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 a Standing Offer
Demande d'offre à commandes

Regional Individual Standing Offer (RISO)

Offre à commandes individuelle régionale (OCIR)

Canada, as represented by the Minister of Public Works and Government Services Canada, hereby requests a Standing Offer on behalf of the Identified Users herein.

Le Canada, représenté par le ministre des Travaux Publics et Services Gouvernementaux Canada, autorise par la présente, une offre à commandes au nom des utilisateurs identifiés énumérés ci-après.

Comments - Commentaires

Title - Sujet
RCMP Multimedia Network Convergence

Solicitation No. - N° de l'invitation	**Date**
M9010-091080/C	2012-03-09
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
M9010-091080	PW-$TSS-003-23889
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
003tss.M9010-091080	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2012-03-26

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

Delivery Required - Livraison exigée
See Herein

Address Enquiries to: - Adresser toutes questions à:	**Buyer Id - Id de l'acheteur**
Beaton(tss div), Michelle	003tss
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(819)956-5847 ( )	(819)956-3703

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
ROYAL CANADIAN MOUNTED POLICE
12000 VANIER PARKWAY
ATTN: RANDY ROBERT, LOADING DOCK 2B
OTTAWA
Ontario
K1A0R2
Canada

Security - Sécurité
This request for a Standing Offer includes provisions for security.
Cette Demande d´offre à commandes comprend des dispositions en matière de sécurité.

Instructions: See Herein

Instructions: Voir aux présentes

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

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
Data Centre Services/Services des centres de traitement de données
5C2, Place du Portage, Phase III
11 Laurier Street
Gatineau
Québec
K1A 0S5

Canada

The documents for this Request For Standing Offer are attached.

REQUEST FOR STANDING OFFER

For

Multimedia Network Convergence
Equipment and Support Services

For

Royal Canadian Mounted Police (RCMP)

Table of Contents

Annexes:

Solicitation M9010-091080/C supercedes the previously published solicitations M9010-091080/A and M9010-091080/B.

PART 1 GENERAL INFORMATION

1.1 Introduction

The Request for Standing Offers (RFSO) is divided into seven parts plus attachments and annexes, as follows:

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

Part 2 - Offeror Instructions: provides the instructions applicable to the clauses and conditions of the RFSO;

Part 3 - Offer Preparation Instructions: provides offerors with instructions on how to prepare their offer to address the evaluation criteria specified;

Part 4 - Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria which must be addressed in the offer, if applicable, and the basis of selection;

Part 5 - Certifications: includes the certifications to be provided;

Part 6 - Security, Financial and Insurance Requirements: includes specific requirements that must be addressed by offerors; and

Part 7 - 7A, Standing Offer, and 7B, Resulting Contract Clauses:

7A, includes the Standing Offer containing the offer from the Offeror and the applicable clauses and conditions;

7B, includes the clauses and conditions which will apply to any contract resulting from a Call-up made pursuant to the Standing Offer.

The Annexes include the Requirement, the Basis of Payment and any other annexes.

1.2 Summary

This Request For Standing Offer (RFSO) is being issued by Public Works and Government Services Canada (PWGSC) on behalf of the Royal Canadian Mounted Police (RCMP) to satisfy a requirement for the supply of networking and Internet Protocol (IP) products as well as related IT professional services to augment, enhance, and in some cases replace existing equipment, with the primary goal of migrating RCMP multimedia (radio, voice and video) onto the existing RCMP IP data network. The IT professional services will provide the RCMP with specialized assistance in the design and planning required to support the RCMP's convergence project on a national scale.

The multimedia services being migrated include:

a) Voice over IP;
b) Voice messaging over the IP Network;
c) Call center deployment of VoIP;

d) Radio over IP;
e) Emergency services;
f) Remote monitoring networks;
g) Wireless LAN and bridging; and
h) Video over IP for surveillance and for conferencing.

The required equipment Device Categories are:

a) Access Routers;
b) Data Centre Bridging;
c) Voice over IP;
d) Radio over IP;
e) IP Video Monitoring;
f) IP Video Conferencing;
g) Wireless LAN; and
h) Wireless IDS/IPS.

The technical specifications for the products in these Device Categories are described in Annex A (Requirement) and Offerors must offer products in all these categories that meet all the mandatory requirements.

Offerors are not required to be the Original Equipment Manufacturer (OEM) of any products to submit an offer, but for any given Device Category, it is mandatory that all the equipment proposed come from a single OEM.

In addition to these Device Categories, there are certain components that the RCMP requires for existing Cisco devices already owned by the RCMP. Offerors must offer either these Cisco components or propose an equivalent substitute, which the Offeror must demonstrate is equivalent in accordance with the provisions of this RFSO.

The required professional services categories are:

a) Network Architect;
b) Network Project Manager; and
c) OEM Product Specialist.

This procurement is set aside under the federal government's Procurement Strategy for Aboriginal Business, as detailed in Annex 9.4 - Requirements for the Set-aside Program for Aboriginal Business, of the Supply Manual (see note below).

The requirement is subject to a preference for Canadian services.

Canada will seek to select the offer which represents overall best value to Canada, established through the combined rating of technical merit and price. The selection of the Offeror will be determined on the basis of a 25% and 75% split between the technical and price components respectively. The offer with the highest combined rating will be considered as the offer representing the best value.

To be considered, Offers must meet all the mandatory evaluation criteria. The rated evaluation criteria focus on Offeror experience with Original Equipment Manufacturers and product functionality in other end-user environments.

The financial offers must contain equipment prices from Published Price Lists (PPLs) and per diem rates for services, and also include a minimum/floor discount rate for the total Standing Offer Period, which will be applied to the PPL pricing each time a Call-up is made. The financial evaluation will be based on the aggregate offer prices for all products and services as detailed in the RFSO.

The evaluation process may result in the issuance of one Standing Offer or none, at the discretion of Canada. If a Standing Offer is issued, it will be for a period of three years from Canada's date of authorization, with the option for Canada to extend for three additional one-year periods.

This procurement is set aside from the international trade agreements under the provision each has for set-asides for small and minority businesses.

Further to Article 1802 of the Agreement on Internal Trade (AIT), the AIT does not apply to this procurement.

