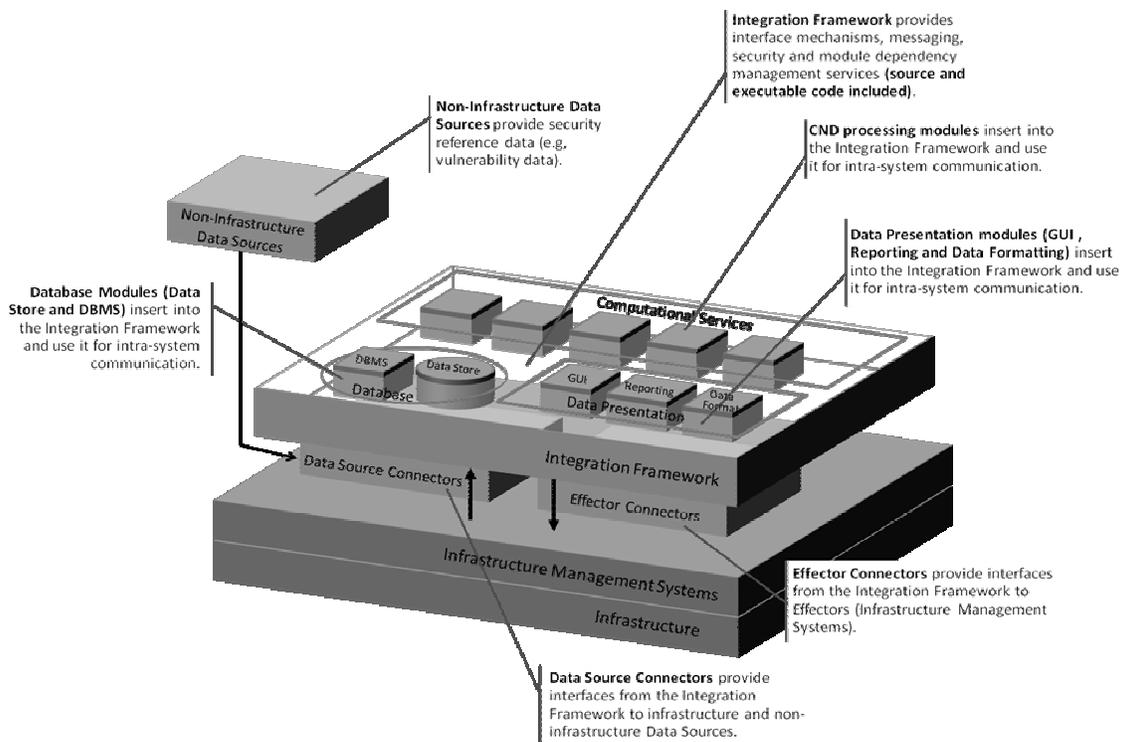
Figure 1: ARMOUR System Conceptual Architecture

Integration Framework: The Integration Framework provides a standards-based (e.g., web-services standards from W3C), open architecture software framework for the integration of all other modules comprising the solution. The Integration Framework provides inter-module messaging, security and event services between the other components and modules of the ARMOUR system;

Data Source Connectors: Data Source Connectors provide interfaces between the Database component (see below) and the various data sources being used to gather information on network data and operational conditions for the ARMOUR system. The interfaces are specific to the data sources being used and connect to both Non-Infrastructure Data Sources and Infrastructure Management Systems;

Database: The Database component includes both the Data Store and the Database Management System (DBMS). The Data Store contains all pre- and post-processed data used by the ARMOUR system. The DBMS represents an off-the-shelf (OTS) solution (e.g., PostgreSQL, Oracle, etc.) used to implement the database, data model, data security, and data archiving functions;

Computational Services: The Computational Services component provides all the functions that act upon the data in the Database component. This component contains the processes that provide analysis and computation of correlated information, potential attacks, courses of action, and prioritization. It also contains the processing modules that generate the configuration information used to implement courses of action;

Data Presentation: The Data Presentation component presents the information contained in the Database component to the operator through both a visualization interface and reporting functions, thereby providing an operator interface to the modules within the Computational Services component. The Data Presentation component also includes functions to present information to the Effector Connectors in formats supported by the Effectors;

Effector Connectors: Effector Connectors provide interfaces to the off-the-shelf (OTS) products being used to implement the courses of action. The Effector Connectors are specific to the Infrastructure Management Systems being used. Data is provided by the Data Presentation component and formatted for implementation by either automatic or manual initiation;

Infrastructure Management Systems (IMSs): IMSs consist of all distributed or centralized control systems that manage aspects of operational network and are involved in the process of data collection or execution of command on behalf of the ARMOUR system. For example, a centralized management application for configuration and control of a host based Intrusion Detection/Prevention System would be considered an IMS. Generally speaking, specific technologies in IMSs will usually also serve as Data Sources or Effectors;

Data Sources: Data Sources consist of all infrastructure and non-infrastructure based resources required to meet the information requirements for the ARMOUR system. For example, host and network based Intrusion Detection Systems would be considered to be Data Sources as would publicly available vulnerability reference databases; and

Effectors: Effectors consist of all infrastructure-based resources required by the ARMOUR system to effectuate (implement) chosen courses of action within the network. For example, host and network-based Intrusion Prevention Systems would be considered to be Effectors.

1.9 Excluded Work and Services

In some instances, automated data collection may not be available from COTS or Open Source Software products to fully address all ARMOUR TD project information requirements. For example, technologies may not be available to automatically collect information concerning DND operations or operational dependencies (e.g., mission to mission dependencies or mission to infrastructure dependencies). Where this is the case, development of automated solutions for automated data collection is excluded from the ARMOUR TD project effort. The Contractor must clearly identify which Data Sources are not available through automated data collection and provide manual workarounds in their architecture.

1.10 Available Data Sources and Effectors

Some Data Sources and Effectors may already be available on the ARMOUR TD project target demonstration network (an operational subset of DREnet). The Contractor is encouraged to leverage existing Data Sources and Effectors in their solutions to the maximum extent possible. For existing Data Sources and Effectors used in the Contractor solution, the Contractor may use the existing operational products for the operational demonstrations. However, the Contractor must integrate the available Data Sources and Effectors into their solution and ensure a functional demonstration can be packaged without dependencies on the operational demonstration environment. Therefore, the Contractor must include such technologies as may be required to support the integration of these Data Sources and Effectors (e.g., test data, equivalent products, systems or simulations). The Data Sources and Effectors that should be integrated in the ARMOUR TD project include:

a) Sourcefire Intrusion Prevention System

b) Symantec Endpoint Protection

c) McAfee Firewall

d) CheckPoint Firewall

e) McAfee Web Gateway

f) DB Protect

g) NetScout

h) Proprietary Packet Capture

While the Contractor is encouraged to leverage the available Data Sources and Effectors, it is not mandatory to do so. The ARMOUR interfaces to these products, or others that are chosen, must be standardized to enable Data Sources and Effectors to be interchanged with other comparable COTS or open source solutions.

1.11 Available Processing Modules

DRDC owns algorithms that could form part of the ARMOUR TD project. The algorithms have been implemented, tested and validated in a laboratory setting and integrated with commercial and open source software at the level of TRL 4 prototype tools. At the request of the Contractor, the algorithm implementations and prototypes can be furnished in source code form for use by the Contractor. The algorithm implementations could be provided in executable form under the ARMOUR TD project Intellectual Property Strategy. For further information on the licensing models, background Intellectual Property, and new foreground Intellectual Property, please see the ARMOUR RFP bid package Annex F.

Algorithm implementations available are:

- AssetRank is a statistical analysis system that consumes a listing of assets and their dependencies and generates an understanding of their value by assigning a ranking to the assets based upon the system dependencies. The system is stochastic, meaning there is an assumption that a random selection at one point in the system does not bias random selections at other points in the system. The system extends Google's PageRank algorithm by analyzing AND and OR vertices in a semantically consistent way, modeling diverse actors, and accounting for out-of-system influences.

- Course of Action Decision Support (COADS) is a graph analysis system that consumes a listing of assets with their rank and removal cost, their dependencies, source assets, target assets, and a maximum removal budget. COADS generates a course of action, within budget, which consists of an optimized set of asset removals which maximally disrupts connectivity between the source and target assets. When consuming a MulVAL attack graph that has been ranked with AssetRank, the course of action suggests patches to apply, services to shut down, and network routes to cut, to maximally disrupt attackers' freedom of movement between sources and targets.

The above AssetRank module consumes the output of the open source MulVAL software:

- MulVAL is a formal, logic-based reasoning system that consumes a networked system's configuration and vulnerability information and generates an understanding of its security by revealing all security consequences deducible from the input data and the MulVAL reasoning model. The reasoning model is declarative and extensible. The tool can easily incorporate external security information sources and is scalable to enterprise networks. The MulVAL system output can be presented using visualization tools and used in further analysis

1.12 Assumptions

This TD is based on the following assumptions:

a.   The ARMOUR approach is based on the technical assumption that cyber-security reference data, infrastructure data and operational data (collectively called data sources) will be available and sufficiently accurate (via existing and added capabilities) to support the requirements of the proactive and reactive cyber security monitoring and response on an operational network. For the ARMOUR TD project, a representative sample of the data sources may be all that is available. It is recognized that some analysis concerning data sources will be required for any transition from the demonstration state to an operational system. The difference between the demonstration state and the operational system state is described in the System Technical Specifications (STS).

b.   A second assumption is that operational authority, responsibility and process will be updated as needed to leverage the capabilities delivered by the ARMOUR TD project solution. The ARMOUR project will not be updating any procedures or processes in place within DRDC or DND.

1.13   Constraints

The work associated to this project is constrained as follows:

1) All ARMOUR TD project work must be completed within 42 months;

2) The ARMOUR TD project solution will not address social engineering attacks (e.g., attacks leveraging human interaction and response intended to convince an unsuspecting user to trigger a malicious action); and

3) The ARMOUR TD project solution will be limited by the capabilities of the detection sensors:

- Will not detect attacks that the sensors cannot detect; and

- Will only react to high-confidence alert data (as determined by meeting requirements for low false positive rates in incident detection technologies described in the STS) to avoid taking action on data that has a high likelihood of being erroneous.

1.14   Development Approach

The work will be partitioned into the following phases:

- Phase 1: Analysis and Design
- Phase 2: Integration Framework and Graphical User Interface (GUI) Development
- Phase 3: Proactive Observe and Orient Function Development
- Phase 4: Proactive Decide and Act Development
- Phase 5: Reactive Response Development
- Phase 6: Project Closeout

The objective of the development cycle for each phase is to develop the ARMOUR TD project functionality, test the functions and system performance, and demonstrate the capabilities. The overall development work must follow a cyclic development approach including requirements refinement, design, build, test, and demonstrate. This approach is required to:

- Increase opportunities for stakeholder feedback;
- Confirm and evaluate progress;
- Communicate progress to stakeholders; and
- Provide an opportunity to refine or redirect the project.

1.15   Test and Demonstration Approach

System Testing is used to assess and measure the overall behaviour and performance of components of the system. The Contractor must plan, setup, conduct and report on ARMOUR TD project system testing as per the Test Design Document and Test Environment (SD 003).

For phases that include a demonstration requirement, demonstrations will typically occur at the end of the phase and must be designed to allow the Technical Authority (TA) and other ARMOUR TD project stakeholders the opportunity to evaluate the overall behaviour and performance of the system in an operational environment on the DREnet. The demonstrations will be based on scenarios that reflect the real operational environment of the system. The TA and Contractor will be involved while stakeholder representatives may observe.

The Contractor must support planning, setup, conduct and report on ARMOUR Demonstrations, as well as support the evaluation of ARMOUR by the TA as per DM 001 to DM 003. The Contractor will install, integrate, and configure all baseline ARMOUR software required to support all demonstrations on the DREnet. The Contractor must continue to provide support for all demonstrations on the DREnet following this initial installation and demonstration, for the duration of the ARMOUR TD project.

Based on the demonstration results, a review of the system capabilities and readiness to enter the next phase will be carried out by the TA. The planning and design for the next phase will be completed based on this review.

In addition to the Demonstration systems installed on the DREnet, the Contractor must provide new software images for the DRDC Cyber Operations Section Lab at the end of each development phase in accordance with CDRL item SD 007. Where possible, these software images must be delivered as virtual machines (VMs) ready for installation at DRDC. Any hardware components (e.g. data sources, effectors) required to run the solution must be provided as part of the lab version of the solution. The baseline software used for each demonstration cycle will be installed at the DRDC Cyber Operations Section laboratory after successful demonstrations have been conducted. The contractor will install, integrate and configure the lab version.

2. PHASES

2.1 Phase 1 – Analysis and Design:

During this phase the Contractor must refine their understanding of the ARMOUR TD project concept of operations and requirements as well as update their proposed solution architecture. The Contractor must perform the following tasks in accordance with the descriptions provided in Appendix A – WORK Definitions:

- Project Management, including conduct of a Project Kick-off Meeting and Preliminary Design Review Meeting;

- Systems Engineering Processes;

- Interactions with DND IM, IT and Operational Stakeholders;

- Operational Concept Review and Requirements Refinement;

- Preliminary Design Refinement;

- Design and Develop Test Environment, Scenarios, Test Cases and Test Data; and

- Algorithm R&D.

Phase 1 should be completed within 5 months after receipt of contract award. Successful completion of Phase 1 will only be granted after the following Contract Deliverable Requirements List (CDRL) items have been delivered by the Contractor and reviewed and approved by the TA at a Preliminary Design Review Meeting (PDRM). Deliverables must be prepared in accordance with Data Item Descriptions (DID) provided in Appendix B – Deliverables:

a) The Project Management Plan, DID - PM 001;

b) Progress Review and Project Meeting Reports, Agendas, and Minutes – PM 002;

c) The Configuration Management Plan, DID – PM 004;

d) The Requirements Management Plan, DID – PM 005;

e) The Development Phase Plan, DID – PM 006;

f) The System Requirements Specification Document, DID – SD 001;

g) The Architectural Design Document, DID – SD 002;

h) System Hardware, Software and Documentation, DID – SD 007;

i) The Certification and Accreditation Plan, DID – SD 008;

j)   The System Concept of Operations, DID – SD 009; and

k)   Demonstration Plan, DID – DM 001.

2.2   Phase 2 – Integration Framework (IF) and Graphical User Interface (GUI)

Phase 2 will commence immediately following authorization by the TA. During this phase, the Contractor will review and update the concept of operations and requirements based on results of the stakeholder feedback from the Phase 1 work; update the system design; and develop, build and demonstrate the Integration Framework (IF) and Graphical User Interface (GUI) capability, in accordance with the ARMOUR TD project STS and any approved requirements changes or updates resulting from previous tasks. The Contractor must perform the following tasks in accordance with the descriptions provided in Appendix A – WORK Definitions:

- Project Management, including the conduct of a Critical Design Review Meeting and Readiness Review Meeting;

- Interactions with DND IM, IT and Operational Stakeholders;

- Systems Engineering and System Security Engineering Processes;

- Operational Concept Review and Requirements Refinement;

- Critical Design, including the development of the Integration and GUI Framework Critical Design, Interface Specifications and Test Plan;

- Design, Build and Test in accordance with the results of the CDRM;

- Design and Develop Test Environment, Scenarios, Test Cases and Test Data;

- Demonstrations in the DRDC Cyber Operations Section Lab;

- Verification and Validation; and

- Algorithm R&D.

Phase 2 should be completed within 6 months after initiation of Phase 2 and concludes with the Phase 3 Readiness Review Meeting. Successful completion of Phase 2 will only be granted after the following Phase 2 CDRL items have been delivered by the Contractor and reviewed and approved by the TA at the Phase 3 Readiness Review Meeting. Deliverables must be prepared in accordance with Data Item Descriptions provided in Appendix B – Deliverables:

a)   The Project Management Plan, DID - PM 001;

b)   Progress Review and Project Meeting Reports, Agendas, and Minutes – PM 002;

c)   The Configuration Management Plan, DID – PM 004;

d)   The Requirements Management Plan, DID – PM 005;

e)   The Development Phase Plan, DID – PM 006;

f)   The System Requirements Specification Document, DID – SD 001;

g)   The Architectural Design Document, DID – SD 002;

h)   The Test Design Document and Test Environment, DID – SD 003

i) The Detailed Design Document, DID – SD 004;

j) Reports of Algorithm R&D, Test, C&A, and Demonstrations, DID – SD 005, SD 006, SD 008 and DM 003;

k) System Hardware, Software and Documentation, DID – SD 007;

l) The System Concept of Operations, DID – SD 009;

m) Demonstration Plan and Demonstration Instance, DID – DM 001 and DM 002; and

n) Readiness Assessment Report, DID – PM 003.