Note to Offerors: A CITT decision was issued on October 27, 2011 under File No. PR-2011-040 "The Tribunal does not consider that the trade agreements require that any specific conditions need apply for the Government to invoke such set-asides." This remains a bona fide requirement.

1.3 Security Requirement

There is a security requirement associated with this requirement. The Standing Offeror must hold a valid Designated Organization Screening and personnel will require appropriate RCMP clearance. The full security requirements are noted in the document. For additional information, consult Part 4 – Evaluation Procedures and Basis of Selection, and Part 6A – Resulting Standing Offer Clauses. Offerors should consult the "Security Requirement 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.

1.4 Debriefings

After issuance of a standing offer, Offerors may request a debriefing on the results of the request for standing offer process. Offerors should make the request to the Standing Offer Authority within 15 working days of receipt of the results of the request for standing offer process. At Canada's discretion, the debriefing may be in writing, by telephone or in person.

PART 2 OFFEROR INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

a) All instructions, clauses and conditions identified in the Request for Standing Offer (RFSO) by number, date and title are set out in the Standard Acquisition Clauses and Conditions (SACC) (http://ccua-sacc.tpsgc-pwgsc.gc.ca/pub/acho-eng.jsp) Manual issued by Public Works and Government Services Canada.

b) Offerors who submit an offer agree to be bound by the instructions, clauses and conditions of the RFSO and accept the clauses and conditions of the Standing Offer and resulting contract(s).

c) The 2006 (2011-05-16) Standard Instructions - Request for Standing Offer - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the RFSO.

1) Subsection 5.4 of 2006, Standard Instructions - Request for Standing Offer - Goods or Services - Competitive Requirements, is amended as follows:

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

2) Subsection 12 of 2006, Standard Instructions - Request for Standing Offer - Goods or Services - Competitive Requirements, is amended as follows:

Delete: Subsection 12
Insert:

12 Rejection of Offer

1. Canada may reject an offer where any of the following circumstances is present:

(a)the Offeror is subject to a Vendor Performance Corrective Measure, under the Vendor Performance Corrective Measure Policy, which renders the Offeror ineligible to submit an offer for the requirement;

(b)an employee, or subcontractor included as part of the offer, is subject to a Vendor Performance Corrective Measure, under the Vendor Performance Corrective Measure Policy, which would render that employee or subcontractor ineligible to submit an offer for the requirement, or the portion of the requirement the employee or subcontractor is to perform;

(c)the Offeror is bankrupt or where, for whatever reason, its activities are rendered inoperable for an extended period;

(d)evidence, satisfactory to Canada, of fraud, bribery, fraudulent misrepresentation or failure to comply with any law protecting individuals against any manner of discrimination, has been received with respect to the Offeror, any of its employees or any subcontractor included as part of the offer;

(e)evidence satisfactory to Canada that based on past conduct or behavior, the Offeror, a sub-contractor or a person who is to perform the Work is unsuitable or has conducted himself/herself improperly;

(f)with respect to current or prior transactions with the Government of Canada

(i)Canada has exercised its contractual remedies of suspension or termination for default with respect to a contract with the Offeror, any of its employees or any subcontractor included as part of the offer;

(ii)Canada determines that the Offeror's performance on other contracts, including the efficiency and workmanship as well as the extent to which the Offeror performed the Work in accordance with contractual clauses and conditions, is sufficiently poor to jeopardize the successful completion of the requirement being bid on.

2.Where Canada intends to reject an offer pursuant to a provision of subsection 1. (f), the Standing Offer Authority will so inform the Offeror and provide the Offeror ten (10) days within which to make representations, before making a final decision on the offer rejection.

2.2 Submission of Offers

a) Offers 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 Request for Standing Offer.

b) Due to the nature of the Request for Standing Offer, transmission of offers by facsimile or electronic mail to PWGSC will not be accepted.

2.3 Enquiries

a) All enquiries must be submitted in writing to the Standing Offer Authority identified hereunder in accordance with the periods set out in the table below. Enquiries received after the time specified for each period may not be answered.

Standing Offer Authority: Michelle Beaton
E-mail Address: michelle.beaton@pwgsc.gc.ca
Telephone: (819) 956-5847
Facsimile: (819) 953-3703

b) While Canada has provided the schedule detailing how it will manage the enquiries process, offerors should make enquiries as early as possible and should not make assumptions about the nature of the requirements of this RFSO. Offerors who do not raise issues and questions they may have during the enquiries period do so at their own risk.

Period 1 - Initial Question Period	Period 2 - Supplementary Question Period	Period 3 – Final Supplementary Question Period
Initial question period for offerors is 5 calendar days	The Supplementary question period for offerors raising	The Final supplementary question period raising

from the date the RFSO is posted on MERX.	issue(s) to Canada's initial response(s) only, will conclude at 14:00 EDT on the 2nd calendar day after the responses to the questions submitted from Period 1, Initial Question Period are posted on MERX.	issue(s) only to Canada's supplementary response(s) only, will conclude 14:00 EDT on the 2nd calendar day after the response(s) to the questions submitted during Period 2, the Supplementary Question Period are posted on MERX.
Canada will then respond to the questions from suppliers.		Canada does not intend to modify the RFSO during this period.

c) Offerors should reference as accurately as possible the numbered item of the RFSO to which the enquiry relates. Care should be taken by offerors 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 offerors do so, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all offerors. Enquiries not submitted in a form that can be distributed to all offerors may not be answered by Canada.

2.4 Applicable Laws

a) The Standing Offer and any contract resulting from the Standing Offer must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

b) Offerors may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their offer, 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 offerors.

Note to Offerors: Offerors are requested to indicate the Canadian province or territory they wish to apply to any resulting Standing Offer and Call-ups in their Offer Submission Form, which can be found at Annex E.

PART 3 OFFER PREPARATION INSTRUCTIONS

3.1 Offer Preparation Instructions

a) Canada requests that offerors provide their offer in separately bound sections as follows:

1) Section I: Technical Offer (3 hard copies and 6 soft copies on USB or CD.)
Original Equipment Manufacturer (OEM) technical documentation must be included in soft copies only. If Canada requires hardcopies in part or in whole during the evaluation, Canada will send an email request to the Offeror, at which time the Offeror must provide the requested hardcopy documentation within 5 working days from the date of Canada's request. Unless requested by Canada, hardcopies of the OEM technical documentation are not required and will not be reviewed if submitted.

2) Section II: Financial Offer (2 hard copies and 3 soft copies on USB or CD); and

3) Section III: Certifications (2 hard copies and 3 soft copies on USB or CD).

b) 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, except for hardcopy OEM documentation that was not requested by Canada.

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

d) Canada requests that offerors follow the format instructions described below in the preparation of their offer:

1) use 8.5 x 11 inch (216 mm x 279 mm) paper;

2) use a numbering system that corresponds to that of the Request for Standing Offer;

3) include a title page at the front of each volume of the offer that includes the title, date, RFSO number, Offeror's name and address and contact information of its representative; and

4) include a table of contents.

e) 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, offerors 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 printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

f) The soft copies of the offers must be in a format that is compatible with Microsoft Office Suite 2000 or Adobe Acrobat 8.0.

g) The Offeror may submit more than one offer. If an alternate offer is submitted, it must be a physically separate document, clearly marked as an alternate offer. Each offer will be evaluated independently, without regard to the other offers submitted by the Offeror. As a result, every offer must be complete on its own. Even though material submitted in one offer will not be used to supplement another offer, submitted by the same Offeror, where inconsistencies are noted among multiple offers submitted by the same Offeror, Canada may take those inconsistencies into account in evaluating the multiple offers. If the Offeror submits multiple offers and wishes to withdraw one or more of those offers, Canada may require that the Offeror withdraw either all its offers or none of them.

h) **Section I: Technical Offer**

The Technical Offer consists of the following:

Offer Submission Form and Joint Venture Offer Form (requested at bid closing): Offerors are requested to include the Offer Submission Form with their offers. It provides a common form in which offerors can provide information required for evaluation and Standing Offer award, such as a contact name, the Offeror's Procurement Business Number, the Offeror's status under the Federal Contractors Program for Employment Equity, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Offer Submission Form is incomplete or requires correction, Canada will provide the Offeror with an opportunity to make the required changes. The Joint Venture Offer Form also includes information that Canada will require, but Canada will provide the Offeror with an opportunity to submit the form or make changes to it if it is incomplete or requires correction.

(A) **A completed and signed Form 4 - Certification Requirements for the Set-Aside Program for Aboriginal Business (mandatory at bid closing)**

Substantiation of Technical Compliance Form (mandatory at bid closing): The technical offer must substantiate the compliance of the Offeror and its offered products with the specific articles of Annex A - Requirement identified in the Substantiation of Technical Compliance Form, which is the requested format for providing the substantiation. The Substantiation of Technical Compliance Form is not required to address any parts of this RFSO not referenced in the form. The substantiation must not simply be a repetition of Canada's requirement, but must explain and demonstrate how the Offeror will meet the requirements and carry out the required Work (or, in some cases, how the Offeror's proposed products meet the described requirements). Simply stating that the Offeror or its product complies is not sufficient. Also, where any given subparagraph includes more than one requirement, the substantiation must address all of them. Where Canada determines that the substantiation for any given Product is not complete, the offer will be considered non-responsive and disqualified. The substantiation may refer to additional documentation submitted with the offer – this information can be referenced in the "Reference" column of Substantiation of Technical Compliance Form, where Offerors are requested to indicate where in the offer the reference material can be found, including the title of the document, and the page and paragraph numbers; where a reference is not sufficiently precise, Canada may request that the Offeror direct Canada to the appropriate location in the documentation.

(B) **Completed Experience Tables (mandatory at bid closing):** The Offeror must demonstrate its previous experience by including fully completed versions of Annex B Tables 4, 5, 6, 7, 8, and 9. There are mandatory experience

requirements, as well as rated experience requirements, which are detailed in Annex B - Evaluation and Basis of Selection.

For each of the types of experience detailed in Tables 4 though 9, in addition to completing the tables, the Offeror's offer must include a document describing how the proposed OEM device for that device category was used in the customer's network and the devices with which they were integrated. The document must demonstrate how the work performed for each Customer Reference meets the requirements described in Tables 4-9. Offerors are requested to indicate in the summary table the page number from the technical offer associated with each requirement.

When describing the proposed OEM devices used in the customer deployment, the Offeror must provide make and model numbers of the device used in the customer network with high level diagram and a description indicating where the device integrated with other Device Categories in the customer network.

(C) **Completed Proposed OEM Strategy (requested at bid closing)**: The Offeror is requested to complete table 10, which sets out the OEM whose Products are proposed for each of the 8 Device Categories. If an Offeror does not complete Table 10, Canada will complete the information using the information in the Offeror's pricing tables.

(D) **Completed Financial Tables without prices (mandatory at bid closing):** The Offeror must include a fully completed version of Annex B, Appendix A – Financial Offer with all prices deleted. This will be used along with all other technical offer documentation to assess whether the Products offered meet the mandatory technical requirements.

Offerors should note that Pricing Table 1 – Components for Existing Devices includes a list of components that the RCMP requires for devices that it already owns. Offerors must offer either the exact component listed, or an equivalent product. Products that are equivalent in form, fit, function and quality to the item(s) listed in this table will be considered where the Offeror:

(i) designates the brand name, model and/or part number of the substitute product;
(ii) states that the substitute product is fully interchangeable with the item specified;
(iii) provides complete specifications and descriptive literature for each substitute product;
(iv) provides compliance statements that include technical specifics showing the substitute product meets all mandatory performance criteria that are specified in the request for standing offer; and
(v) clearly identifies those areas in the specifications and descriptive literature that support the substitute product's compliance with any mandatory performance criteria

Products offered as equivalent in form, fit, function and quality will not be considered if:

(vi) the offer fails to provide all the information requested to allow the Standing Offer Authority to fully evaluate the equivalency of each substitute product; or

(vii) the substitute product fails to meet or exceed the mandatory performance criteria specified in the request for standing offer for that item.

i) **Section II: Financial Offer**

The Financial Offer consists of the following:

Financial Offer Tables: Offerors must submit their financial offer in accordance with Annex B, Appendix A – Financial Offer. Offerors are not required to show the Goods and Services Tax or Harmonized Sales Tax. However, if shown, it must be shown separately, if applicable.