2.3 Phase 3: First Demonstration: Proactive Observe and Orient

Phase 3 will commence immediately following authorization by the TA. During this phase, the Contractor will review and update the concept of operations and requirements based on results of the stakeholder feedback from the Phase 2 work; update the system design and develop, build and demonstrate the Proactive Observe and Orient capabilities, in accordance with the ARMOUR TD project STS and any approved requirements changes or updates resulting from previous phases. The Contractor must perform the following tasks in accordance with the descriptions provided in Appendix A – WORK Definitions:

- Project Management, including the conduct of a Critical Design Review Meeting and Readiness Review Meeting;

- Systems Engineering and System Security Engineering Processes;

- Interactions with DND IM, IT and Operational Stakeholders;

- Operational Concept Review and Requirements Refinement;

- Critical Design, including the development of the Proactive Observe and Orient capabilities Critical Design, Interface Specifications and Test Plan as well as updates to the Integration and GUI Framework as required;

- Design, Build and Test in accordance with the results of the CDRM;

- Design and Develop Test Environment, Scenarios, Test Cases and Test Data;

- Demonstrations on the DRDC DREnet;

- System Administration;

- Verification and Validation; and

- Algorithm R&D.

Phase 3 should be completed within 10 months after the approval of the Phase 3 Readiness Review (conclusion of phase 2) and concludes with a Phase 4 Readiness Review Meeting. Successful completion of Phase 3 will only be granted after the following Phase 3 CDRL items have been delivered by the Contractor and reviewed and approved by the TA at the Phase 4 Readiness Review Meeting. Deliverables will be prepared in accordance with Data Item Descriptions provided in Appendix B – Deliverables:

a) The Project Management Plan, DID - PM 001;

b) Progress Review and Project Meeting Reports, Agendas, and Minutes – PM 002;

c) The Configuration Management Plan, DID – PM 004;

d) The Requirements Management Plan, DID – PM 005;

e) The Development Phase Plan, DID – PM 006;

f) The System Requirements Specification Document, DID – SD 001;

g) The Test Design Document and Test Environment, DID – SD 003

h) The Detailed Design Document, DID – SD 004;

i) Reports of Algorithm R&D, Test, C&A, and Demonstrations, DID – SD 005, SD 006, SD 008 and DM 003;

j) System Hardware, Software and Documentation, DID – SD 007;

k) The System Concept of Operations, DID – SD 009;

l) Demonstration Plan and Demonstration Instance, DID – DM 001 and DM 002; and

m) Readiness Assessment Report, DID – PM 003.

2.4   Phase 4: Second Demonstration: Proactive Decide and Act

Phase 4 will commence immediately following authorization by the TA. During this phase, the Contractor will review and update the concept of operations and requirements based on results of the stakeholder feedback from the Phase 3 work; update the system design and develop, build and demonstrate the Decide and Act capabilities, in accordance with the ARMOUR TD project STS and any approved requirements changes or updates resulting from previous tasks. The Contractor must perform the following tasks in accordance with the descriptions provided in Appendix A – WORK Definitions:

- Project Management, including the conduct of a Critical Design Review Meeting and Readiness Review Meeting;

- Systems Engineering and System Security Engineering Processes;

- Interactions with DND IM, IT and Operational Stakeholders;

- Operational Concept Review and Requirements Refinement;

- Critical Design, including the development of the Decide and Act capabilities Critical Design, Interface Specifications and Test Plan as well as updates to the Integration and GUI Framework as required;

- Design, Build and Test in accordance with the results of the CDRM;

- Design and Develop Test Environment, Scenarios, Test Cases and Test Data;

- Demonstrations on the DRDC DREnet;

- System Administration;

- Verification and Validation;

- Algorithm R&D; and

- Licensed Research Community Code Hosting and Maintenance.

Phase 4 should be completed within 10 months after the approval of the Phase 4 Readiness Review (conclusion of phase 3) and concludes with a Phase 5 Readiness Review Meeting. Successful completion of Phase 4 will only be granted after the following Phase 4 CDRL items have been delivered by the Contractor and reviewed and approved by the TA at the Phase 5 Readiness Review Meeting. Deliverables must be prepared in accordance with Data Item Descriptions provided in Appendix B – Deliverables:

a) The Project Management Plan, DID - PM 001;

b) Progress Review and Project Meeting Reports, Agendas, and Minutes – PM 002;

c) The Configuration Management Plan, DID – PM 004;

d) The Requirements Management Plan, DID – PM 005;

e) The Development Phase Plan, DID – PM 006;

f) The System Requirements Specification Document, DID – SD 001;

g) The Test Design Document and Test Environment, DID – SD 003

h) The Detailed Design Document, DID – SD 004;

i) Reports of Algorithm R&D, Test, C&A, and Demonstrations, DID – SD 005, SD 006, SD 008 and DM 003;

j) System Hardware, Software and Documentation, DID – SD 007;

k) The System Concept of Operations, DID – SD 009;

l) Demonstration Plan and Demonstration Instance, DID – DM 001 and DM 002;

m) Code Repository, DID – DM 004; and

n) Readiness Assessment Report, DID – PM 003.

2.5 Phase 5: Third Demonstration: Reactive Response

Phase 5 will commence immediately following authorization by the TA. During this phase, the Contractor will review and update the concept of operations and requirements based on results of the stakeholder feedback from the Phase 4 work; update the system design and develop, build and demonstrate the Reactive Response capabilities, in accordance with the ARMOUR TD project STS and any approved requirements changes or updates resulting from previous tasks. The Contractor must perform the following tasks in accordance with the descriptions provided in Appendix A – WORK Definitions:

- Project Management, including the conduct of a Critical Design Review Meeting and Readiness Review Meeting;

- Systems Engineering and System Security Engineering Processes;

- Interactions with DND IM, IT and Operational Stakeholders;

- Operational Concept Review and Requirements Refinement;

- Critical Design, including the development of the Reactive Response capabilities Critical Design, Interface Specifications and Test Plan as well as updates to the Integration and GUI Framework as required;

- Design, Build and Test in accordance with the results of the CDRM;

- Design and Develop Test Environment, Scenarios, Test Cases and Test Data;

- Project Demonstrations on the DRDC DREnet;

- System Administration;

- Verification and Validation; and

- Licensed Research Community Code Hosting and Maintenance.

Phase 5 should be completed within 7 months after the approval of the Phase 5 Readiness Review (conclusion of phase 4) and concludes with the Phase 6 Readiness Review Meeting. Successful completion of Phase 5 will only be granted after the following Phase 5 CDRL items have been delivered by the Contractor and reviewed and approved by the TA at the Phase 6 Readiness Review Meeting. Deliverables must be prepared in accordance with Data Item Descriptions provided in Appendix B – Deliverables. Note, in many cases these documents are considered final updates based on results of the Phase 5 work:

a) The Project Management Plan, DID - PM 001;

b) Progress Review and Project Meeting Reports, Agendas, and Minutes – PM 002;

c) The Configuration Management Plan, DID – PM 004;

d) The Requirements Management Plan, DID – PM 005;

e) The Development Phase Plan, DID – PM 006;

f) The System Requirements Specification Document, DID – SD 001;

g) The Test Design Document and Test Environment, DID – SD 003

h) The Detailed Design Document, DID – SD 004;

i) Reports of Algorithm R&D, Test, C&A, and Demonstrations, DID – SD 005, SD 006, SD 008 and DM 003;

j) System Hardware, Software and Documentation, DID – SD 007;

k) The System Concept of Operations, DID – SD 009;

l) Demonstration Plan and Demonstration Instance, DID – DM 001 and DM 002;

m) Code Repository, DID – DM 004; and

n) Readiness Assessment Report, DID – PM 003.

2.6 Phase 6: TD Final Deliverables, and TD Project Close-out

Phase 6 will commence immediately following authorization by the TA. The objective of this phase is to complete the TD project, finalize and provide DRDC with the deliverables, document the results and position the project for a successful transition to the client. The Contractor must produce a final report that summarizes the lessons learned from phases 1 to 5, user feed-back progression along the project, and the recommendations for operational deployment of the system. The Contractor must perform the following tasks in accordance with the descriptions provided in Appendix A – WORK Definitions:

- Project Management, including the conduct of a Final Review Meeting;

- System Administration;

- Licensed Research Community Code Hosting and Maintenance; and

- TD Close-out.

Phase 6 should be completed within 1 month of the completion of Phase 5 and concludes with a Final Review Meeting. Successful completion of Phase 6 will only be granted after the following CDRL items have been delivered by the Contractor and reviewed and approved by the TA at the Final Review Meeting. Deliverables must be prepared in accordance with Data Item Descriptions provided in Appendix B – Deliverables:

a) Progress Review and Project Meeting Reports, Agendas, and Minutes – PM 002;

b) Final Report, DID – PM 007; and

c) Transition Plan, DID – PM 008

3. ADDITIONAL REQUIREMENTS

3.1 Technical Requirements

Research activities: Some ARMOUR TD project functionalities will be addressed by existing COTS technologies. However, other functionalities will require research to reach an acceptable solution. An example of such an area is the development of the Reachability Analyzer. A more complete description of the challenges involved in the ARMOUR TD project is provided in the STS document. The Contractor project team must have the expertise to carry out this research.

3.2 Management Requirements

Project Manager: The Contractor must appoint one person to act as the Contractor project manager (PM). The PM must be vested with the appropriate authority within the Contractor's organization to plan, co-ordinate, control and supervise Contractor professional resources and have the authority to allocate financial resources.

Work site: The development work must be carried out at the Contractor's own facilities. The demonstrations must be held at Crown facilities.

Language Requirements: All deliverables must be submitted in English.

3.3 Government Supplied Services

Access to stakeholders: The TA will facilitate access to representatives of the military clients, as well as with other departmental and international stakeholders, who may provide feedback and pertinent knowledge that the Contractor could use in the development of the ARMOUR TD project.

Laboratory and Networks: The DRDC Cyber Operations Section laboratory and network will be made available to the Contractor for demonstration purposes. However, this does not include DRDC networking equipment and software licenses.

Parallel research considerations: It is expected that separate but related DRDC research initiatives will be conducted in parallel to the ARMOUR TD project contract. The results of these parallel activities, such as algorithms, Government-of-the-shelf (GOTS) technology or processes, could be made available to the Contractor. Current related research includes attack graph generation and evaluation, courses of action optimization and recommendation, defensive posture assessment, situational awareness concept definitions, and impact assessment algorithms.

APPENDIX A – WORK DEFINITIONS

1. WORK DEFINITIONS

1.1 Project Management

Project management activities relate the process of leading, planning, organising, staffing, monitoring and controlling contractor activities and resources, in order to achieve contract objectives. The Contractor will perform project management, within its organization, to ensure successful development of the ARMOUR TD project. This function will be continuously ongoing during the entire ARMOUR TD project lifetime (Phases 1-6).

The Contractor must refine the project management plan proposed in response to the RFP and maintain this plan through periodic updates during each phase. The project management plan will be developed in such a way as to support the development activities required to demonstrate the functional capabilities described in Section 5 and 6 of the ARMOUR TD project STS, while meeting the performance targets as described in Section 6.2 of the STS.

The Contractor must hold, as part of the project management function, various meetings with the TA during the lifetime of the ARMOUR TD project. These meetings will include:

- Project Kick-off Meeting:

    1) Frequency: once, at the beginning of Phase 1.

    2) Location: DRDC Ottawa

The kick-off meeting will be held at the start of the contract that will review the overall project including work content, schedule, technical and procedural issues, and contract deliverables.

- Progress Review Meetings

    1) Frequency: weekly, unless mutually agreed otherwise.

    2) Location: Normally via audio conference or videoconference. May be scheduled at DRDC Ottawa.

- Preliminary Design Review Meetings

    1) Frequency: Once during Phase 1, for a formal design review, and as required to discuss any technical issues during the project.

    2) Location: Normally at DRDC Ottawa. May be held at the Contractor's facility, subject to approval by the TA. Conducting these meetings via videoconference or audio conference facilities may be permitted subject to approval of the TA.

- Critical Design Review Meetings

    1) Frequency: Once during Phases 2, 3, 4 and 5, for a formal design review, and as required to discuss any technical issues during the project.

    2) Location: Normally at DRDC Ottawa. May be held at the Contractor's facility, subject to approval by the TA. Conducting these meetings via videoconference facilities may be permitted subject to approval by the TA.

- Readiness Review Meetings

    1) Frequency: At the end of each phase.

2) <u>Location:</u> Normally at DRDC Ottawa. May be held at the Contractor's facility, subject to approval by the TA. Conducting these meetings via videoconference facilities May be permitted subject to approval by the TA.

- Final Review Meeting

1) <u>Frequency:</u> Once, at the end of Phase 6.

2) <u>Location:</u> DRDC Ottawa

1.2   Consultations with DND IM/IT and Operational Stakeholders

The Contractor must consult DRDC and various DND IM/IT and Operational stakeholders to become familiar with the operational and corporate IT environment. This could include periodic meetings with the operational clients, related DND projects staff, DND engineering and security organisations. Consultations will be coordinated by the Contractor in consultation with the TA.

The objective of these consultations is to ensure the testing and demonstration environments are representative of the true operational environment. It will also provide valuable input for the refinement of system requirements and in the development of representative test cases and scenarios. Finally, multi-lateral communication with the various IM/IT organisations will facilitate the partial deployment of ARMOUR on the operational network supporting the phase specific demonstrations.

1.3   Systems Engineering and System Security Engineering Processes

Throughout the ARMOUR TD project, the Contractor must follow industry best practice for Systems Engineering process. This will include at minimum the following activities:

- Deliver, maintain and follow a Project Management Plan (PM 001) that includes processes and methodologies for system and software development planning;

- Deliver, maintain and follow a Configuration Management Plan (PM 004);

- Deliver, maintain and follow a Requirements Management Plan (PM 005);

- Deliver, maintain and follow a phase-by-phase Development Phase Plan (PM 006);

- Deliver, maintain and follow a system Certification and Accreditation Plan (SD 008);

1.4   Operational Concept Review and Requirements Refinement

The Contractor will initially develop the Operational Concept and Requirements Specification based on a review of the ARMOUR TD project STS and interactions with DND IM/IT and Operational stakeholders. The results of the Operational Concept and Requirements review must be documented in accordance with CDRL items SD 009 and SD 001 and must include security requirements in addition to functional capability requirements. During each subsequent development phase, the Contractor must review the ARMOUR operational concept and requirements on an ongoing basis and ensure that that they meet project goals and making updates to DID SD 009 and SD 001 as required.

The Contractor will refine requirements and respond to requirement changes. The nature of this TDP project is such that technical requirements are likely to evolve or change during the course of the development effort. The Contractor may consult the TA for feedback on the requirements. Requirements must be documented at the beginning of each Phase and refined after each development cycle of a phase. The Contractor Requirements Management Plan (PM 005) must include a change management process to ensure appropriate review and approval of scope, cost, personnel and schedule impacts of changing requirements. This change management process must include review and final approval of all requirements change by the ARMOUR TD project TA.

1.5 Preliminary Design Refinement

The Contractor will refine the Contractor proposed architecture in light of the requirements refinement described in Appendix A, Section 1.2 and 1.4. The Contractor must refine, and finalize the overall system Architectural Design Document (SD 002), starting from the initially proposed solution. As part of this task, the Contractor will hold a PDRM with the TA to review the proposed system architecture.

The Contractor will be required to justify their selection of COTS and Open Source software to the TA as described in the Data Item Description for the Architectural Design Document (SD 002).

The Contractor will conduct a technology watch on related software product families during the project. In cases where this survey identifies software that would add significant value to the project, the Contractor must consider integrating this software as part of the ARMOUR TD project. Any inclusion of software identified as part of the technology watch must be justified as described in the Architectural Design Document (SD 002) above and complete the change management process as captured in the Configuration Management Plan (PM 004).

1.6 Critical Design

The Contractor must develop the critical design of the ARMOUR TD project to a sufficient level of detail such that the system can be built and tested by the Contractor and evaluated by the TA. The initial critical design must be documented in the Detailed Design Document (SD 004). The work must be completed during Phase 2 with additional critical design work carried out during the development cycles of Phase 3 to 5 as the development proceeds. The contract must employ IT Security Engineering activities to ensure that resulting design will be sufficient to meet or exceed the requirements for an Interim Authority to Process (IAP), in accordance with the DND Certification and Accreditation Guidelines[1]. The Certification and Accreditation work must be carried out according to a C&A Plan (SD 008).

1.7 Design, Build and Test

The Contractor must Design, Build and Test the ARMOUR TD system during Phases 2-5 in accordance with the approved ARMOUR Critical Design. The Contractor must conduct activities such as detailed design, coding, integrating and testing units, components and systems (including penetration tests) that are part of the ARMOUR solution. The Contractor must also assemble, compile and perform any other activities associated with the delivery of the ARMOUR TD project solution to the TA.