Published Price List(s): The Financial Offer must include a separate copy of all available Published Price List(s) (PPLs) which contain products related to any of the 8 Device Categories identified in Annex A - Requirement (whether or not the products were used to complete the tables in Annex B, Appendix A – Financial Offer). The related device category must be indicated for each item on the PPL. Any product unrelated to the 8 device categories must be grayed-out. At its sole discretion, if PWGSC determines that an item does not relate directly to the Device Categories, PWGSC may decide to gray-out the item in question. The PPL(s) must include the prices for the Hardware, the Licensed Software, accessories, spare parts, and all related equipment. The PPL must be provided in a Microsoft Excel format. The prices identified in the PPL(s) must:

be in Canadian dollars;
include shipping and handling charges to any destination in Canada;
include maintenance and warranty requirements as identified in the RFSO;
include configuration services as identified in Annex A – Requirement;
exclude Goods and Services Tax (GST) and Harmonized Sales Tax (HST); and
be effective during the RFSO posting period.

All Costs to be Included: The Financial Offer must include all costs for the requirement described in the RFSO for the entire Standing Offer Period, including any extensions. The identification of all necessary equipment, software, peripherals, cabling and components required to meet the requirements of the RFSO and the associated costs of these items is the sole responsibility of the Offeror.

Blank Prices: Offerors are requested to insert “$0.00” for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Offeror leaves any price blank, or inserts wording in a price cell (such as N/A or no charge), Canada will treat the price as “$0.00” for evaluation purposes and may request that the Offeror confirm that the price is, in fact, $0.00. No offeror will be permitted to add or change a price as part of this confirmation. Any offeror who does not confirm that the price for a blank item is $0.00 will be declared non-responsive.

j) **Section III:Certifications**

Offerors must submit the certifications required under Part 5.

PART 4 EVALUATION PROCEDURES AND BASIS OF SELECTION

Evaluation Procedures and Basis of Selection are as described in Annex B – Evaluation and Basis of Selection.

PART 5 CERTIFICATIONS

Offerors must provide the required certifications to be issued a standing offer. Canada will declare an offer non-responsive if the required certifications are not completed and submitted as requested.

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

Offerors must submit the certifications as provided below:

5.1 Certifications Precedent to Issuance of Standing Offer

The certifications listed below should be completed and submitted with the offer but may be submitted afterwards. If any of these required certifications is not completed and submitted as requested, the Standing Offer Authority will so inform the Offeror and provide the Offeror with a time frame within which to meet the requirement. Failure to comply with the request of the Standing Offer Authority and meet the requirements within that time period will render the offer non-responsive.

a) **Federal Contractors Program for Employment Equity – Certification**

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 the issuance of a standing offer. If the Offeror, or, if the Offeror 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 issuance of a standing offer.

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 offers from ineligible contractors, including an offer from a joint venture that has a member who is an ineligible contractor, will be declared non-responsive.

If the Offeror 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 Offeror 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.

Each Offeror is requested to indicate in its offer whether it is:

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

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

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

subject to FCP, and has a valid certification number (i.e., has not been declared an ineligible contractor by HRSDC).

Further information on the FCP is available on the following HRSDC Website:
http://www.hrsdc.gc.ca/en/gateways/topics/wzp-gxr.shtml

Note to Offerors: *Offerors are requested to use Annex E, Form 1 - Offer Submission Form to provide information about their status under this program. For a joint venture offeror, this information must be provided for each member of the joint venture.*

b) **OEM Certification**

1) Any Offeror that is not the Original Equipment Manufacturer (OEM) for every item of hardware that forms part of its offer is required to submit the OEM's certification regarding the Offeror's authority to provide and maintain the OEM's hardware, which must be signed by the OEM (not the Offeror). No Standing Offer will be issued to an Offeror who is not the OEM of the hardware it offers to supply to Canada, unless the OEM certification has been provided to Canada. Offerors are requested to use the OEM Certification Form included at Annex E, Form 3. Although all the contents of the OEM Certification Form are required, using the form itself to provide this information is not mandatory. For offerors/OEMs who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided.

2) If the hardware offered by the Offeror originates with multiple OEMs, a separate OEM certification is required from each OEM.

3) For the purposes of this request for standing offer, OEM means the manufacturer of the hardware, as evidenced by the name appearing on the hardware, on all accompanying documentation, on mandatory certification reports, and on any support software, which must be the same.

c) **Offeror Certifies that All Equipment and Software is "Off-the-Shelf"**

Any equipment and software offered to meet this requirement must be "off-the-shelf" (unless otherwise stated in this RFSO), meaning that each item of equipment and software is commercially

available and requires no further research or development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment). If any of the equipment or software offered is a fully compatible extension of a field-proven product line, it must have been publicly announced on or before the RFSO closing date. By submitting an offer, the Offeror is certifying that all the equipment and software offered is off-the-shelf.

5.2 Certifications Required with the Offer

Offerors must submit the following duly completed certifications with their offer:

a) **Canadian Content Certification**

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

This procurement is conditionally limited to Canadian services.

Subject to the evaluation procedures contained in the request for standing offer, offerors acknowledge that only offers with a certification that the services offered are Canadian services, as defined in clause A3050T, may be considered.

Failure to provide a completed certification with the Offer at the time of bid closing will result in the services offered being treated as non-Canadian services.

Each Offeror wishing to benefit from the preference for Canadian services must certify using Annex E, Form 1 attached – Offer Submission Form whether or not the services offered are Canadian services as defined in paragraph 4 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*.

b) **Set-aside for Aboriginal Business**

1) This procurement is set aside under the federal government's Procurement Strategy for Aboriginal Business, as detailed in Annex 9.4 - Requirements for the Set-aside Program for Aboriginal Business, of the *Supply Manual*. Offerors must complete and sign the certification attached as Annex E, Form 4.

2) Certification Requirements for the Set-aside Program for Aboriginal Business.

3) By signing the certification, the Offeror warrants that it is an Aboriginal business as defined in the Set-aside Program for Aboriginal Business.

4) SACC Manual clause M3030T (2011-05-16) applies.