This task also includes Contractor testing as part of the Contractor's quality assurance processes. Visibility into these processes must be granted upon request by the TA.

1.8 Design and Develop Test Environment, Scenarios, Test Cases and Test Data

The Contractor must design and develop the Test Environment, Scenarios, Test Cases and Test Data required to verify the capabilities developed during Phases 2-5.

The Contractor must, subject to the approval of the TA:

- Define the testing strategy and expected outcomes in such a way as to demonstrate that the solution delivers the required functions, meets the required measures of performance, and meets the required metrics (Refer to the ARMOUR TD project STS for details concerning measures of performance and metrics);

- Develop and validate the testing scenarios;

- Develop and validate the system test environment. The test environment will include the development of a Contractor Test Bed, the DRDC Cyber Operations Section laboratory, and the Operational Test Environment (a subset of the DRDC Ottawa DREnet);

- Develop test cases which are compatible with previously identified functions, system performance metrics, and expected test results; and

- Develop Test Data as required to fully test and demonstrate that the ARMOUR TD project solution delivers the required functions and meets system performance metrics. Test Data may include any or all aspects of the data required for system testing and demonstration in the Contractor Test Bed, DRDC Cyber Operations Section laboratory and the Operational Test Environment.

1.9 Demonstrations and Evaluations

Demonstrations are vital for maintaining operational client support and for generating national and international interest in the ARMOUR TD project. ARMOUR evaluations must occur at the end of each development phase 2 to 5. These evaluations will take the form of ARMOUR TD Project Demonstrations in which the TA and the stakeholders will execute the Test Scenarios and Test Cases as described in Section 1.8. The Contractor must setup, conduct and report on ARMOUR evaluations performed by the TA and stakeholders. The intent of the ARMOUR TD Project Demonstrations are: evaluate the system and the quality of the resulting capabilities in accordance with the Test Environment, Test Scenarios and Test Data as described in Section 1.8; compare the results to the expected outcomes and expected test results; and direct (or re-direct) the project accordingly. Each evaluation will represent a key evaluation exercise within the ARMOUR TD project.

The Contractor must supply all System Hardware, Software and supporting documentation and code as needed to support the demonstrations in accordance with SD 007.   The Contractor must install and configure the ARMOUR TD system in accordance with the approved test scenarios and provide technical and operational support to the TA during the demonstrations. It is expected that a period of one to two weeks will be reserved for demonstration support at the end of each development phase. This does not include time that must be allocated for demonstration installation, configuration and test prior to the demonstration period itself.

Planned demonstrations will be conducted at DND facilities within the National Capital Region (NCR). The demonstrations will take place in a DND unclassified operational network environment (DREnet). The Contractor must allocate appropriate resources to support the TA, DND Information Management (IM), IT and security organisations, as well as the stakeholders, to deploy ARMOUR and integrate demonstration scenarios with the environment. Demonstration capabilities, including required hardware and software, must be left in place after demonstrations; however, the hardware and software need not be maintained or supported by the Contractor between demonstrations, and may be reused in future demonstrations.

The Contractor must also provide technical and operational support for ad-hoc demonstrations during the project. The Contractor must allocate appropriate resources for a minimum of 15 person-days per development phase in order to support these ad-hoc demonstrations. Support for ad-hoc demonstrations must also include the production of supporting demonstration material and other communications activities for the TA.

1.10 System Administration

The Contractor must provide support services for the ARMOUR instances residing on DND sites (refer to deliverable DM 001 and SD 007). These services include workstation configuration, software product installation and maintenance, user support and troubleshooting. These services

must extend from the start of the first demonstration (Phase 3) and continue for the duration of the project to the end of the project Close-out (Phase 6).

1.11   Verification and Validation

The Contractor will deliver software images to DRDC after the successful completion of each Demonstration phase and must assist DRDC in the installation, integration and configuration of all baseline software in the DRDC Cyber Operations Section laboratory in accordance with deliverable SD 007. Software images must include both a source code repository and executable code as used in the corresponding Demonstration.   The Contractor will assist DRDC as DRDC performs independent Verification and Validation activities leading to software acceptance. Verification and validation activities are necessary to ensure that the DRDC Cyber Operations Section lab maintains a proper and working system necessary to support their fundamental research goals and activities.

1.12   Algorithm R&D

During each development phase, the Contractor must perform Algorithm R&D as required to prepare for anticipated challenges that may impact upcoming development phases in order to de-risk effort for the upcoming demonstration cycle. At minimum, the Contractor must include Algorithm R&D activities to address the areas requiring further investigation identified in Section 7 of the ARMOUR TD project STS. Algorithm R&D activities include conducting technology reviews, options analysis, design and prototype development to resolve potential issues that could impact the development and delivery of the identified items. In addition, the Contractor may identify other items that the Contractor deems to be high-risk items of the following development phase and include these in the Algorithm R&D activities beyond the minimum identified in the STS.

1.13   Licensed Research Community Code Hosting and Maintenance

The ARMOUR TD project intends to license project results for the purposes of furthering development and advancing the state-of-the-art to allies, research institutions, academia and commercial vendors (the 'CND research community'). The Contractor must initiate and maintain a code repository on servers that are foreseen to offer free hosting services (e.g., a third party service), while maintaining access controls to those organizations that are granted a license by DRDC. The code repository must provide the CND research community with access to the Integration Framework (source and executable code), dependent processing modules (executable code or source and executable code, depending on third-party license terms) and test data or test simulators required to run the research version.

Where possible, the executable software solution should be made available as a virtual machine (VM) image for download and experimentation by the licensed CND research community. Dependent vendor software that is not part of the ARMOUR TD project development (e.g., COTS products integrated into the ARMOUR TD project solution) will be included as executable code only and contained in the VM image. This dependent executable code may have limited functionality compared to commercial versions, however, sufficient functionality must be available for the CND research community to conduct ongoing automated CND research and development. Subject to license terms, dependent Open Source Software (OSS) will be made available as source code through this code repository. It is intended that software (source and executable) will be released to the code repository following each operational demonstration of development phases 4 and 5.

The Contractor must launch the code repository, make arrangements for hosting of a project website, manage the availability of source and executable code, and track the process whereby the licensed CND research community may provide feedback, submit change requests or deliver code modifications. Changes to the licensed CND research community code are not expected to impact the ARMOUR TD project code stream directly.   Change requests and submitted code

changes received from the CND research community will be reviewed by DRDC and any changes that are deemed sufficient priority to include in the ARMOUR TD project will be addressed as appropriate through contractual channels of the TD including the Requirements Management Plan (PM 005) and Configuration Management Plan (PM 004) process established for the project. The Contractor must manage the process whereby the CND research community input is received, tracked and passed to DRDC for review. The Contractor management of the availability of source and executable code must include a source code repository able to adequately control, track and manage version control.

1.14   Close-Out

The Contractor must conduct TD Close-out activities with the intent of providing the TA with a thorough summary of the project history, achievements, and lessons learned. The Contractor must give a presentation of the Final Report. The presentation may be held as part of the Final Review Meeting.

APPENDIX B – DELIVERABLES

1.   ESTIMATED SCHEDULE FOR DELIVERY

The project work should be delivered in phases similar to the schedule provided below. The schedule for delivery stated in Table 1 for each phase is an estimate only. The vendor is expected to provide a detailed schedule for each phase as part of their Project Management Plan. The vendor must complete all work within 42 months. Contractors are encouraged to provide schedules that can accelerate demonstration delivery, however, accelerated schedules will only be accepted where it is demonstrated that the accelerated schedule will not result in undue risk to the project.

Table B-1: List of Project Phases and Estimated Schedule for Delivery

Project Phase	Estimated Schedule For Delivery
Phase 1: Analysis and Design	5 months from contract award
Phase 2: Integration Framework and Graphical User Interface (GUI)	6 months from Phase 2 approval to proceed
Phase 3: Proactive Observe and Orient	11 months from Phase 3 approval to proceed
Phase 4: Proactive Decide and Act	11 months from Phase 4 approval to proceed
Phase 5: Reactive Response	8 months from Phase 5 approval to proceed
Phase 6: Project Wrap-up (Closeout)	1 month from Phase 6 approval to proceed

The Contractor delivered schedule must include the following Milestones:

Table B-2: List of Project Milestones

Project Phase
Phase 1: Preliminary Design Review Meeting (Phase 1 complete, Phase 2 approval)
Phase 2: Critical Design Review Meeting
Phase 2: Readiness Review Meeting (Phase 2 complete, Phase 3 approval)
Phase 3: Critical Design Review Meeting
Phase 3: First Demonstration Completion
Phase 3: Readiness Review Meeting (Phase 3 complete, Phase 4 approval)
Phase 4: Critical Design Review Meeting
Phase 4: Second Demonstration Completion
Phase 4: Readiness Review Meeting (Phase 4 complete, Phase 5 approval)
Phase 5: Critical Design Review Meeting
Phase 5: Third Demonstration Completion
Phase 5: Readiness Review Meeting (Phase 5 complete, Phase 6 approval)
Phase 6: Final Review Meeting

2.   DELIVERABLES

The following table presents the contract deliverables for the ARMOUR TD project. Additional details are provided in Section 3 of Appendix B. All deliverables must be submitted in English.

Table B-3: Contract Deliverables Descriptions

CDRL[2]	DID[3]	Deliverables	Description
1	PM 001	Project Management Plan	The Project Management Plan is an evolutionary document describing how the Contractor will employ resources to meet the requirements.
2	PM 002	Progress Review and Project Meeting Reports, Agendas, and Minutes	The Progress Review Report must provide details regarding the progress of the project in preparation for the Progress Review meetings. For each project meeting, the Contractor must prepare and submit a meeting agenda. During the meeting, the Contractor must record the discussions, action items, and decisions in order to prepare the minutes accordingly and submit them to the TA.
3	PM 003	Readiness Assessment Report	The Readiness Assessment Report must provide details of the progress of the work in preparation for a Readiness Review meeting.
4	PM 004	Configuration Management Plan	The Configuration Management Plan describes how the Contractor must handle the code developed, the configuration items, the software versions and the life cycle of these elements during the entire project.
5	PM 005	Requirements Management Plan	The system Requirements Management Plan describes how the Contractor must track, change and manage the ARMOUR TD project requirements in relation to the work elements.
6	PM 006	Development Phase Plan	The Development Phase Plan describes the main objectives and milestones of the upcoming development phase.
7	PM 007	Final Report	The Final Report is intended to summarize the activities and achievements for the whole project.
8	PM 008	Transition Plan	The Transition Plan includes the Contractor's viewpoint on issues related to the transition of the ARMOUR TD project demonstrator to an operational system.
9	SD 001	System Requirements Specification Document	The System Requirements Specification Document (SRS) consists in a reviewed list and description of the ARMOUR TD project requirements. The SRS is an evolutionary document.
10	SD 002	Architectural Design Document	The Architectural Design Document explains how the design addresses the requirements. It is an evolutionary document.

---

[2] Contract Deliverable Requirements List (CDRL) number.

[3] Data Item Description corresponding to the CDRL.

APPENDIX B – Deliverables

CDRL[2]	DID[3]	Deliverables	Description
11	SD 003	Test Design Document and Test Environment	The Test Design Document includes the test environment characteristics, the scenarios, the test cases associated with the system requirements. The Test Design Document is an evolutionary document that will be used to plan demonstrations and acceptance test criteria. In addition to the Test Design, the Contractor must also demonstrate the existence of the Test Environment itself at the Contractor site.
12	SD 004	Detailed Design Document	The Detailed Design Document must explain how each sub-system, system, component, data structure, interface and algorithm are related and address identified requirements in the SRS document.
13	SD 005	Algorithm R&D Reports	The Algorithm R&D Reports describe the nature of the algorithm challenges, the objectives of the R&D effort, its activities and its results.
14	SD 006	Test Reports	The Test Reports capture the results of the execution of the test cases identified in the Test Design Document and Test Environment (SD 003).
15	SD 007	System Hardware, Software and Documentation	The System Hardware, Software and Documentation deliverable includes an image of the ARMOUR TD project software source and executable code with supporting software and hardware documentation. The final version (e.g., at the end of the contract) of this deliverable includes all software, hardware and documentation procured through purchase or leasing agreements and associated with the development of the ARMOUR TD project.
16	SD 008	Certification and Accreditation (C&A) Plan	The Certification and Accreditation (C&A) Plan includes all documentation needed supporting the achievement of an Interim Authority to Process (IAP) including System Description, Threat and Risk Assessment, Concept of Operations, design responses to TRA outcomes, IAP conditions of operation and other items as defined in the DND/CF Information System C&A Guidelines.
17	SD 009	System Concept of Operations	The System Concept of Operations documents the ARMOUR solution in relation to operational concepts related to automated CND. The concept of operations must be based on the OODA loop operational model (Observe, Orient, Decide, Act).
18	DM 001	Demonstration Plan	The Demonstration Plan describes the demonstration objectives, demonstration scenarios, demonstration environment, and the demonstration steps to be executed for each demonstration included in Phases 2-5.
19	DM 002	Demonstration Instance	The Contractor must provide the Demonstration Instance, including demonstration material, in support of formal system demonstrations and ad-hoc demonstrations given to stakeholders.
20	DM 003	Demonstration Report	The Demonstration Report captures the results of the execution of the operational demonstrations for each of Phase 3-5.

CDRL[2]	DID[3]	Deliverables	Description
21	DM 004	Code Repository	The Code Repository provides an online resource available to the CND Research Community where they can obtain current source and executable code for the version of the ARMOUR TD project results that are being made available under license for the purpose of furthering development and advancing the state of the art.

3. DELIVERABLE REQUIREMENTS

Electronic format:

All documents and reports produced as deliverables under this SOW and its Appendices must be delivered in electronic format on an appropriate, virus-free, properly labelled, support media such as CD-ROM. DRDC will provide templates which must be used when submitting any documentation to DRDC. Final documents and reports must also be provided in hard copy. The following format, and subsequent upgrades, must be used by the Contractor, unless otherwise agreed to by the TA: Searchable Adobe portable document format (PDF), Microsoft Word, Excel, PowerPoint, Visio, Project, or Access formats.

Design and Documentation standards:

Software requirements, architecture, design, testing and implementation documents produced as part of this contract must follow the ISO 35 (such as ISO/IEC 12207), IEEE (such as IEEE 829, 830), SEI-CMM or equivalent and applicable documentation and process standards. The Contractor must also take into consideration the Common Criteria (also known as ISO 15408) security standards in the design activities and relevant documents. In addition the project will provide the appropriate outputs of the C&A process to guide design efforts, e.g. Threat Risk Assessment (TRA) recommendations.

Approval:

The TA must approve all deliverables. Providing that the TA is satisfied that approval should be granted for a given deliverable, such approval must be granted without unreasonable delay.

Table B-4: Contract Deliverable Requirements List (CDRL)

CDRL	DID	Deliverables
1	PM 001	Project Management Plan
2	PM 002	Progress Review and Project Meeting Reports, Agendas, and Minutes
3	PM 003	Readiness Assessment Report
4	PM 004	Configuration Management Plan
5	PM 005	Requirements Management Plan
6	PM 006	Development Phase Plan
7	PM 007	Final Report
8	PM 008	Transition Plan
9	SD 001	System Requirements Specification Document
10	SD 002	Architectural Design Document
11	SD 003	Test Design Document and Test Environment
12	SD 004	Detailed Design Document
13	SD 005	Algorithm R&D Reports
14	SD 006	Test Reports
15	SD 007	System Hardware, Software and Documentation
16	SD 008	Certification and Accreditation Plan

APPENDIX B – Deliverables

17	SD 009	System Concept of Operations
18	DM 001	Demonstration Plan
19	DM 002	Demonstration Instance
20	DM 003	Demonstration Report
21	DM 004	Code Repository

3.1 PM 001: Project Management Plan:

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Project Management Plan	PM 001
2. Description/Purpose The Project Management Plan is an evolutionary document describing how the Contractor will employ resources to meet the requirements.	4. Delivery Date Project baseline version: 20 working days after contract award Iteration: An updated version will be provided at the beginning of each phase and each development cycle.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References
10. Preparation Instructions The Contractor must prepare a Project Management Plan following IT project management best practices. The Project Management Plan will include, as a minimum, the following: - WBS, including tasks and sub-tasks relevant to each deliverable; - Schedule with sequencing information; - List of deliverables and milestones, including the target dates; - Resource plan: including the names and responsibilities of each team member and subcontractors as well as the reporting structure; - System development life cycle approach; - System and software development processes: including relationship between Requirements Refinement, Design, Build, Test, Problem Reporting and Corrective Action; - System and software development standards, practices and methodologies; - System and software development environment and tools; - Quality Assurance Plan; - Risk analysis and mitigation plan; - Communications plan; and - Relationship to other plans/documents. The Project Management Plan baseline version consists of a high-level plan for the entire project and the detailed plan for Phase 1. Subsequent iterations of the Project Management Plan will provide details for the following phase or development cycle, as well as a revised high-level plan for the remainder of the project. The Contractor must include the six development phases in its Project Management Plan. With the exception of Phase 1 and 6, the components of each phase must, at minimum, include the follows: • Requirements Refinement, Design, Build, Test, Problem Reporting and Corrective Action (contractor premises); • Review resulting system design for C&A requirements in accordance with the C&A Plan (SD 008); • Build the ARMOUR TD project solution; • Conduct demonstrations as a venue for evaluation by DRDC; and • Carry out planning and design for the next phase based on the Algorithm R&D, test and demonstration results.	

3.2 PM 002: Progress Review and Project Meeting Reports, Agendas, and Minutes

DATA ITEM DESCRIPTION	3. Identification No.
• Title Progress Review and Project Meeting Reports, Agendas, and Minutes	PM 002
• Description/Purpose The Progress Review Report must provide details of the progress of the contract in preparation for any scheduled project meeting. The Project Meeting Report captures the details of any project meeting. Each Project Meeting Report must include: • The Agenda must list meeting date, location, topics and schedule; • The Minutes must include attendees, a summary of the discussions, list of action items, and record of decisions.	4. Delivery Date Progress Reviews Report: 5 working days before each Progress Review Meeting. Draft agenda: 5 working days before each meeting Final agenda: 2 working days before each meeting Draft minutes: 2 working days after each meeting Final minutes: 5 working days after each meeting
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 2 working days after receipt
	9. References
10. Preparation Instructions The Progress Review Report may be prepared in the Contractor's format and must contain, as a minimum, the following information: • The status of action items resulting from the previous Progress Review Meeting or Milestone Review Meeting; • A brief summary of the major activities over the past period; • An updated project schedule indicating the current project status in relation to the Project Management Plan schedule; • A brief description of the problems encountered and the proposed remedial action. Information must include the impact of the problem on overall project schedule and cost; • Expected project achievements over the next report period; • Current post-mortems and lessons learned; • Phase containment related issues; • Financial status of the contract; and • Proposed amendments to any previous documents. The information contained in the Progress Review Report must be in sufficient detail for the TA to review and discuss its content at the scheduled meeting. The intent of this requirement is to permit the TA to familiarize herself/himself with the progress and project problems prior to the scheduled meeting so that the meeting time is spent in meaningful discussions leading to resolution of the problem areas. The content of each project meeting agenda will be discussed between the TA and the Contractor PM after Contract award and as required during the project.	

APPENDIX B – Deliverables

The minutes for each meeting must include, at a minimum, the following:

- List of attendees;
- Meeting agenda, date, location;
- Action items list, identification number, details, status, OPI and schedule.
- Discussion summary and contributors for each agenda item.
- Time and location for the next meeting

The Contractor may use its own agenda and minute format for these deliverables. The agendas and minutes are subject to approval by the TA. The Contractor is responsible for amendments to the agendas and minutes as may be required.

3.3 PM 003: Readiness Assessment Report

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Readiness Assessment Report	PM 003

2. Description/Purpose The Readiness Assessment Report must provide details of the progress made towards preparation for the next contract phase and must be provided in advance of the Readiness Review Meeting.	4. Delivery Date Report: 5 working days before each Readiness Review Meeting.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 2 working days after receipt
	9. References

10. Preparation Instructions

The Readiness Review Report may be prepared in the Contractor's format and must contain, as a minimum, the following information:

- The results of the current phase development activities, including the results of any testing or demonstration feedback received;
- The results of the Operational Concept Review and Requirements Refinement activities from the current phase demonstrations;
- The results of the Algorithm R&D activities performed in preparation for the upcoming phase;
- Lessons learnt from the current phase;
- Any other preparation notes for the upcoming phase which were compiled during the current phase;
- Proposed amendments to any previous documents; and
- Contractor recommendations as to their readiness to begin the upcoming phase.

The information contained in the Readiness Assessment Report must be in sufficient detail for the TA to review and discuss its content at the Readiness Review Meeting. The intent of this requirement is to permit the TA to familiarize herself/himself with the progress and project problems prior to the Readiness Assessment Meeting. The TA may assess the readiness for the project to be approved in advance to the upcoming phase or make recommendation for project off ramp (contract termination).

3.4   PM 004: Configuration Management Plan

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Configuration Management Plan	PM 004
2. Description/Purpose The Contractor must prepare a Configuration Management Plan which describes how the code developed, the configuration items, the software versions and the life-cycle of these elements will be handled during the project.	4. Delivery Date Project baseline version: 20 working days after contract award Iterations: as required.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References: IEEE 828, IEEE 1042
10. Preparation Instructions The Contractor must prepare a Configuration Management Plan tailored to ARMOUR TD project needs, which, at a minimum, should address the following issues: - Software release management process; - Software change management process; - Code acceptability criteria; - Software modules and versions testing methodology; - Code and version maintenance process; - Code and version retirement process. The Contractor must identify the tools used for this purpose, if applicable. The Contractor may use its internal configuration management documentation format for this deliverable.	

3.5 PM 005: Requirements Management Plan

DATA ITEM DESCRIPTION	2. Identification No.
1. Title Requirements Management Plan	PM 005
2. Description/Purpose The Requirements Management Plan describes how the Contractor must track, change and manage the ARMOUR TD project requirements in relation to the work elements.	4. Delivery Date Draft: 20 working days after contract award Final: 40 working days after contract award Iteration: as required for each phase.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References: ISO/IEC 12207, SEI-CMM.

10. Preparation Instructions
The Contractor must prepare and maintain a Requirements Management Plan which, as a minimum, consists of the following:
 	
    - Requirements book;
    - Requirements traceability matrix;
    - Requirements modification process; and
    - Design items / software functionality list linked to the requirements matrix.
 	
The Contractor may use its internal requirement management documentation format for this deliverable.	

3.6 PM 006: Development Phase Plan

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Development Phase Plan	PM 006

2. Description/Purpose	4. Delivery Date
This plan will cover the main objectives and milestones of the upcoming development phase. The purpose is to formally approve the upcoming development work included in the next phase.	Draft: A minimum of 10 working days before the scheduled start of the upcoming phase. Final: At the start of the new development phase. Iterations: for each phase.

	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)

7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References

10. Preparation Instructions

The Development Phase Plan is composed of updated project management documents and technical documents. The Development phase plan must include, as a minimum, the following:

- Detailed WBS and schedule for the subject development Phase;
- Development Phase objectives;
- System increments from previous development phase, or from off-the-shelf capabilities (for the first development phase) including a summary of issues from previous development phases test and demonstration reports;
- Updated architectural design;
- Updated Detailed design including subject development phase components to be added/refined, as identified in the objective; and
- Updated Test design Document.

3.7   PM 007: Final Report

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Final Report	PM 007
2. Description/Purpose The Contractor must prepare a Final Report at the end of the project. This report is intended to summarize the activities and achievements for the whole project.	4. Delivery Date Draft: No later than 20 working days after the start of Phase 6 Final: At the end of Phase 6
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References
10. Preparation Instructions The Final Report must include the final version of every project document. It must, at minimum, discuss the following subjects: • Summary of all the development phases objectives, activities, and results (including feed-back from operational community); • Lessons learned; and • Areas identified for further research. The Final Report will be formatted using the DRDC Standard template as provided by the TA.	

3.8   PM 008: Transition Plan

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Transition Plan	PM 008

2. Description/Purpose	4. Delivery Date
The Contractor must prepare a Transition Plan for the ARMOUR TD project. This plan will include the Contractor's viewpoint on issues related to the transition of the ARMOUR TD project demonstrator to an operational system.	Draft: No later than 20 working days after the start of Phase 6 Final: At the end of Phase 6

	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References: ISO/IEC 12207

10. Preparation Instructions

The Transition Plan must include a summary of the various meetings and discussions held during the course of the project which were related to the ARMOUR TD project operational deployment. The Transition Plan will address, as a minimum, the following subjects:

- Concept of Operations;
- Deployed system requirement specifications, including security and performance requirements;
- System testing considerations;
- Life-cycle support plan and requirements, including cost estimates;
- Deployment plan, including cost and duration estimates;
- Challenges; and
- Proposed solutions and work-around.

3.9 SD 001: System Requirements Specification Document

DATA ITEM DESCRIPTION	3. Identification No.
1. Title System Requirements Specification Document	SD 001
2. Description/Purpose The System Requirements Specification Document (SRS) consists in a description of the ARMOUR TD project requirements. The SRS will be reviewed and updated for each development phase.	4. Delivery Date First version: No later than 40 working days after start of Phase 1. Final: With final report. Iterations: As part of each phase plan.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References: IEEE 830

10. Preparation Instructions

The Contractor must produce a System Requirements Specification Document (SRS) and update its content as required during the project. The technical documentation provided as part of the RFP package is intended to ensure the Contractor understands the ARMOUR TD project concept. The SRS, must include the technical documentation referenced in the contract as input and further detail the initially stated requirements. The SRS must include detailed security requirements for the ARMOUR TD project. The detailed requirements must be written in a format to support testability:

- Consistent;
- Complete;
- Unambiguous;
- Quantitative; and
- Verifiable in practice.

3.10 SD 002: Architectural Design Document

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Architectural Design Document	SD 002
2. Description/Purpose The Architectural Design Document explains the ARMOUR TD project components and sub-systems and how they address the requirements. It is an evolutionary document.	4. Delivery Date Initial version: 20 working days after the contract award Iterations: 10 working days before each Readiness Review Meeting (as required during the development cycles)
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References: ISO 12207, ISO 35

10. Preparation Instructions

The Architectural Design Document , at a minimum, must include:

- The system high-level architecture;
- The system sub-systems and documented relationships with the main system;
- The information models (in the form of UML models);
- COTS and Open Source software name, versions and general configuration information, as applicable*;
- Interfaces general description;
- Security architecture.

Each of the architectural design sub-systems must be linked to the appropriate system requirements provided. Each version of this document must include comments pertaining to the changes introduced from previous versions and their supporting rationale.

*The Contractor must justify the use of custom, COTS and Open Source software developed/selected to be part of the ARMOUR TD project. The Contractor will make use of quality attributes to assess the selected COTS / Open Source. This software assessment will be part of the Architectural Design Document. The quality attributes used to assess the software should, at a minimum, include the following:

1. API characteristics;
2. Compliance with recognized standards;
3. Support availability;
4. Functionality;
5. Licensing cost;
6. Integration ease;
7. Scalability;
8. Security features;
9. Trusted source;
10. Ubiquity;
11. Extensibility;
12. Source (organisation/company) characteristics (size, stability); and
13. IP related issues and restriction for the use of the product.

The Contractor must use a similar set of quality attributes to evaluate any product identified by the technology watch activity or by the TA.

3.11 SD 003: Test Design Document and Test Environment

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Test Design Document and Test Environment	SD 003
2. Description/Purpose The Test Design Document includes the test environment characteristics, the scenarios, the test cases associated with the system requirements. The Test Design Document is an evolutionary document that will be used to plan demonstrations and acceptance test criteria. In addition to the Test Design, the Contractor must also demonstrate the existence of the Test Environment itself at the Contractor site.	4. Delivery Date Initial version: No later than 40 working days after contract award. Iterations: As required during the development cycles.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References: IEEE 829

10. Preparation Instructions

The Test Design Document includes a description of the modeled environment, the actual test environment configuration to be used, requirements for creation of test data, the generic scenarios to be used as baselines, and the relevant test cases. It is expected that the scenarios will remain the same during the project. Test cases should be added as functionalities of the system are detailed and developed.

The Test Design Document must include test cases, scenarios and test environment configurations applicable to:

- Unit tests;
- Integration tests;
- System tests; and
- Interface tests.

The Test Environment must be representative of the DND IT infrastructure environment as much as possible. The constraints and requirements pertinent to this environment are described in the System Requirements Specification document and will be refined during Phase 1. For each test environment configuration, the testing tools must be identified.

The testing approach (white box, grey box, black box, etc.) and test method (Observation, Analysis, Execution, etc) must be described and explained.

Attention must be paid to regression testing in the following contexts:

- integrated software from previous project phases that may have been modified during the course of the current phase development activities;
- integrated software from the current project phase that may have been modified as a result of debugging activities during the current phase testing activities; and
- integrated software (COTS/Open Source/developed software) version changes during the course of the project Unit tests.

APPENDIX B – Deliverables

The scenarios will be developed by the Contractor, subject to the approval of the TA. The scenarios are intended to reflect common operational situations, while making optimal use of the system features in support of Computer Network Defence. Scenarios may include:

- Title;

- Objective;

- Background;

- Scope (national, regional, deployed, international);

- Configuration and preconditions (types of inputs, environment set-up);

- Size (environment descriptive data);

- Roles and tasks; and

- Sequence of activities.

Failure scenarios must also be considered as part of the Test Design Document.

3.12 SD 004: Detailed Design Document

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Detailed Design Document	SD 004
2. Description/Purpose The Detailed Design Document must explain how each sub-system, system, component, data structure, interface and algorithm are related and address identified requirements in the system requirements specification document.	4. Delivery Date Draft: Not less than 10 working days before the end of Phase 1 Final: No later than 20 working days after start of Phase 6 (as part of the Final Report deliverable) Iterations: As part of every development phase plan.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References: ISO 12207, ISO 35

10. Preparation Instructions
 This document must, at minimum, include the following:
 	
      - Interfaces (API, GUI, communications, files) detailed description and design;
      - Data model detailed design (in the form of UML models);
      - Algorithm detailed design;
      - Sub-systems and components detailed design;
      - Software and hardware detailed configuration.	

3.13 SD 005: Algorithm R&D Reports

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Algorithm R&D Reports	SD 005
2. Description/Purpose The Algorithm R&D Reports describe the nature of the algorithm challenges and their relationship to the requirements, the objectives of the algorithm R&D effort, its activities and its results.	4. Delivery Date Draft: No later than 10 working days before each Readiness Review Meeting. Final: No later than 10 working days after each Readiness Review Meeting.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation Draft: 5 working days after receipt. Final: 10 working days after receipt.
	9. References IEEE 829

10. Preparation Instructions

The report must, at minimum, include the following:

- Description of R&D Challenge

- Research Objectives;

- Hypothesis;

- Approach;

- Set-up and facilities;

- Metrics;

- Needs (access to data sources, clearance, etc);

- Research results;

- Research conclusions; and

- Minutes of discussions (when applicable)

3.14   SD 006: Test Reports

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Test Reports	SD 006
2. Description/Purpose The Test Reports capture the results of the execution of the test cases identified in the Test Design Document and Test Environment (SD 003).	4. Delivery Date Draft: No less than 10 working days before each Readiness Review Meeting. Final: No later than 10 working days after each Readiness Review Meeting.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation Draft: 5 working days after receipt Final: 10 working days after receipt
	9. References: IEEE 829

10. Preparation Instructions
The Test Reports must be prepared in reference to the Test Design Document and Test Environment and as a minimum, include the following: - Identification (name) of tester;   - Test Cases executed;   - Test Cases not executed with explanation concerning reasons for non-execution;   - Test Case results;   - Debug or failure resolution activities conducted for any failed tests;   - Test Case Re-execution results following debug; and   - Test/Developer notes regarding the test case results.   *Note: It is required that tests will be conducted within each development phase in preparation for any Operational Demonstrations.

3.15 SD 007: System Hardware, Software and Documentation

DATA ITEM DESCRIPTION	3. Identification No.
1. Title System Hardware, Software and Documentation	SD 0007
2. Description/Purpose As a result of each development phases, the Contractor must deliver an instance of the ARMOUR TD project source and executable code with supporting hardware, software and documents to the TA. At the end of the contract, the Contractor must deliver all software, hardware and documentation procured with ARMOUR TD project development funds.	4. Delivery Date Initial version: At the end of the first development phase. Final version: At the end of the last development phase. Iterations: At the end of each development phase.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References

10. Preparation Instructions

The Contractor must provide the TA with the current instance of the ARMOUR TD project solution (source and executable code) which will reside in the DRDC Cyber Operations Section laboratory, on the Cyber Operations Section network. The intent is to allow DRDC scientists to become familiar with the ARMOUR TD project as well as to conduct parallel research activities. The Contractor must deliver all required hardware and software, in a ready-to-use format, which is required to use/demonstrate the system's functionalities. Basic user documentation must also be delivered.

-Hardware: Depending upon the solution, this may include one client PC, system application servers and database servers, basic networking equipment such as routers, wiring, hubs, network cards, network sensors such as Intrusion Detection System (IDS, etc.).