PART 6 – SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirement

a) At the Request for Standing Offers closing date, the following conditions must be met:

1) the Offeror must hold a valid organization security clearance as indicated in Part 7A - Standing Offer.

b) Canada will not delay the issuance of any standing offer to allow offerors to obtain the required clearance.

c) Security clearances for individual personnel who do not already hold the requisite clearance can be coordinated following award.

d) For additional information on security requirements, 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.

6.2 Financial Capability

a) SACC Manual clause M9033T (2011-05-16), Financial Capability, applies to this RFSO; except that subsection 3 is deleted and replaced with the following: “If the Offeror is a subsidiary of another company, then any financial information required by the Standing Offer Authority in 1(a) to (f) must be provided by each level of parent company, up to and including the ultimate parent company. The financial information of a parent company does not satisfy the requirement for the provision of the financial information of the Offeror; however, if the Offeror is a subsidiary of a company and, in the normal course of business, the required financial information is not generated separately for the subsidiary, the financial information of the parent company must be provided. If Canada determines that the Offeror is not financially capable but the parent company is, or if Canada is unable to perform a separate assessment of the Offeror’s financial capability because its financial information has been combined with its parent’s, Canada may, in its sole discretion, award the Standing Offer to the Offeror on the condition that the parent company grant a performance guarantee to Canada.”

b) In the case of a joint venture offer, each member of the joint venture must meet the financial capability requirements.

PART 7 A - STANDING OFFER

7.1 Requirement

a) The Offeror offers to supply to the Client the goods and services described in the Standing Offer, including the Requirement, in accordance with, and at the prices set out in, the Standing Offer. This includes:

1) Supplying the purchased Hardware;

2) Providing the Hardware Documentation;

3) Providing maintenance and support services for the Hardware during the Hardware Maintenance Period;

4) Granting the license to use the Licensed Software described in the Standing Offer;

5) Providing the Software Documentation; and

6) Providing professional services.

b) Defined Terms: Words and expressions defined in the General Conditions or Supplemental General Conditions and used in the Standing Offer have the meanings given to them in the General Conditions or Supplemental General Conditions.

7.2 Security Requirement for Canadian Supplier

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

b) The Standing Offeror personnel requiring access to PROTECTED information, assets or sensitive work site(s) must EACH hold an appropriate RCMP clearance, granted or approved by RCMP. (NOTE: All security screenings undertaken by the RCMP on behalf of PWGSC for this Standing Offer will also be duplicated to CISD.)

In addition, Standing Offeror personnel must submit to a local verification of identity / information by RCMP, prior to admittance to the facility / site. The RCMP reserves the right to deny access to any facility / site or part thereof to any Standing Offeror personnel, at any time.

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

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

e) The Standing Offeror must comply with the provisions of the:

Security Requirements Check List and security guide (if applicable), attached at Annex D;

Industrial Security Manual (Latest Edition).

7.3 Standard Clauses and Conditions

a) All clauses and conditions identified in the Standing Offer and resulting contract(s) 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.

b) General Conditions

2005 (2011-05-16) General Conditions – Standing Offers – Goods or Services, apply to and form part of the Standing Offer.

7.4 Term of Standing Offer

a) **Period of Standing Offer**

1) The period for making Call-ups against the Standing Offer is for 3 years from the date the Standing Offer is issued.

2) The Contract Period of individual Call-ups may extend beyond the Standing Offer Period. That is, a Call-up may be placed up until the last day of the Standing Offer Period; the resulting contract will be in force until all the work has been completed, including warranty services.

b) **Extension of Standing Offer**

1) The Offeror offers to extend its offer for 3 additional one-year periods, under the same conditions and at the rates or prices specified in the Standing Offer, or at the rates or prices calculated in accordance with the formula specified in the Standing Offer.

2) The Offeror will be advised of the decision to authorize the use of the Standing Offer for an extended period by the Standing Offer Authority 30 days before the expiry date of the Standing Offer. A revision to the Standing Offer will be issued by the Standing Offer Authority.

7.5 Authorities

a) **Standing Offer Authority**

The Standing Offer Authority for the Standing Offer is the contracting officer named on page one of this Standing Offer.

The Standing Offer Authority is responsible for the establishment of the Standing Offer, its administration and its revision, if applicable. Upon the making of a Call-up, as Contracting Authority, he/she is responsible for any contractual issues relating to individual Call-ups made against the Standing Offer.

b) **Technical Authority**

The Technical Authority for the Standing Offer is:

Name: _____
Title: _____
Organization: _____
Address: _____

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

1) The Technical Authority is the representative of the department or agency for whom the Work will be carried out pursuant to a Call-up under the Standing Offer and is responsible for all the technical content of the Work under the resulting contract. Any proposed changes to the scope of the requirement are to be discussed with the Technical Authority, but any resulting change can only be confirmed by a revision issued by the Standing Offer Authority.

2) The Technical Authority will be responsible for Standing Offer management for the RCMP as well as escalation of any issues such as service, ordering and billing.

3) The Technical Authority will provide the Offeror with a list of authorized RCMP Support Coordinators and Call-up Coordinators.

c) **Support Coordinator**

Support Coordinators have the authority to report warranty incidents, open incident tickets and obtain status updates.

d) **Call-up Coordinator**

Call-up Coordinators are the RCMP points of contact for the coordination and tracking of deliveries, and technical questions regarding to Call-ups. They do not have the authority to issue Call-ups or Call-up amendments. All Call-ups placed by the RCMP will be issued by the RCMP Procurement Division.

e) **Offeror Contacts**

Account Manager
Name:_____
Email: _____
Telephone Number:_____

The Account Manager will be the first point of escalation and must liaise with the RCMP for management issues regarding the Standing Offer and resulting contracts.

Ordering Representative
Name:_____
Email: _____
Telephone Number:_____

The Ordering Representative will be the single point of contact for Call-ups. The Ordering Representative will liaise with the RCMP Call-up Coordinator and the RCMP Procurement Directorate regarding Call-up coordination. All Call-ups will be sent directly to the Ordering Representative by the RCMP Procurement Directorate.

Billing Representative
Name:_____
Email: _____
Telephone Number:_____

The Billing Representative will be the single point of contact for any billing questions or issues.