-Software: Depending upon the solution, this may include client application software, server application software, database application software, supporting OS, agent software, COTS/Open Source software etc. The software must be packaged in a ready-to-install format, on appropriate media such as CD-ROMs. Preference must be given to packaging the solution as a ready-to-install virtual machine (VM) image where possible. The Contractor must also ensure that all equipment provided for this deliverable will have appropriate licenses for all software products installed, and include anti-virus for any windows based software with current updates.

- Documentation: The documentation must include installation and configuration instructions for all software packages and hardware items. A basic user manual covering system user interface and features must also be provided. All original documentation for COTS and Open Source software will be provided as well. The source code for developed software must also be provided.

Data Modeling documentation must be provided in the form of UML models.

All software owned by the Contractor must be documented to permit its usage and integration by government employees and other contractors in the context of the ARMOUR TD project and follow on research activities.

The Contractor must provide increments to the initial system. It is expected that most hardware initially delivered will remain the same for most development phases, and hence, will not have to be delivered again as new ARMOUR TD project versions are developed. At the project closure, the Contractor must deliver all hardware, software and documents procured for the ARMOUR TD project, including test equipment and other peripheral components.

3.16   SD 008: Certification and Accreditation Plan

DATA ITEM DESCRIPTION	3. Identification No.
1. Title Certification and Accreditation (C&A) Plan	SD 008
2. Description/Purpose As part of the development phases, the Contractor must deliver a C&A Plan and supporting documentation necessary to achieve Interim Authority to Process (IAP) for operational deployment. The scope and purpose is to allow the project to achieve IAP and, in the future, complete C&A .	4. Delivery Date First version: No later than 40 working days after start of Phase 1. Final: With final report. Iterations: As part of each phase plan.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References Department of National Defence/Canadian Forces (CF), Information System Certification and Accreditation Guideline, Version 1.4, December 2006 CSEC/RCMP Harmonized Threat and Risk Assessment Methodology
10. Preparation Instructions The C&A Plan is composed of C&A documents. The C&A Plan must include, as a minimum, the following: - Summary of C&A decisions that affect the Architectural and detailed designs; - Updated Concept of Operations; - System Description/topology; - Threat and Risk Assessment (TRA) in accordance with the CSEC/RCMP Harmonized Threat and Risk Assessment (HTRA); - Documented design responses to ARMOUR TRA; - Stated conditions necessary to reduce TRA risks; and - Other items as needed to meet the DND/CF Information System Certification and Accreditation Guidelines.	

3.17   SD 009: System Concept of Operations

DATA ITEM DESCRIPTION	3. Identification No.
• Title System Concept of Operations	SD 009
• Description/Purpose As part of each development phase, the Contractor must refine and deliver an updated System Concept of Operations document. The System Concept of Operations is a description of how the system will be used by the operational community. It is non-technical, and presented from the viewpoints of the various stakeholders. The System Concept of Operations documents the ARMOUR solution in relation to operational concepts related to automated CND. The System Concept of Operations must be based on the OODA loop operational model (Observe, Orient, Decide, Act).	4. Delivery Date Project baseline version: 20 working days after contract award Iteration: An updated version is required at the beginning of each phase and each development cycle.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 5 working days after receipt
	9. References

10. Preparation Instructions

The Contractor must produce a System Concept of Operations document and update its content as required during the project. The concept of operations description provided as part of the System Requirements Specification included in the RFP package is intended to ensure the Contractor understands the ARMOUR TD project concept. For the System Concept of Operations deliverable, the Contractor must make use of the documentation referenced in the contract as a starting point and further detail the initially stated concepts. The System Concept of Operations is intended to:

- Get stakeholder agreement identifying how the system will be operated;
- Define the high-level system concept;
- Define the environment in which the system will operate;
- Derive detailed requirements, especially user requirements; and
- Provide the criteria to be used for validation of the completed system.

The System Concept of Operations must incorporate input from the stakeholder community including but not limited to the Director General Cyber (DG Cyber), Cyber Task Force (Cyber TF), Canadian Forces Information Operations Group (CFIOG), Canadian Forces Network Operations Centre (CFNOC), Director Information Management Engineering and Integration (DIMEI), Director Information Management Security (D IM Secur), Director Enterprise Architecture (DEA), Director Information Management Technologies, Products and Services (DIMTPS), Defence Research and Development Knowledge Information Management (DRDKIM) and the Network Command and Control Integrated Situation Awareness Capability (NetC2 ISAC) project.

The System Concept of Operations must, at minimum, include the following information:

- Identified capability deficiencies;
- Operational environment;
- Operational scenarios;
- User oriented operational description;
- System relationship to capability deficiencies; and
- System support and maintenance.

3.18   DM 001: Demonstration Plan

DATA ITEM DESCRIPTION	3. Identification No.
• Title Demonstration Plan	DM 001
• Description/Purpose The Demonstration Plan describes the demonstration objectives, demonstration scenarios, demonstration environment, and the demonstration steps to be executed for each demonstration included in Phases 2-5.	4. Delivery Date Initial version: Not less than 10 working days before the end of Phase 1. Iterations: As required during the subsequent development phases.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 10 working days after receipt
	9. References

10. Preparation Instructions

The Demonstration Plan Document includes a description of the demonstration objectives, demonstration scenarios, demonstration environment, and the demonstration steps to be executed for each demonstration planned in phases 2 to 5. For the Phase 2 demonstration, the demonstration will take place in the Cyber Operations Section Lab Environment. For the remaining demonstrations, the demonstration will use an Ottawa based subnet or subnets of the DREnet to demonstrate the system. The description of the demonstration environment will identify any requirements to augment the DREnet operational environment to fully demonstrate the capabilities to be demonstrated in each phase (e.g., test systems and test data).

The Demonstration Plan must include demonstration scenarios and demonstration steps to be executed during the demonstration.

The scenarios will be developed by the Contractor, subject to the approval of the TA. The scenarios are intended to reflect common operational situations, while making optimal use of the system features in support of Computer Network Defence. Scenarios may include:

- Title;
- Objective;
- Background;
- Scope (national, regional, deployed, international);
- Configuration and preconditions (types of inputs, environment set-up);
- Size (environment descriptive data);
- Roles and tasks; and
- Sequence of activities.

3.19 DM 002: Demonstration Instance

DATA ITEM DESCRIPTION	3. Identification No.
• Title Demonstration Instance	DM 002
• Description/Purpose The Contractor must provide a Demonstration Instance and demonstration material in support of the ARMOUR TD project demonstration activities. These demonstration activities consist of formal system demonstrations, typically occurring at DRDC at the end of each development phase, and may include ad-hoc demonstrations given to stakeholders at different locations.	4. Delivery Date Formal Demonstration Instance: 10 working days before scheduled demonstration date. Ad-hoc demonstrations material: At the end of phase 1 and at the end of each development phase. Iterations:
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 4 working days after receipt
	9. References

10. Preparation Instructions

The formal Demonstration Instance and demonstration material consists of the ARMOUR TD project instance delivered as part of the system Hardware (HW), Software (SW) and documentation deliverable, and the required HW and SW required for the system demonstration defined in the Demonstration Plan deliverable (DM 001) in order to successfully demonstrate the system in the target operational environment (DREnet). Depending on the solution proposed, the trial HW and SW might include traffic generating equipment, data sets, and test scripts to support full system functionality demonstration.

The ad-hoc demonstration material consists of a standalone laptop-based system demonstration of ARMOUR capabilities. This demonstration material will be in sufficient detail to allow for an accurate demonstration of the ARMOUR TD project features developed to date. Depending on the proposed ARMOUR TD project solution, a standalone version may be prohibitive to produce. Therefore, other demonstration support material formats, such as flash video, secure remote access to the Contractor's system and GUI mock-ups will be acceptable.

3.20   DM 003: Demonstration Report

DATA ITEM DESCRIPTION	3. Identification No.
• Title Demonstration Report	DM 003
• Description/Purpose The Contractor must provide a Demonstration Report following each of the ARMOUR TD project demonstration activities. The Demonstration Report must summarize the outcomes of the demonstration including stakeholder feedback and intended Contractor response.	4. Delivery Date 10 working days following each demonstration.
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 5 working days after receipt
	9. References

10. Preparation Instructions

The Demonstration Report is prepared following each of the ARMOUR TD project demonstration activities and services as a means to capture the feedback from the various stakeholders observing the demonstrations and provide Contractor recommendations for response to the feedback. The Demonstration Report must, at minimum, include the following information:

- Executive summary of stakeholder feedback and Contractor recommendations;

- High level description of the demonstration environment and goals;

- List of stakeholders involved capturing their interest in the TD;

- Summary feedback from each stakeholder;

- Detailed table of capabilities demonstrated and stakeholder feedback received; and

- Contractor recommended response to stakeholder feedback.

3.21   DM 004: Code Repository

DATA ITEM DESCRIPTION	3. Identification No.
• Title Code Repository	DM 004
• Description/Purpose The Code Repository provides an online resource available to the CND Research Community where they can obtain current source and executable code for the version of the ARMOUR TD project results that are being made available under license for the purpose of furthering development and advancing the state of the art.	4. Delivery Date 10 working days following the end of development phase 4 and 5
	5. Office of Primary Interest (OPI) Contractor
	6. Office of Collateral Interest (OCI)
7. Application/interrelationship	8. DND Approval Limitation 5 working days after receipt
	9. References

10. Preparation Instructions

The Contractor must initiate and maintain a Code Repository on servers which are foreseen to offer free hosting services (e.g., a third party service), while maintaining access controls to those organizations that are granted a License by DRDC. The Code Repository must provide the CND research community with access to the Integration Framework (source and executable code), dependent processing modules (executable code or source and executable code, depending on third-party license terms) and test data or test simulators required to run the research version.

Where possible, the executable software solution should be made available as a virtual machine (VM) image for download and experimentation by the licensed CND research community. Dependent vendor software that is not part of the ARMOUR TD project development (e.g., COTS products integrated into the ARMOUR TD project solution) will be included as executable code only and contained in the VM image. Subject to license terms, dependent Open Source Software (OSS) will be made available as source code through this code repository. It is intended that software (source and executable) will be released to the code repository following each operational demonstration of development phase 4 and 5.

The Contractor must set up the Code Repository, make arrangements for hosting of a project website, manage the availability of source and executable code, and tracking the process whereby the licensed CND research community may provide feedback, submit change requests or deliver code modifications. The Contractor must manage the process whereby the CND research community input is received, tracked and passed to DRDC for review. The Contractor management of the availability of source and executable code must include a source code repository able to adequately control, track and manage version control.

APPENDIX C – OPTIONAL SERVICES REQUIREMENT

1.   INTRODUCTION

Depending on the maturity of technology delivered within each phase of the ARMOUR TD project Basic Requirement SOW, The Optional Services Requirement may be exercised concurrently on an "as and when requested" basis, via a 626 Task Authorization. The Optional Services Requirement which may be performed is the provision of software and supporting professional services to DND to further develop, deploy, support, and maintain ARMOUR TD related components and associated professional services required to integrate the ARMOUR TD project results as an Initial Operating Capability (IOC) within the CF. The following non-exhaustive list are examples of the types of tasks that may be issued:

- Conduct Personnel, Operations and Maintenance (PO&M) impact studies and planning in order to assess the overall PO&M needs of an operational deployment of an ARMOUR-like capability and develop a transition plan to meet these needs.

- Conduct analysis of completed ARMOUR demonstrations in order to identify operational gaps and, if necessary, improve the ARMOUR components through a design, develop, test and demonstrate life-cycle.

- Assess the current scale, scope and number of DND networks including relevant constraints, protocols, services, applications, infrastructures, and policies relative to ARMOUR functional capabilities;

- Support the transition of ARMOUR capability or components onto DND networks;

- Transformation services to support the integration of ARMOUR within the DND community through procedures, process and training;

- Project Management services to schedule, guide, manage, budget and provide oversight and support to assigned tasks;

- Conduct such operations and maintenance activities to support a project source code repository and web site for access by licensed organizations within the CND research community including allies, research institutions, academia and commercial companies;

- Maintain a process for code receipt and review;

- Analyze and develop strategies and recommendations for continued operation and maintenance of the project repository after completion of the exercised options;

- Conduct technology analysis activities in support of DRDC initiatives stemming from the ARMOUR TD project Basic Requirement outcomes or ARMOUR TD related CND research community input;

- Develop operator policies, practices and procedures to ensure cyber defence operations can maximally benefit from ARMOUR functional capabilities;

- Assess technology integration strategies that contribute to the development of the ARMOUR Integration Framework and component functional capabilities;

- Review and develop operational requirements, integration specifications, system requirements, and design and test documents;

- Improve the ARMOUR software components through a software design, develop, test and demonstrate life-cycle;

- Conduct technical and operator training as required to establish a cadre of technical and operator staff qualified to operate the ARMOUR capability on an ongoing basis; and

- Communicate the nature of the ARMOUR TD project results across the CND research community and promote the use and adoption of the Integration Framework and software components through conferences, workshops, the ARMOUR website and presentations to the CND research community (including allies, research institutions, academia and commercial entities).

APPENDIX C – Optional Services Requirement

Task Authorization

Task Authorization will follow the process as described in the ARMOUR TD RFP bid package and resulting contract using the DND 626 Form. The DND 626 Task Authorization form will include an appended Task Description detailing the specific Optional Services Requirement tasks to be conducted.

Duration:

The Optional Services Requirement may be exercised any time after contract award of the Basic Requirement and includes up to three option periods of two years each. The duration of tasks requested under a given DND 626 Task Authorization will be specified in the DND 626 Form.

CONSTRAINTS

In as much as the ARMOUR TD project Basic Requirement work is expected to contribute to the evolution of an automated CND capability for the CF, there are a number of conditions that may be experienced during the TD phase that may impact the Optional Services Requirement:

- Due to changing technology and operational concepts, the traditional schedule of Concept, Preparation and Design, Implementation and finally Exploitation will be impacted by evolving requirements:

  - The ARMOUR TD will integrate COTS products that are undergoing their own development cycle.

  - The cyber domain concept of operations within the CF is undergoing its own evolution.

- Based on the above, the ARMOUR TD implementation cycle requires the project to merge with other schedules and "demonstrate along the way" using a "cyclical" development approach instead of sequential approach to systems development and integration such as: requirements, development, integration, test and deploy.

- The management component for such an approach is more demanding but the benefit to such a project is that the exploitation phase is built in from the beginning of the project and it is conceivable that operations benefits could begin to be received by CF in early cycles, before the end of the project.

- Network Command and Control Integrated Situation Awareness Capability (Net C2 ISAC) – This capital project may procure and deploy network sensor and analysis capabilities useful to the capabilities demonstrated by the ARMOUR TD project and may be an integration point for exploitation outcomes that may be the focus of the Optional Services Requirement.

- The ARMOUR TD project delivery approach will be the result of consultation with the operational sponsor and operators.

- Software development and testing practices conducted during the Basic Requirement should include product hardening (e.g., removal of unnecessary services, changing default passwords, resolution of issues identified during penetration testing) and result in production release ready code that is near, or at, commercial product levels, in order to minimize additional R&D efforts that may be tasks under the Optional Services Requirement. However, some additional software development and testing is expected to be tasked as under the Optional Services Requirement to enhance the demonstration version capabilities and deliver a production ready version sufficiently robust to be used in an operational environment.

- An integrated project team (IPT) approach will be used to assist in the Basic Requirement portion and across the option period. The team will be comprised of DRDC scientists, representatives of the operational client community and Defence contractors, depending upon the nature of the task.

1.1   Resources

To fulfill the objectives of this Requirement, the Contractor must provide a number of resources to execute the work on an "as-and-when-requested" basis. The following table describes the roles and responsibilities that each resource type may be required to perform.

Table C-1: Resource Responsibilities for Optional Services Requirement

RESOURCE	RESPONSIBILITIES
Project Management	
Project Manager	Perform overall project planning, execution and supervision;
	Provide a project plan and propose breakdown structure for delivery and provide work plan and budget;
	Perform all project management and leadership activities (e.g., planning, assigning resources, assign due dates, enforce project schedule and milestones, maintain the team on track);
	Keep track of all the project activities, progress, budget and deliverables;
	Identify, assess and continually manage risk, issues and change;
	Report regularly to the TA on the evolution of the work, the issues that arise and solutions to be applied in order to meet the requirements within the budget and schedule constraints.
Project Communications Specialist	Prepare and execute project communication plans targeted internally to the project team and externally to the military sponsor, military client and to the CND research community;
	Advise the TA on communication issues, approaches and strategies to implement communication means appropriate to each community of interest (client, sponsor, project team and scientists);
	Edit and publish a periodic electronic and hard copy ARMOUR TD newsletters;
	Develop brochures, posters and other advertisement media;
	Deliver training to operators and trainers.
Project Control Officer	Assist the Project Manager in carrying out PM responsibilities to control the project implementation activities;
	Establish and manage a project control reporting framework;
	Implement performance monitoring processes and procedures;
	Collect, analyze and publish performance monitoring indicators;
	Enforce execution of approved project plans.