Support Desk
Email: _____
Toll-Free Telephone Number: _____
Web Site: _____

f) **Identified Users**

In additional to the Standing Offer Authority, the Identified User authorized to make Call-ups against the Standing Offer is the Royal Canadian Mounted Police (RCMP).

Reorganization of Identified User: The Offeror's obligation to perform the Work will not be affected by (and no additional fees will be payable as a result of) the renaming, reorganization, reconfiguration, or restructuring of the Identified User. The reorganization, reconfiguration and restructuring of the Identified User includes the privatization of the Identified User, its merger with another entity, or its dissolution, where that dissolution is followed by the creation of another entity or entities with mandates similar to the original Identified User.

g) **No Contracting Outside Authorities**

The Offeror agrees not to accept Call-ups to perform work in excess of or outside the scope of this Standing Offer without specific written authorization from the PWGSC Standing Offer Authority. The Offeror acknowledges that the Identified User is without authority to vary or amend the terms or the scope of this Standing Offer.

7.6 Joint Venture Offeror

a) The Offeror confirms that the name of the joint venture is _____ and that it is comprised of the following members: [*list all the joint venture members named in the Offeror's original offer*].

b) With respect to the relationship among the members of the joint venture Offeror, each member agrees, represents and warrants (as applicable) that:

1) _____ has been appointed as the "representative member" of the joint venture Offeror and has fully authority to act as agent for each member regarding all matters relating to the Standing Offer and any resulting Call-ups;

2) by giving notice to the representative member, Canada will be considered to have given notice to all the members of the joint venture Offeror; and

3) all payments made by Canada to the representative member will act as a release by all the members.

c) All the members agree that Canada may set aside authority to use the Standing Offer or terminate any Call-up in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.

d) All the members are jointly and severally or solidarily liable for the performance of the entire Standing Offer and any resulting Call-ups.

e) The Offeror acknowledges that any change in the membership of the joint venture (i.e., a change in the number of members or the substitution of another legal entity for an existing member) constitutes an assignment and is subject to the assignment provisions of the General Conditions.

f) The Offeror acknowledges that all security and controlled goods requirements in the Standing Offer, if any, apply to each member of the joint venture Offeror.

Note to offerors: This Article will be deleted if the Offeror issued a Standing Offer is not a joint venture. If the Offeror is a joint venture, this clause will be completed with information provided in its offer (see Annex E, Form 5).

7.7 Call-up Procedures

a) The Offeror agrees only to accept individual Call-ups made by the RCMP National Headquarters or PWGSC Acquisitions Branch pursuant to this Standing Offer that do no exceed the applicable Call-up Limitations. The Offeror acknowledges that any Call-up made by an Identified User exceeding the applicable Call-up Limitation is not permitted under this Standing Offer without authority.

b) PWGSC is the Contracting Authority for all Call-ups.

c) Equipment

The RCMP Headquarters or the PWGSC Standing Offer Authority will send a 942 Call-up Against a Standing Offer to the Offeror either by fax, email or web portal.

The 942 will include at a minimum:

Standing Offer Number;

Call-up number;

The product ID number;

The product Name;

The product model;

The OEM Name;

The required delivery date;

The delivery location;

Special site delivery or installation preparation requirements identified by the Call-up Coordinator;

The Call-up Coordinator name; and

The invoicing address.

The Offeror must acknowledge receipt of the Call-up within 2 business days (unless otherwise specified), either by email or web-portal (unless otherwise specified).

The acknowledgement must include at a minimum:

The Call-up number;

Best delivery date (which must be no later than the Call-up Delivery Date).

If the required number of Products exceeds or threatens to exceed the Contractor's ability to supply by the Delivery Date, the Contractor must

immediately advise the Call-up Coordinator. The Call-up Coordinator will have the option of terminating the Call-up for default, extending the delivery date, or of accepting late delivery;

Special site delivery or installation preparation requirements identified by the Offeror; and

d) Services

1) If a requirement for Professional Services is identified, the RCMP will send a description of the requirement to the Offeror to confirm the estimated level of effort and resource requirement.

2) Within 7 business days of receiving the requirement description, the Offeror shall provide the RCMP with the following information:

(A) The resource name and resume demonstrating compliance with the requirements identified in Annex A – Requirement;

(B) Confirmation that the resource will be available on the required dates and if not an explanation and alternative dates;

(C) Information required for the RCMP to commence the Personnel Security Clearance process.

3) Following receipt of the information required in section 1) above, the RCMP Headquarters or the PWGSC Standing Offer Authority may send a 942 Call-up Against a Standing Offer to the Offeror either by fax, email or web portal. No Call-up will be issued until the resource has obtained the required personnel security clearance.

(A) If the resource already has the required security clearance, the RCMP will have 30 days to consider the Call-up.

(B) If the resource does not have the required personnel security clearance, the RCMP will have a minimum of 6 months to process the security clearance and consider the Call-up.

4) The 942 will include:
(A) Standing Offer Number;
(B) Call-up number;
(C) The Service Category;
(D) The number of days and/or hours required;
(E) The work required;
(F) The date the work must start;
(G) The location;
(H) Security clearance level required prior to commencement of the work;
(I) The Call-up Coordinator name; and
(J) The invoicing address.

5) The Offeror must acknowledge receipt of the Call-up within 2 business days (unless otherwise specified), either by email or web-portal (unless otherwise specified).

e) The Offeror must provide a status update for each outstanding Call-up when requested by the Standing Offer Authority, the Technical Authority, or a Call-up Coordinator.

f) Priority Call-ups are defined as Call-ups that are required to address priority needs. Priority Call-ups will be identified as such by the Call-up Coordinator. The Offeror offers to make exceptional efforts to deliver the order on a priority Call-up on or before the date identified on the Call-up.

7.8 Call-up Instrument

The Work will be authorized or confirmed by the Identified User using form *942 – Call-up Against a Standing Offer* or electronic document.

Each Call-up results in a separate contract between Canada and the Offeror.

The Offeror acknowledges that no costs incurred before the receipt of a signed Call-up can be charged to this Standing Offer or any Call-ups made against it.

The Offeror acknowledges and agrees that the terms and conditions set out in the Resulting Contract Clauses that form part of this Standing Offer apply to every Call-up made under this Standing Offer.

For any Call-ups cancelled prior to delivery at the request of PWGSC or the RCMP, the Offeror must cease processing on the requested date and no charges or fees will be incurred.

7.9 Limitation of Call-ups

Individual Call-ups made directly by the RCMP must not exceed $400,000.00 (including GST/HST and any applicable discounts and disposal surcharges).

Any Call-ups in excess of $400,000.00 (including GST/HST and any applicable discounts and disposal surcharges) must be issued directly by PWGSC.

7.10 Priority of Documents

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

a) the call up against the Standing Offer, including any annexes;

b) the articles of the Standing Offer;

c) the general conditions 2005 (2011-05-16), General Conditions - Standing Offers - Goods or Services;

d) the supplemental general conditions – Hardware Purchase, Lease and Maintenance 4001 (2010-08-16) ;

e) the supplemental general conditions – Licensed Software 4003 (2010-08-16) ;

f) the general conditions 2030 (2011-05-16);

g) Annex A - Requirement;

h) Annex B - Evaluation and Basis of Selection;

i) Annex C - Report Formats;

j) Annex D – SRCL; and

k) The Offeror's offer _____ (*insert date of offer*), _____ (*if the offer was clarified or amended, insert at the time of issuance of the offer*: "as clarified on _____" ***or*** "as amended _____. (*insert date(s) of clarification(s) or amendment(s) if applicable*).

7.11 Certifications made with the Offer

a) **Compliance**

Compliance with the Certifications provided by the Offeror is a condition of authorization of the Standing Offer and subject to verification by Canada during the entire period of the Standing Offer and of any resulting contract that would continue beyond the period of the Standing Offer. In the event that the Offeror does not comply with any certification or that it is determined that any certification made by the Offeror in its offer is untrue, whether made knowingly or unknowingly, the Standing Offer Authority has the right to terminate any resulting contract for default and set aside the Standing Offer.

b) **SACC Manual Clauses**

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

SACC Manual clause M3060C (2008-05-12), Canadian Content Certification

c) **Aboriginal Business Certification**

1) The Offeror warrants that its certification of compliance is accurate and complete and in accordance with the "Requirements for the Set-aside Program for Aboriginal Business" detailed in Annex 9.4 *of the Supply Manual*.

2) The Offeror must keep proper records and documentation relating to the accuracy of the certification provided to Canada. The Offeror must obtain the written consent of the Standing Offer Authority before disposing of any such records or documentation before the expiration of six (6) years after final payment under the Call-ups made against this Standing Offer, or until settlement of all outstanding claims and disputes under the Standing Offer, whichever is later. All such records and documentation must at all times during the retention period be open to audit by the representatives of Canada, who may make copies and take extracts. The Offeror must provide all reasonably required facilities for any audits.

3) Nothing in this clause must be interpreted as limiting the rights and remedies which Canada may otherwise have pursuant to the Standing Offer.

7.12 Representations and Warranties

The Offeror represents and warrants that, throughout the Standing Offer Period:

a) All Product will be manufactured at a facility registered under ISO 9001:2008 by an accredited registrar under the ISO 9001:2008, whether that registration is held by the Offeror or the Original Equipment Manufacturer of the System.

b) all electrical equipment offered under this Standing Offer is certified or approved for use in accordance with the Canadian Electrical Code, Part 1, by a certification organization accredited by the Standards Council of Canada (SCC) and bears the certification logo that is applicable to

the accredited agency. NOTE: Offerors may obtain further information by contacting the SCC at 613-238-3222.

c) in the case of each Product offered that includes a digital apparatus, an accredited agency has certified that it does not exceed the FCC Class A limits for radio noise emissions set out in the Radio Interference Regulations and the Products must bear the certification logo of the appropriate accredited agency.

Compliance with these representations and warranties is a condition of authorization of the Standing Offer and subject to verification by Canada during the entire Standing Offer Period and during any resulting Call-up. If the Offeror does not comply with any of these representations or warranties or it is determined that any representation or warranty made by the Offeror is untrue, whether made knowingly or unknowingly, the Standing Offer Authority has the right to terminate any resulting Call-up(s) for default and set aside the Standing Offer.

7.13 Applicable Laws

The Standing Offer and any contract resulting from the Standing Offer must be interpreted and governed, and the relations between the parties determined, by the laws in force in _____.

7.14 Standing Offer Reporting

a) The Offeror must compile and maintain records on its provision of goods, services or both to the federal government under contracts resulting from the Standing Offer. This data must include all purchases. The data must be aggregated and submitted on a monthly basis to the PWGSC Standing Offer Authority and the RCMP Technical Authority in the format identified in Annex C – Report Formats. The format may be modified throughout the Standing Offer Period if requested by the PWGSC Standing Offer Authority. The required reports are as follows:

1) **Report on Usage**

A monthly report on usage, which must be provided no later than ten working days after the end of each month. The Usage Report is a detailed report that will be produced using information from all invoices submitted the previous month. It will be used to monitor expenditures and usage against the Standing Offer.

2) **Report on Late Deliveries**

A monthly report on late deliveries, which must be provided no later than ten working days after the end of each month. The Late Deliveries Report will be produced using all deliveries that had delays and actually took place the previous month. It will be used to monitor vendor performance under the Standing Offer as well as track related credits.

3) **Report on Warranty Incidents**

A monthly report on warranty incidents, which must be provided no later than ten working days after the end of each month. The Warranty Incident Report will be produced using all warranty calls placed the previous month. It will be used to monitor product and vendor performance under the Standing Offer.

b) All data fields of the report must be completed as requested. If some data is not available, the reason must be indicated in the report. If no goods or services are provided during a given period, the Offeror must still provide a “NIL” report.

c) Failure to provide fully completed reports in accordance with the above requirements may result in the setting aside of the Standing Offer and the application of a vendor performance corrective measure.

d) If requested by the PWGSC Standing Offer Authority, the Offeror must provide details on its processes for compiling the data required to fulfill its reporting obligations.

e) The Offeror must retain all the data and the filed reports for 6 years from the date of the last Call-up made under this Standing Offer. Should Canada, at its sole discretion require access to the information, Canada will submit its request in writing to the Standing Offeror. The Standing Offeror must deliver at no additional cost to Canada the documentation within 5 working days from the date Canada's request is submitted..