RESOURCE	RESPONSIBILITIES
Webmaster	Perform all ARMOUR related Web Management activities (e.g., create new Web site pages, populate the Web site utilizing templates, standard graphics, develop new forms, graphics and documents);
	Manage the content of and access to all related documents according to the approved ARMOUR communication plans;
	Support operators and site problems;
	Support ARMOUR development, test, experimentation and demonstration activities on request.
System Architecture and Design	
Lead System Architect	Provide leadership and oversight for ARMOUR architecture, standards, models and technical choices;
	Provide technical leadership for the overall architecture of the solution and its integration within operational environment;
	Provide technical leadership in analysis and resolution of technology challenges identified as part of the concepts, design or implementation activities, or that may arise during the development of the system;
	Seek TA approval for any selected technical solution prior to any implementation. A cost-effectiveness analysis as well as integration requirements to operational environment study must be applied to justify any choice;
	Communicate all architectural and technical choices to the TA.
Software Solution Architect	Maintain a functional architecture for ARMOUR project;
	Provide an oversight for DND CND operational processes;
	Provide advice to the TA to ensure that the business requirements are met by the selected solution;
	Based on research and analysis of technology challenges, provide advice to the TA on the resolution of technology challenges identified as part of the concepts, design or implementation activities, or that may arise during the development of the system.
System/Network Analyst	Analyze the targeted system and network infrastructure and publish design guidelines and recommendations to guide design and implementation activities;
	Analyze technology challenges identified as part of the concepts, design or implementation activities, or that may arise during the development of the system and make recommendations for their resolution based on the results of the analysis;
	Manage and support the deployment of any ARMOUR TD project related results at system and network levels for testing, experimentation and deployment purposes;
	Advise on the procurement of system and network equipment to support the growing needs of the ARMOUR TD project based initial operational capability.

RESOURCE	RESPONSIBILITIES
Technical Writer	Work with the Contractor development team to create robust technical documentation using a rigorous documentation process such as IEEE-12207;
	Manage and enforce documentation standards;
	Produce technical documents and assign writing and reviewing responsibilities as required;
	Maintain software system documentation including the description of the project and business purpose, high level and detailed levels architecture/design and network topology, detailed installation instructions of all key software components;
	Develop operator guides, quick reference guides, context-sensitive online help or site navigation maps;
	Validate information contained in any produced document;
	Develop and validate operator and train-the-trainer training materials.
User Interface Analyst	Maintain and enforce the User Interface Design methodology;
	Continue to review and assess the operator interface requirements and preferences based on the Functional architecture and user feedback from operational rollout;
	Create and validate mock-ups of additional operator interfaces prior to implementation;
	Develop and assess User Acceptance Metrics.
Hardware Architect	Design, develop and implement ARMOUR hardware architecture;
	Analyse computer software systems, data, communications and response requirements;
	Develop computer hardware configurations to support the ARMOUR project procurement processes;
	Develop techniques to improve system throughout and optimize hardware utilization;
	Develop and enforce hardware maintenance and monitoring protocols;
	Analyse ARMOUR physical systems shortfalls and propose corrective affordable hardware measures.
Data Warehouse Architect	Design, develop and maintain ARMOUR logical data architecture, models and databases;
	ANALYZE TECHNOLOGY CHALLENGES IDENTIFIED AS PART OF THE CONCEPTS, DESIGN OR IMPLEMENTATION ACTIVITIES, OR THAT MAY ARISE DURING THE DEVELOPMENT OF THE SYSTEM AND MAKE RECOMMENDATIONS FOR THEIR RESOLUTION BASED ON THE RESULTS OF THE ANALYSIS;Provide technical oversight in the use and optimization of data modeling techniques for ARMOUR project;
	Apply data warehouse design principles and tenets;
	Provide expertise relating to data issues correlation of security relevant data from multiple and overlapping sources
	Maintain data coherence and persistence.

RESOURCE	RESPONSIBILITIES
Computer Network Defence Functional Analyst	Act as a Computer Network Defence (CND) Subject Matter Expert (SME), providing oversight for functional analysis and understanding of the CF CND operational processes; Maintain and communicate up-to-date analyses about DND CND systems shortfalls and improvement requirements; Survey allies similar initiative and publish news updates; Support the assessment and critique of any ARMOUR proposed solution and its potential to address known CF CND requirements.
Information Technology Security Analyst	Assume responsibility to review, develop and enforce Information Technology (IT) security policies, standards, guidelines and procedures; Conduct reviews of backups and recovery plans; Provide advice on the security aspects of application systems under development.
Information Technology Certification and Accreditation Specialist	Review, develop and enforce Information Technology (IT) certification and accreditation work plans, in accordance with DND C&A Guidelines; Conduct security threat and risk assessment (TRA) studies of the planned ARMOUR TD project related initial operational capability.
System Programming	
Senior Programmer	Ensure the feasibility of implementing incremental changes to the overall architecture and design of the system to be developed; Provide directives to the team of programmers to implement and program changes and enhancements to the targeted system solution; Implement and program the system solution and the associated components; Provide advice on various software systems technologies including distributed systems at various levels such as clients, servers and peer-to-peer systems, service oriented architectures, messaging, e-mail, wireless protocols, and remote method invocation, TCP/IP networking at various levels such as TCP/IP addresses, sockets and ports, IP multicasts and DNS, and integration of legacy systems with the core system; Analyze technology challenges identified as part of the concepts, design or implementation activities, or that may arise during the development of the system and make recommendations for their resolution based on the results of the analysis; Plan, control and evaluate systems testing, and provide directives to the team of programmers.

RESOURCE	RESPONSIBILITIES
Intermediate Programmer	Support the deployment and the experimentation of the test-bed to fulfil the needs of the experimentations such as providing logging/tracking mechanisms, storing experimentation data and producing results to be analyzed by the researchers; Work with the system operators to determine what data will be used; Provide strategies to replicate sources of information that cannot be directly accessed by the system; Analyze technology challenges identified as part of the concepts, design or implementation activities, or that may arise during the development of the system and make recommendations for their resolution based on the results of the analysis. Implement and program the system solution and the associated components; Provide development leadership to support junior programmers; Advise on best course of actions related to lower level implementation details; Security review and modification of contributed source code.
Junior Programmer	Implement and program the system solution and the associated components; Perform system, units and integration tests, and report on results obtained; Verify accuracy and completeness of programs by preparing sample data, and testing them by means of system test runs performed by various project participants.
Senior WEB Developer	Design, build, implement and maintain new web sites or upgrade existing web sites in line with client specifications; Prototype and produce web site simulations from client requirements to determine the best proposal for web site appearance and operation; Develop and prepare diagrammatic plans for web based service delivery using web-services (or similar web-based service oriented architecture technologies); Select and use available web development tools for linking web-based clients, applications and systems to "back-end" information systems and databases; Design, code, verify and correct web pages and systems based on web-services (or similar web-based service oriented architecture technologies) to meet system requirements; and Analyze problems outlined by systems analysts/designers in terms of such factors as style and extend of information to be transferred across web-services infrastructures or similar web-based service oriented architecture technologies.

RESOURCE	RESPONSIBILITIES
System Engineering and Operations	
Operating System Administrator	Monitor, manage and support system architecture, hardware, servers, operating systems and application software;
	Perform and provide installation, configuration, maintenance and troubleshooting services in support of server communication architecture, server to workstation and hardware, software, peripherals and related equipment;
	Maintain user access and IT security practices and policies enforced by the department;
	Develop and/or maintain system backup strategies;
	Develop and/or maintain operating guidelines, procedures and standards in support of existing systems or newly introduced hardware, software or application releases;
	Provide advise and cost estimates to the PM on the purchase of new IT hardware and software to optimize the use of computer systems;
Project Test Coordinator	Develop, implement and supervise an overall testing strategy, plans and activities;
	Act as the subject matter expert with regard to testing tools and techniques;
	Develop standards and processes to follow with regard to system integration testing, and system readiness assessment;
	Ensure that the standards established by the Quality Assurance Specialist (QAS) are applied by reviewing work plans and interim deliverables;
	Develop test scenarios and test scripts.
Quality Assurance Specialist	Provide support in quality assurance activities;
	Develop and enforce quality assurance policies, procedures, metrics, forms and tools;
	Audit quality reviews and activities providing confirmation that the quality assurance process is being adhered to;
	Audit the project making recommendations for improvement;
	Identify risk areas and propose risk mitigation strategies;
	Security review and approval of source code.
Tester	Establish and operate software testing procedures for unit test, integration test and regression testing with emphasis on automating the testing procedures;
	Establish and operate interoperability testing procedures to ensure that the interaction and coexistence of various software elements conform to appropriate departmental standards and have no unforeseen detrimental effects on the shared infrastructure;
	Establish departmental benchmarks and the tools to assess system performance;
	Establish a validation and verification capability which assumes functional and performance compliance of delivered or proposed solutions with defined operator requirements.

2. CONDUCT OF WORK

2.1 Location of Work

The work associated to the Optional Services Requirement will take place within the National Capital Region (NCR). Some aspects of the Optional Services Requirement could include tasks located at CF Bases within Canada. Canada is open to suggested deployment strategies for this cycle that would minimize travel costs. For example, staging of equipment at a central location for subsequent installation at distributed sites.

Location of work shall be specified in a DND 626 – TASK AUTHORIZATION. The majority of pre-staging and any development work may be performed at the Contractor's facility. The Technical Authority or other authorized government representatives shall have access at all times to the work in progress and to premises where any part of the work is being performed at the Contractor's facility.

2.2 Language of Work

The Contractor's resources must be fluent in English. Ability to communicate in French is considered an asset.

2.3 Hours of Work

The majority of the work to be conducted at DND facilities will be performed between 0700 and 1800 hours daily. In some cases, work may have to be performed outside of above noted working hours to minimize disruption and/or to support experimentation.

2.4 Equipment and Software

This work may require the Contractor to acquire specific equipment, including necessary hardware, software packages, software upgrades or other items essential to support the development or implementation effort. At the request of the Technical Authority, purchases may be initiated under this contract. The portion of funds allocated for possible purchases will be reviewed by the Technical Authority and authorized by means of the DND 626 – Task Authorization. When authorised, any acquisition shall be done in accordance with prevailing Government of Canada requirements, rules and regulations for equipment and software procurement.

The TA or authorized government representative will control the installation of software on DND computers and will also approve the deployment and removal of Contractor equipment to and from DND facilities. Approval by the Technical Authority is required before any equipment procured outside DND, may be brought into DND facilities.

2.5 Travel

Travel required for project management and other tasks within the NCR will not be reimbursed. It is anticipated that limited travel outside of the NCR, but within Canada, will be required in support of some Optional Services Requirement tasks. Travel outside the NCR for will be paid in accordance with current Treasury Board Guidelines for government contracted personnel at the time of the travel. Travel outside the NCR will be specified for each individual task using DND form 626.

2.6 Equipment Provided by Canada

The Contractor will be provided access to facilities and technology supporting the ARMOUR code repository as established in the Basic Requirement in support of the Optional Services Requirement. The Contractor may be provided access to the test-bed infrastructure in the DRDC Cyber Operations Section ARMOUR lab at DRDC Shirley's Bay for the duration of the Optional Services Requirement. Canada may provide the Contractor additional hardware, Canada-developed software and/or related artefacts at the Contractor request, if these requests are considered relevant to the task. Use of Government Furnished Equipment (GFE) will be coordinated and authorized by the Technical Authority, through the appropriate DND agency and specified for the task using DND form 626.

2.7 **Documents to Be Provided to the Contractor**

Canada will provide the Contractor any reference and technical documentation deemed necessary for the conduct of the work and these will be specified in an approved DND 626 – Task Authorization. This could include, for example, documentation related to DND network monitoring technology, network topology or standards. The Contractor may request documents at any time during the contract period and these requests will be evaluated and approved on a case-by-case basis by the Technical Authority.

APPENDIX D – RESOURCE CATEGORY REQUIREMENTS

Each task in the Basic Requirement and the Optional Services Requirement of the ARMOUR TD project will require a selection of resources from the following complete enumeration of Resource Categories.

Table D-1: Resource Category Requirements

RESOURCE	RESOURCE CATEGORY REQUIREMENTS
	Project Management
Project Manager	1. Professional certification from PMI or Post-Graduate Degree in Project Management or Certificate in Project Management from a recognized Canadian educational institution; or at least eight (8) years experience as a Project Manager of software development project(s) (larger than ten (10) Person-Years), within the last twelve (12) years; 2. Experience managing at least three (3) multi-disciplinary software development teams, and/or experience managing software development project(s) in a R&D environment for a combined period of at least four (4) years; 3. At least five (5) years experience using a project management methodology including the following: • Planning and scheduling management; • WBS structuring; • Cost management; • Risk management; • Quality management; • Change management; • Communication management. 4. Experience in two (2) major IT projects (at least 10 Person-Years) successfully conducted with the methodology in point 3, with a reference of the client for each; 5. At least two (2) years experience with a project management software tool.
Project Control Officer	1. PCO experience of at least three (3) years within the last six (6) years with IT project(s) including responsibilities for calculating and reporting of Earned Value schedule tracking; cost tracking; milestone deliverables; and project performance; 2. Production or maintenance of project plans using Microsoft Project® or a similar tool, and performing scheduling, implementation control and managing total system costs for the deployment and the operation of at least one (1) main (more than 1 million dollars) system.
Project Communications Specialist	1. Experience of at least four (4) years within the last six (6) years in communication planning and execution for IT project(s), with the design, management and implementation of project communication plans; 2. Experience of at least two (2) years in development and delivery of training material; 3. Experience of at least two (2) years in product or solution marketing including preparation of promotional or marketing materials (brochures, presentations, etc.) and delivery of marketing presentation to customer and at trade shows or conferences; 4. Experience using MS Office Suite and graphic design software; 5. Experience using WEB technologies as means to implement project communication plans; 6. Experience with geographically distributed teams' communication.

RESOURCE	RESOURCE CATEGORY REQUIREMENTS
Webmaster	1. Experience of at least four (4) years within the last six (6) years with e-business application development, with managing the content of WEB site(s), ensuring the site(s) are up to date and writing programs to create and publish content; 2. Experience of at least two (2) years using programming languages (e.g. VB-Script, Visual Basic, etc.) and WEB/Internet technologies (ASP, HTML, XML, IIS, WEB development, etc.).
System Architecture and Design	
Lead System Architect	1. Experience of at least eight (8) years within the last twelve (12) years in software development; 2. Experience of at least two (2) years with software modeling techniques and tools with Object-Oriented design, Software Development Methodology (e.g., using UML 2.x); 3. Experience of at least two (2) years (cumulative duration) in leading the development of CND related products or solutions.
Software Solution Architect	1. Experience of at least five (5) years within the last eight (8) years with IT project(s) translating business and functional requirements into technical specifications that can be used by the system and/or programming team.
System/Network Analyst	1. Experience of at least three (3) years within the last five (5) years with IT project(s) performing all of the following: • deployment of at least two (2) main systems in a complex network environment; • designing storage architectures (SAN, NAS, Fibre channel); • analyzing performance considerations and project bandwidth requirements in different environments; and • Experience with different platforms, operating systems, database technologies, telecommunication protocols, 2. Experience with systems view products describing the systems and those interconnections between systems that both provide for and support the project functions.
Technical Writer	1. Experience of at least three (3) years within the last five (5) years with IT projects performing all of the following: • researching and analyzing source materials such as specifications, drawings, models, design briefs and IT documents and synthesizing the information into technical write-ups for software developers (specifications), operators (manuals) and trainers (training materials); and • conducting in-depth interviews with software architect, designer, developer, or operator to understand the system to be developed. 2. Experience writing technical documents using software development process standards such as the IEEE-12207; 3. Experience verifying the adequacy of documentation by testing the system.

RESOURCE	RESOURCE CATEGORY REQUIREMENTS
User Interface Analyst	1. Experience of at least four (4) years within the last six (6) years with IT project(s), including experience in at least three (3) of the following categories: • With the help of operators, translating user functional requirements into graphical user interface (GUI) technical specifications that can be used by the system and/or programming team; • capturing insight on workflows, functional and non-functional requirements; • modeling the business process; • profile primary and secondary operator community; • tracking daily usage patterns and functionality; and • system development constraints; 2. Experience with the following: • Web trends; • Browsers; and • Web usability best practices. 3. Experience of at least three (3) years within the last six (6) years translating user functional requirements into graphical user interface (GUI) specifications that can be used by the system and/or programming team for CND related applications and systems or military command and control (C2) user interfaces; 4. Experience of at least two (2) years within the last six (6) years performing GUI software development activities for CND related applications and systems or military C2 user interfaces.
Hardware Architect	1. Experience of at least four (4) years within the last eight (8) years designing system solutions to fulfill requirements for high availability, robustness, performance and scalability with a main focus on the hardware; 2. Experience designing High Availability (HA) systems such as telecom systems or military systems; 3. Experience with hardware estimation for large database systems and applications related to network management systems or security information management systems.

RESOURCE	RESOURCE CATEGORY REQUIREMENTS
Data Warehouse Architect	1. Experience of at least four (4) years within the last six (6) years as a Data Warehouse Architect/Specialist for IT project(s). 2. The administrative responsibility for physical design of at least three (3) data warehouse systems, including: • modelling activities; • creation of database tables and maintenance of the warehouse, in order to develop the vision of physical view of the warehouse; and • designing the data warehouse system to maintain historical data that has been extracted from operational data storage and transformed into formats accessible to the organization's analytical community; 3. DWA experience with at least four (4) of the following data warehouse technology streams with a combined duration of at least three (3) years: • Metadata exploitation; • Performance management; • Data quality; • Schema development; • Data access; • Data management exploiting relational databases (at least one (1) from Oracle or SQL Server); • Extracting, Transforming/Transporting and Loading (ETL) data from source systems into the data warehouse.
Computer Network Defence Functional Analyst	1. CNDA experience of at least five (5) years within the last eight (8) years doing the functional analysis of CND related projects (R&D or operational) and their interfaces for at least two (2) IT projects, advising on concepts and system requirements.
Information Technology Security Analyst	1. Experience of at least five (5) years within the last eight (8) years with IT project(s) that collectively addresses all of the following: • IT Security architecture(s); • IT Security Risk Management Methodology; • Threats to, and vulnerabilities of, networks; • Implementation of IT Security safeguards for personnel and IT Security Assets; • IT Security system monitoring, incident response, recovery, and restoration; and • IT Security audit and assessment
Information Technology Security Certification and Accreditation Specialist	1. Experience of at least five (5) years within the last eight (8) years with IT project(s), conducting security threat and risk assessments of at least three (3) application systems; 2. Experience of at least three (3) years within the last five (5) years in providing Certification and Accreditation support for at least three (3) Government of Canada projects; 3. Experience of at least one (1) year in all of the following main technologies: Security of Open Source Software, Security Information and Event Management (SIEM) systems, Host Based Intrusion Detection and Prevention Systems (IDS/IPS), Network Based IDS/IPS, Firewalls, and CND tools and techniques.

RESOURCE	RESOURCE CATEGORY REQUIREMENTS
	System Programming
Senior Programmer	1. At least five (5) years experience within the last eight (8) years for at least two (2) IT projects, leading the software development of a solution to meet the overall architecture and design of the system; 2. At least three (3) years experience within the last five (5) years for at least two (2) IT projects, leading the maintenance and support of a code repository, including code release tagging and packaging, code branches, code merges and code check-out/in procedure management.
Intermediate Programmer	1. Experience of at least four (4) years within the last six (6) years as a software developer for IT project(s). 2. Experience with all of the following main technologies: • C/C++ on Windows; • client-server and .NET system development; • Java; • client-server and application server (e.g. J2EE) system development; • integration of applications with relational databases; • integration of applications with legacy systems; • Web technologies; • Web services; and • XML
Junior Programmer	1. Experience of at least two (2) years within the last three (3) years as a software developer for IT project(s). 2. Experience with all of the following main technologies: • C/C++ on Windows; • client-server and .NET system development; • Java, client-server and application server (e.g. J2EE) system development; • integration of applications with relational databases; • integration of applications with legacy systems; • Web technologies; • Web services; and • XML

RESOURCE	RESOURCE CATEGORY REQUIREMENTS
Senior WEB Developer	1. Experience of at least four (4) years within the last six (6) years with IT project(s) performing all of the following: • design, build, implement and maintain new web sites or upgrade existing web sites in line with client specifications; • prototype and produce web site simulations from client requirements to determine the best proposal for web site appearance and operation; • develop and prepare diagrammatic plans for web based service delivery using web-services (or similar web-based service oriented architecture technologies); • select and use available web development tools for linking web-based clients, applications and systems to "back-end" information systems and databases; and • design, code, verify and correct web pages and systems based on web-services (or similar web-based service oriented architecture technologies) to meet system requirements.
System Engineering and Operations	
Operating System Administrator	1. Experience of at least three (3) years within the last five (5) years with IT project(s) performing all of the following: • monitoring, managing and supporting system architecture, hardware, servers, operating systems and application software; • performing/providing installation, configuration, maintenance and troubleshooting services in support of server communication architecture, server to workstation and hardware/software, peripherals and related equipment; and • developing and maintaining system backup strategies; 2. Experience with all of the following main technologies: • Network architecture; • Configuration and operation of servers, PCs, portable computers, peripheral devices; • Interaction of network components and PCs to maintain, identify, isolate, diagnose and resolve hardware connectivity and software compatibility-related problems; • Communication architecture, devices, techniques and practices for their installation, configuration, integration and troubleshooting.
Project Test Coordinator	1. Experience of at least four (4) years within the last six (6) years with IT project(s) performing all of the following: • developing test strategies and plans for at least three (3) main systems that have been successfully delivered; • preparing and supervising integrated test plans and schedules for at least three (3) main systems; 2. Experience interacting with cross-functional teams to facilitate an integrated approach to testing engagements; 3. Experience mentoring a group of testers; 4. Experience in methodology guidance, test criteria/standards, quality practices.

RESOURCE	RESOURCE CATEGORY REQUIREMENTS
Quality Assurance Specialist	1. Experience of at least four (4) years within the last eight (8) years with IT project(s), in software system quality efforts including requirement reviews, test strategy development and planning, defect reporting and fix tracking, performance benchmarking and risk management for at least two (2) main systems that have been successfully delivered; 2. Experience with standards for software to be developed, processes and good practices in order to recommend and enforce the right policies according to the needs of the system to be developed, which follow the ISO 35 (such as ISO/IEC 12207), IEEE (such as IEEE 829, 830), CMMi, SEI-CMM or equivalent and applicable documentation and process standards. 3. Experience with processes and methodologies for product security testing and evaluation or certification.
Tester	1. Experience of at least three (3) years within the last five (5) with IT project(s) performing all of the following: • using process and tools to test coded software before it is released; • identifying test data requirements; and • configuring and maintaining test data to support testing; 2. Experience performing use case, test cases, checklists and requirements verification; 3. Experience with at least three (3) of the various types of testing: • Unit testing; • Stress and load testing; • Integration testing; • System and performance tests using manual methods and tools; • Performance benchmarking; • Security testing; • Tracking usability issues and inconsistencies. 4. Experience with client/server and multi-tiers development with a database (Oracle or SQL Server); 5. Experience with Service Oriented Architecture or Web-Services technology testing.

APPENDIX E - LIST OF ABBREVIATIONS

API	Application Programming Interface
ARMOUR TD	Automated Computer Network Defence Technology Demonstration
C&A	Certification and Accreditation
CDRL	Contract Deliverable Requirement List
CF	Canadian Forces
CFNOC	Canadian Forces Network Operations Centre
CMMi	Capability Maturity Model Integration
CND	Computer Network Defence
COTS	Commercial off-the-Shelf
CSEC	Communication Security Establishment Canada
DDRM	Detailed Design Review Meeting
DEA	Director Enterprise Architecture
DID	Data Item Description
DIMEI	Director Information Management Engineering and Integration
DIMTPS	Director Information Management Technologies, Products and Services
DIR IM Secur	Director Information Management Security
DND	Department of National Defence
DREnet	Defence Research Establishment network
DRDC	Defence Research & Development Canada
GOTS	Government off-the-Shelf
GUI	Graphical User Interface
HTRA	Harmonized Threat And Risk Assessment
HW	Hardware
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IAP	Interim Authority to Process
IEC	International Electrotechnical Commission
IF	Integration Framework
IM	Information Management
IOC	Interim Operating Capability
IP	Intellectual Property
ISO	International Standards Organization
IT	Information Technology

Net C2 ISAC	Network Command and Control Integrated Situation Awareness Capability
NCR	National Capital Region
OCI	Office of Collateral Interest
OPI	Office of Primary Interest
OSP	Open Source Project
OSS	Open Source Software
PA	Project Authority
PC	Personal Computer
PDF	Portable Document Format
PDRM	Preliminary Design Review Meeting
PM	Project Manager / Project Management
PRM	Project Review Meeting
PWGSC	Public Works and Government Services Canada
R&D	Research and Development
RCMP	Royal Canadian Mounted Police
RFP	Request for Proposal
RRM	Readiness Review Meeting
SEI-CMM	Software Engineering Institute - Capability Maturity Model
SOA	Service Oriented Architecture
SOW	Statement of Work
SRS	System Requirements Specification
STS	System Technical Specification
SW	Software
TA	Technical Authority
TD	Technology Demonstration
TDP	Technology Demonstration Program
TRA	Threat and Risk Assessment
UML	Unified Modeling Language
V&V	Validation and Verification
VM	Virtual Machine
WBS	Work Breakdown Structure
XML	Extensible Markup Language

Government of Canada	Gouvernement du Canada	Contract Number / Numéro du contrat
		W7714-115274
		Security Classification / Classification de sécurité Unclassified

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine Defence R&D Canada	2. Branch or Directorate / Direction générale ou Direction Cyber Operations

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

Implementation of the ARMOUR Technology Demonstration project

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

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

	No / Non	Yes / Oui
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)		✓
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.	✓	
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?	✓	

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

Canada		NATO / OTAN		Foreign / Étranger	
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)

Government
of Canada

Gouvernement
du Canada

Contract Number / Numéro du contrat
W7714-115274

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

	Government of Canada	Gouvernement du Canada

Contract Number / Numéro du contrat
W7714-115274
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			CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET
											A	B	C			
Information / Assets Renseignements / Biens																
Production																
IT Media / Support TI																
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE? [✓] No / Non [ ] Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, 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).

Contract Number / Numéro du contrat
W7714-115274
Security Classification / Classification de sécurité
Unclassified

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Jonathan Risto	Project Manager, ARMOUR TDP	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-990-6015	613-993-9940	jonathan.risto@drdc-rddc.gc.ca	2012-09-12

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

Name (print) - Nom (en lettres moulées) Gasha Medjovic - CFIMP GReHQ - Industrial Security
Senior Security Analyst
Tel: 613-949-1066 / Fax: 613-949-1069
E-mail: sasa.medjovic@forces.gc.ca

Signature

Date 2012-09-17

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

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

No / Non ☐ Yes / Oui ☑

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Peter Murray	A/Supply Team Leader	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
819-956-1387	819-997-2229	Peter.Murray@tpsgc-pwgsc.gc.ca	2013-01-07

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
			Oct. 4/12

Joelle Smith MOFFATT
Contract Security Officer, Contract Security Division
Joelle.Smith@tpsgc-pwgsc.gc.ca
Tel/Tél - 613-948-1726 / Fax/Téléc - 613-954-4171

Security Classification / Classification de sécurité
Unclassified

Canada

ARMOUR Technology Demonstration - Security Clearance Requirements

Within the ARMOUR Technology Demonstration (TD), there is a requirement to have personnel authorized to access different levels of information. For the majority of the personnel working on the project, a current RELIABILITY STATUS clearance will be sufficient. This valid and current clearance will be required for the entire duration of the project (from contract award to project close out). All personnel included in the contract proposal must have this clearance at the time of bid submission. All personnel working on the ARMOUR TDP must have this clearance active prior to commencing work on the project.

In addition to the above requirement, the Key Technical Personnel on the project team will require Level II (SECRET) clearance. The Key Technical Personnel, as outlined in the RFP, are individuals who fill the following positions:

- Project Manager (PM);
- Lead System Architect (LSA);
- Software Solution Architect (SSA);
- User Interface Analyst (UIA);
- Computer Network Defence Functional Analyst (CNDFA);
- Information Technology Security Analyst (ITSA);
- Certification and Accreditation Specialist (CAS);
- Senior Programmer (SP); and
- Quality Assurance Specialist (QAS).

Some additional personnel beyond the above list will require a Level II (SECRET) security clearance during the course of the ARMOUR TD project main contract. This includes any individual(s) who will be involved in the deployment of the ARMOUR TD project demonstration system on the DRENet at DRDC-Ottawa site(s). This level of clearance will be required for the entire duration of the project (from contract award to project close out), and this clearance must be active prior to commencing work on the project.

Some personnel will require a Level II (SECRET) security clearance to perform tasks as part of the Optional Work outlined in the RFP, if such Optional Work is exercised. At minimum, any individual(s) who will be involved in the deployment of capabilities related to the ARMOUR TD

project results on the CFNOC or any other DND/CF operational network will require Level II (SECRET) clearance. Where this clearance is required, it will be clearly identified on the DND/CF Task Authorization - Form 626. All resources assigned to work on these tasks must have this level of clearance at the time of contractor response to the DND/CF Task Authorization – Form 626.

ANNEX F

ARMOUR TD Project Intellectual Property Strategy

The ARMOUR Technology Demonstration (TD) project wants to influence and enable external research programs to develop capabilities for the Department of National Defence and other government departments. To that end, the ARMOUR TD project will build its technology on an Integration Framework that will allow processing modules by various third parties to plug in and provide capabilities that contribute to an automated end-to-end computer network defence tool. The external programs we aim to assist and influence are those of industry, academia, research institutes and allies.

Canada Owned Foreground Information - Integration Framework

The Foreground Information of the Integration Framework resulting from performance the ARMOUR TD project Work will be owned by Canada in alignment with the TBS "Policy on Title to Intellectual Property Arising Under Crown Procurement Contracts."

If the Contractor wants to use the Integration Framework Foreground Information for the commercial exploitation or further development of the Foreground Information, the Contractor must obtain a license from DRDC. The Contractor should make a request in writing for such a license no later than 30 working days following completion of the Contract. In its request for a license to DRDC, the Contractor must explain why the license is required and how the Contractor intends to use the information.

Government Supplied Processing Modules

DRDC owned processing modules may form part of the ARMOUR TD project Work. At the request of the Contractor, these modules can be furnished in source code form for use by the Contractor and could be provided in executable form under the License for the Purpose of Further Development and Advancing the State of the Art or Licensing for Commercialization described below.

Licensing ARMOUR TD Project Results for the Purpose of Further Development and Advancing the State of the Art

For the purposes of further development and advancing the state of the art in the field of computer network defence, DRDC intends to make available, either as a whole or any parts thereof, the ARMOUR TD project results and a working version of the delivered ARMOUR system used to demonstrate the ARMOUR TD project results to industry, academia, research institutes and allies for non-operational use. This could include: a copy of turn-key installation of the ARMOUR system; source code and executable code of the Canada owned Foreground Information; executable code of the Contractor owned Foreground Information; executable code of proprietary processing modules; and system documentation. If this information is made available, it will be facilitated by a license to the Foreground Information, including a sublicense to the necessary Background Information required to fully exercise Canada's rights in the ARMOUR TD project Contract deliverables and in the Canada owned Foreground Information.

If Canada does license this information, the information may only be used for the purposes of further development and advancing the state of the art. The information may not be used for operational purposes or commercialization.

For greater certainty, it is acknowledged that the processing modules used in the delivered ARMOUR system may be a proprietary version of a commercial off the shelf product not developed in the performance of the ARMOUR TD project Work. In this case, only executable version of the proprietary processing modules will be provided under Canada's license to a third-party. In the event that the third-party wishes to evaluate a higher performance version of the proprietary processing module, the third-party must negotiate a separate license for the high performance version with the owner of the proprietary processing module.

Reference Terminology

for the

Automated Computer Network Defence

(ARMOUR)

Technology Demonstration

(TD)

Defence Research and Development Canada

3701 Carling Avenue

Ottawa, ON K1A 0Z4

Version

2.0

Date

18 January 2013

Table of Contents

1 Purpose

The purpose of this document is to provide a common document containing definitions of terminology commonly used within the Automated Computer Network Defence (ARMOUR) Technology Demonstration (TD) Project and related documentation. Terms applicable to the System Technical Specification are identified by the acronym "STS". Terms applicable to the Statement of Work are identified by the acronym "SOW".

2 Terminology

Access (STS, SOW)
Ability and means to communicate with or otherwise interact with an asset, to use asset resources to handle information, to gain knowledge of the information the asset contains, or to control asset components and functions.
(Source: NIST IR 7298 Revision 1)

Abstracted Infrastructure Data (STS)
The Normalized Infrastructure Data is processed by the Common Infrastructure Abstraction process to create the Abstracted Infrastructure Data. For example, a subnet of related workstations with the same configuration and reachability may be abstractly represented as a single device.
(Source: ARMOUR)

Act Phase (OODA loop) (STS, SOW)
In the Act phase of the OODA loop, the selected courses of action are implemented.
(Source: ARMOUR)

Asset (STS, SOW)
Anything that has value to the organization. For example, an operation, network route and hosts are all assets.
(Source: ISO/IEC13335-1:2004)

Attack (Cyber Attack) (STS, SOW)
Malicious activity, via cyberspace (an environment in which digitized information is distributed on networks of computers), targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information.
(Source: NIST IR 7298 Revision 1)

Attack Asset (STS)
Any cyber asset that can be used in an attack. For example, network routes, the fact that a service is running and a software vulnerability are attack assets.
(Source: ARMOUR)

Attack Dependence Metric (STS)
A metric indicating the degree of dependence the attacker (with capabilities according to an attacker model) places on Attack Assets.
(Source: ARMOUR)

Attack Graph (STS, SOW)
An attack graph (exploit-dependency graph) is a mathematical abstraction of the preconditions for the attacker to gain privileges in the network, and the post conditions indicating which privileges were gained. The attack graph is represented by a graph data structure and encodes the way individual attacks may be chained together to form complex multi-step attacks.

(Source: ARMOUR)

Attack Graph Analyzer (Proactive and Reactive) (STS)
A module in the Computational Services component that computes an attack dependence metric for every vertex in the attack graph (proactive or reactive). It does this through analysis of the attack graph based on vulnerability characteristics (e.g.: maturity of exploits), attacker models, and prioritized operational goals to protect. The calculated attack dependence metrics are stored as an attribute of the attack graph and enable the production of the Ranked Attack Assets List (Proactive or Reactive).
(Source: ARMOUR)

Attack Graph Generator (STS)
A module in the Computational Services component that generates attack graphs.
(Source: ARMOUR)

Attack Path (STS, SOW)
A sequence of attack steps within an attack graph from an attack source to a goal to protect.
(Source: ARMOUR)

Attack Path Overlay (STS)
A visual representation of the details contained in an attack graph onto a non-attack-graph visualization method. For example, representing the details of an attack path onto a network visualization is an attack path overlay onto the network visualization.
(Source: ARMOUR)

Attack Source (STS)
The starting point of an attack (see definition).
(Source: ARMOUR)

Attack Steps (STS, SOW)
An atomic attack within an attack path corresponding to the gaining of a privilege. For example, gaining the privilege to execute arbitrary code on a host is an attack step.
(Source: ARMOUR)

Attacker Model (STS)
Describes the capabilities (e.g., computation resources, skills, exploits) of a class of attackers.

Automated Response (STS, SOW)
 A response that is partially or completely automatic.
(Source: ARMOUR)

Automated Response Generator Module (STS)
A module within the Computational Services component that effectuates courses of action. Automated responses may include reconfiguration of software settings (e.g. reconfiguring or disabling a process), disabling a user account, or reconfiguration of network connectivity.
(Source: ARMOUR)

Automation Settings (STS)
Establishes thresholds for the Automated and Semi-Automated Response Generators to determine actions that may be effectuated without operator intervention (selection and instantiation).
(Source: ARMOUR)

Bell-LaPadula Model (STS)
A mathematical model of a multi-level security policy focused on maintaining the confidentiality of objects.
(Source: ARMOUR)

Biba Model (STS)
A mathematical model of a multi-level security policy focused on maintaining the integrity of objects.
(Source: ARMOUR)

Certification and Accreditation (C&A) (SOW)
    Certification
    A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.
    Accreditation
    An administrative action by which a designated authority declares that an information system is approved to operate in a particular security configuration within a prescribed set of safeguards. An accreditation is usually based on a technical certification of the system's security mechanisms. To accredit a system, the approving authority must determine that any residual risk is an acceptable risk.

Collect (SOW)
Collect in terms of "collect and predict" means the collection of data in the observe phase of the OODA loop. In the Observe phase, both asset and operationsl data is collected and stored.
(Source: ARMOUR)

Common Infrastructure Abstraction module (STS)
A module within the Computational Services component that abstracts common elements within the Normalized Infrastructure Data into a single representation. The purpose of this module is to reduce the amount of information to be processed by other modules. For example, a subnet of related workstations with the same configuration and reachability may be abstractly represented as a single device. This information is stored as Abstracted Infrastructure Data.
(Source: ARMOUR)

Component (STS, SOW)
A collection of system resources that form a logical part of the systemhaving specified functions and interfaces, and is treated as existing independently of other parts of the system.
(Source: RFC 4949)

As used in ARMOUR documentation, a component refers to any of the Data Sources, Data Source Connectors, Database, Computational Services, Data Presentation and Sharing, Effector Connectors or Effectors defined in the conceptual architecture of the ARMOUR TD.
(Source: ARMOUR)

Compromise (Security compromise) (STS, SOW)
A security violation in which a system resource is exposed, or is potentially exposed, to unauthorized access.
(Source: RFC 4949)

Computational Services Component (STS)
Comprises all modules (see definition) that process data from the Database component to deliver intelligent CND capabilities.
(Source: ARMOUR)

Computer Network Defence (STS, SOW)
Cyber actions taken to defend against unauthorized activity within computer networks.
(Source: ARMOUR)

Confidentiality (STS, SOW)
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.
(Source: NIST IR 7298 Revision 1)

Course of Action (STS, SOW)
A set of actions to mitigate threats and attacks. Each of the individual actions that make up a course of action must be implemented to have the desired effect. The plural of "course of action" is "courses of action".
(Source: ARMOUR)

Course of Action List (Proactive and Reactive)
The output from the Course of Action Analyzer (Proactive and Reactive) providing a list of courses of action that may be effectuated in an automated or semi-automated manner.
(Source: ARMOUR)

Criticality (STS)
A measure of the degree to which an organization depends on an asset for the success of an operation or of a business function.
(Source: ARMOUR)

Cross-Source Correlation Module (STS)
A module within the Computational Services component, cross-source correlation is a process to combine multiple references of the same information) into a single representation. For example, information collected from a configuration management database and vulnerability scanner concerning the same host may be correlated into a single representation of data concerning that host.
(Source: ARMOUR)

Cyberspace (STS, SOW)
A global domain within the information environment consisting of the interdependent network of information systems infrastructures that may include the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
(Source: ARMOUR)

Database Component (STS)
Comprises the database management system (DBMS) and data store. It provides data security (confidentiality, integrity, and availability) and data archiving services. It is the repository of the raw data as well as the modified and value-added results of Computation Services component modules.
(Source: ARMOUR)

Data Presentation Component (STS)
Comprises the graphical user interface (GUI), reporting, and data formatting modules. The products of the GUI and reporting modules are intended for human consumption while the products of the data formatting module are intended for automated processing.
(Source: ARMOUR)

Data Sources (STS)
Comprises the infrastructure and non-infrastructure information feeds to the ARMOUR system. Examples include vulnerability reference data, audit logs, security alerts, network management events, etc.
(Source: ARMOUR)

Data Source Connectors (STS)
APIs that provide interfaces between the ARMOUR Integration Framework and all Data Sources. The Data Source Connectors are defined by the types of data, technology and data transformation requirements of the ARMOUR system.
(Source: ARMOUR)

Data Store (STS)
Data storage devices accessed by the DBMS and comprising part of the Database component.
(Source: ARMOUR)

Decide Phase (OODA loop) (STS, SOW)
In the Decide phase of the OODA loop, optimized and prioritized courses of action are computed to respond to the situations identified and characterized in the Orient phase.
(Source: ARMOUR)

Defensive Posture (STS, SOW)
The degree to which assets are exposed to cyber attack, according to an attacker model, and the criticality of the assets in an operational context.
(Source: ARMOUR)

Effector Connector (STS)
APIs that provide interfaces between the ARMOUR Integration Framework and all Effectors. The Effector Connectors are defined by the types of data, technology and data transformation requirements of the ARMOUR system.
(Source: ARMOUR)

Effectors (STS)
Technologies implementing courses of action. For example, configuration console for a host intrusion prevention system, ticketing system, or network management system.
(Source: ARMOUR)

Exploit(s) (Exploit code) (STS)
An exploit (from the same word in the French language, meaning "achievement", or "accomplishment") is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerised). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack.
(Source: http://en.wikipedia.org/wiki/Exploit_(computer_security), accessed on May 27th, 2011)

Fully-Automated Response (STS, SOW)
A response process that does not require operator intervention.
(Source: ARMOUR)

Fully-Automated Response Module (STS, SOW)
A module within the Computation Services Component that processes proactive and reactive courses of action and does not require operator Intervention.
(Source: ARMOUR)

Hosts (STS)
A commonly used term for an addressable system or computer in TCP/IP based networks like the Internet.
(Source: www.gcpedia.gc.ca/wiki/Cyber_Security_Lexicon ISO/IEC FCD 18043: 2005-06-10)

Incident (security incident) (STS, SOW)
An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
 (Source: NIST IR 7298 Revision 1)

Incident Analyzer (STS)
A module within the Computation Services Component that assesses infrastructure-based events to identify the host and other relevant information (e.g.: vulnerability and privilege level gained) of ongoing incidents.
(Source: ARMOUR)

Infrastructure Data (STS)
Information about the organization's network physical and logical assets (e.g., events, router configurations, hosts, and host services).
(Source: ARMOUR)

Infrastructure Management System (STS)
IT systems supporting Information and Communication Technology (ICT) Infrastructure Management and Security Management as described in the Information Technology Infrastructure Library (ITIL). For additional information concerning ITIL, please refer to the ITIL website at: http://www.itil-officialsite.com/
(Source: ARMOUR)

Integration Framework (STS, SOW)
A software architecture and resulting implementation that provides inter-module messaging, security, event and format verification services. Format verification services are applied to data as it is received from the Data Source Connectors or transmitted to the Effector Connectors for the ARMOUR system.
(Source: ARMOUR)

Inter-Module Messaging (STS)
Communication services between modules within the Integration Framework.
(Source: ARMOUR)

Intrusion (STS, SOW)
An unauthorized act of bypassing the security mechanisms of a system. A type of threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections.
(Source: RFC 4949)

Intrusion Detection Systems (IDS) (STS, SOW)
Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)
(Source: NIST IR 7298 Revision 1)

Intrusion Detection Systems (Host-Based) (STS, SOW)
IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily "see" the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.
(Source: NIST IR 7298 Revision 1)

Intrusion Detection Systems (Network-Based) (STS, SOW)
IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.
(Source: NIST IR 7298 Revision 1)

Intrusion Prevention System (IPS) (STS, SOW)
System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
(Source: NIST IR 7298 Revision 1)

Intrusion Detection and Prevention System (IDPS) (STS)
Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.
(Source: NIST IR 7298 Revision 1)

Loss Cost (STS)
A metric that reflects the impact to operations, personnel time, and monetary cost of effectuating COA items.
(Source: ARMOUR)

Malicious software (STS)
Software intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
(Source: NIST IR 7298 Revision 1)

Malware
See Malicious software.

Module (STS)
As used in ARMOUR, a module is any of the software architectural parts comprising the components (see definition of component) of the ARMOUR TD. For example, the Attack Path Generator is a module within the Computational Services component.
(Source: ARMOUR)

North Atlantic Treaty Organization (NATO) Cyber Defence Data Exchange and Collaboration Infrastructure (CDXI) (STS, SOW)
NATO CDXI is a mechanism for member nations to share vulnerability data. It is an application that provides the means to exchange and collaborate on reference data and event data.
(Source: ARMOUR)

Normalized Infrastructure Data (STS)
The Normalized Infrastructure Data includes correlated information to identify operations, operational services, hosts, installed software, remotely or locally listening host services, vulnerabilities, and dependency information. Dependency information includes operation to operation, operations to operational services, (operational or host) service to (operational or host) service, and host service to host.
(Source: ARMOUR)

Normalized Infrastructure Events (STS)
Correlated network events are stored as the Normalized Infrastructure Events relative to the Normalized Infrastructure Data in the data warehouse.

(Source: ARMOUR)

National Vulnerability Database (NVD) (STS, SOW)
NVD is the U.S. government repository of standards based vulnerability management data.
(Source: ARMOUR)

OODA loop (STS, SOW)
Concept originally applied to combat operations and having the four phases of observe, orient, decide, and act (OODA). ARMOUR applies the concept to computer network defence (CND) operations.
(Source: ARMOUR)

Observe (OODA loop) (STS, SOW)
In the Observe phase, both system and operations data is collected and stored. Information from sensors and network management systems push data to ARMOUR as the data is generated.
(Source: ARMOUR)

Operational Services (STS)
Capabilities supporting operations (or business processes) and resulting from host services provided by infrastructure. Examples of operational services are command and control, surveillance, email, printing, and file sharing.
(Source: ARMOUR)

Operations and Infrastructure Analyzer (STS)
A module within the Computational Services components that, evaluates operations and host service dependencies to identify priority goals to protect.
(Source: STS)

Operations data (STS, SOW)
Information about the organization's missions (e.g. operation identifier, priority, operational dependencies).
(Source: ARMOUR)

Operational dependencies (STS, SOW)
Relationships between operations and their dependencies including operation to operation dependencies, operation to infrastructure and infrastructure to infrastructure dependencies and infrastructure to physical location.
(Source: ARMOUR)

Operation Dependence Metric (STS)
A metric assigned to operations, application services, host services, possible host-to-host-on-protocol-and-port connections, and hosts. It is derived from the operation priority values of uniquely identified operations.
(Source: ARMOUR)

Orient (OODA loop) (STS, SOW)
In the Orient phase, the operational priority metric and attack information is computed. Modules in the Computation Services component retrieve data from the database and store results back to the database.
(Source: ARMOUR)

Prioritized Course of Action List (STS)
A list of courses of action identified to mitigate potential attack paths due to known vulnerabilities and network configurations that may be exploited.
(Source: ARMOUR)

Proactive Computer Network Defence (STS, SOW)

Actions taken to increase the assurance of operations by evaluating and increasing the security of the network, evaluated independently of information related to individual incidents.
(Source: ARMOUR)

Proactive Course of Action Analyzer (STS)
A module that provides a prioritized list of recommended courses of action to mitigate potential attack paths due to known vulnerabilities and network configurations that may be exploited.
(Source: ARMOUR)

Ranked Attack Assets Lists (Proactive and Reactive) (STS)
A list of attack assets ranked according to the attack dependence metric.
(Source: ARMOUR)

Reachability Analyzer Module (STS)
A module within the Computation Services component that creates the Reachability Graph.
(Source: ARMOUR)

Reachability Graph (STS)
Data represented in a graph data structure that contains all information describing connectivity between source and destination hosts, including port and protocol information.
(Source: ARMOUR)

Reactive Computer Network Defence (STS, SOW)
Actions taken to increase the assurance of operations by evaluating and increasing the security of the network by responding to individual incidents.
(Source: ARMOUR)

Reactive Course of Action Analyzer (STS)
A module that provides a prioritized list of recommended courses of action to mitigate actual attacks due to identified incidents, known vulnerabilities and network configurations that may be exploited.
(Source: ARMOUR)

Reference Data (STS, SOW)
Describes software vulnerabilities, configurations and exploits that can lead to security compromise.
(Source: ARMOUR)

Secunia (STS)
A commercially available reference-data repository.
(Source: ARMOUR)

Semi-Automated Response (man-in-the-loop) (STS, SOW)
A response process requiring operator intervention.
(Source: ARMOUR)

Semi-Automated Response Generator Module (STS, SOW)
A module within the Computation Services Component that processes proactive and reactive courses of action and requires operator intervention to initiate the response.
(Source: ARMOUR)

Simulation Mode (STS)
A mode that allows the security analyst to perform speculative analysis to discover the potential security impact of hypothetical changes to the infrastructure, operational environment, or vulnerabilities.
(Source: ARMOUR)

Speculative analysis (STS)

Analysis based on the modification of vulnerability reference data, infrastructure data and operational dependency data, by making hypothetical changes and examining the subsequent results of the ARMOUR evaluations.
(Source: ARMOUR)

Strategic Change (STS, SOW)
A large scale architectural change to significant physical or logical assets requiring planning, acquisition, and deployment. For example, installation of new services or changing host operating systems.
(Source: ARMOUR)

System (STS, SOW)
A set of connected assets forming a complex whole. In the context of ARMOUR, system never refers to individual hosts.
(Source: ARMOUR)

Tactical Change (STS, SOW)
A small scale change to logical assets requiring a low to moderate level of effort. For example, stopping a host service or installing a patch.
(Source: ARMOUR)

Threat (STS, SOW)
A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.
(Source: RFC 4949)

Vulnerability (STS, SOW)
A weakness in a system, application, or network that is subject to exploitation or misuse.
(Source: NIST IR 7298 Revision 1)