7.15 Updated Information about Products

During the Standing Offer Period for each Device Category, the Offeror is requested to provide regular updates to the Technical Authority regarding upgrades to the capabilities of the Products, such as when additional operating systems are supported or new drivers become available.

7.16 Price Lists

Following issuance of a Standing Offer, it is the Offeror's responsibility to supply and update price lists and/or catalogues as Canada may require. The Offeror must provide one (1) copy of its catalogue and price list and updates to each of the RCMP and the Standing Offer Authority.

7.17 Price Revisions

a) The Published Price List submitted with the Offer will serve as ceiling prices for the Standing Offer. The ceiling prices are subject to downward revision in accordance with the following paragraphs:

1) During the Standing Offer Period, if a price decrease is published or publicly announced, the Offeror will provide the benefit of such decreases to Canada.

2) During the Standing Offer Period, where in accordance with (1) above the Offeror is required to reduce the prices listed in its Standing Offer, it must immediately send a notification to the Standing Offer Authority to reflect the price reduction as well as a revised electronic copy of the full PPL in a Microsoft Excel format.

3) The revised pricing will come into effect on the date the revised price is announced or published.

4) The Offeror acknowledges and agrees that Canada may accept or reject any proposed price revisions. If, following review by the Standing Offer Authority, the revised rate is rejected, any affected Call-ups will be amended or accounts adjusted accordingly.

b) The floor discount rates identified in the Standing Offer represent the minimum discount to be applied to the PPL pricing for the Standing Offer Period. From time to time, the Offeror can increase the discount rate for either the complete Standing Offer or for a specific Call-up. Any revisions to a floor discount rate must result in a greater discount than the floor discount rate identified in the Standing Offer, and reductions to a discount rate will not be accepted.

c) The Offeror must notify the Standing Offer Authority immediately if a discount rate is revised for the remainder of the Standing Offer Period and the Standing Offer Authority will issue a revision to the Standing Offer.

d) Consumer Price Index (CPI)

Canada will allow for the professional services rates as set out in the Basis of Payment to be adjusted based on the Canadian Consumer Price Index (CPI) at the end of each year commencing on the first extension year, not to exceed a CPI increase of more than 10%.

1) Source: The Consumer Price Index publication, Table 5 - The Consumer Price Index for Canada, all-items, not seasonally adjusted, historical data published by Statistics Canada, Percentage change from the corresponding month of the previous year will be used to determine the CPI rates and is accessible at: http://www5.statcan.gc.ca/subject-sujet/result-esultat.action?pid=3956&id=2178&lang=eng&type=OLC&pageNum=1&more=0

2) Application: Fixed profession services rates have been provided for the duration of the Standing Offer (initial 3 years plus 3 extension years). Commencing the 4th year of the Standing Offer (1st extension year), the professional services rates may be increased yearly, based on the average CPI increase from the previous year. All price changes in this area will be confirmed in writing by way of a formal revision issued to the Standing Offeror as solely issued by the designated Standing Offer Authority.

3) Calculation of the CPI Rate:

(A) Standing Offer Year 4 (1st year extension):
Ceiling price for the professional services category = Standing Offer Year 3 ceiling price for the pricing element X ((100 + average Consumer Price Index Percentage Change Factor, rounded to the 4th decimal, from 16 months prior to SO year 4 start date up to and including 3 months prior to SO year 4 start date)/100)

(B) Standing Offer Year 5 (2nd year extension):
Ceiling price for the professional services category = Standing Offer Year 4 ceiling price for the pricing element X ((100 + average Consumer Price Index Percentage Change Factor, rounded to the 4th decimal, from 16 months prior to SO year 5 start date up to and including 3 months prior to SO year 5 start date)/100)

(C) Standing Offer Year 6 (3rd year extension):
Ceiling price for the professional services category = Standing Offer Year 5 ceiling price for the pricing element X ((100 + average Consumer Price Index Percentage Change Factor, rounded to the 4th decimal, from 16 months prior to SO year 6 start date up to and including 3 months prior to SO year 6 start date)/100)

4) Example:

Whereby the fixed per diem rate in year 3 of the Standing Offer is $800, and whereby the Standing Offer was awarded in December 2007 and therefore the first extensions year begins in December 2010. Using the August 2011 CPI Table 5 (http://www.statcan.gc.ca/pub/62-001-x/2011008/t040-eng.htm), the monthly CPI rates that would be used for purposes of calculating the average CPI increasewould be August 2009 to September 2010 inclusively.

The formula would be as follows: Standing Offer Year 4 rate = $800 x (100 + 0.9667) / 100
Standing Offer Year 4 rate = $807.73

7.18 Extension of Existing Product Line - New Products

a) During the Standing Offer Period, if technological improvements have been made to the products available for purchase under the Standing Offer, the Offeror may propose new products that are an extension of an existing product line or the “next generation” of an existing product line that meet or exceed the specification(s) of existing products under the Standing Offer, if the price for the new product does not exceed:

the ceiling price for the product originally offered in the Standing Offer; plus 5%;

the current published list price of the substitute product, minus any applicable Government discount; or

the price at which the substitute product is generally available for purchase,

whichever is the lowest.

b) Whether or not to accept or reject a proposed new product is entirely within the discretion of Canada. If Canada does not accept a proposed new product that is proposed to replace an existing product, the Offeror must continue to deliver the original product. If accepted, the addition of the new product will be documented for the administrative purposes of Canada by a revision to the Standing Offer, by adding the new product to the Standing Offer.

c) No new products will be included in the Standing Offer until six months after the Standing Offer is issued.

7.19 Call-up-Specific Product Substitutions of Hardware

a) If the Offeror is unable to provide a specific item of Hardware ordered under the Standing Offer and wishes to offer a substitute in respect of that order, the Offeror must submit a request to the Standing Offer Authority together with a certificate that the proposed substitute item meets or exceeds the specification(s) of the existing product being substituted and the price for the substitute product must not exceed:

the ceiling price for the product originally offered in the Standing Offer;

the current published list price of the substitute product, minus any applicable Government discount; or

the price at which the substitute product is generally available for purchase,

whichever is the lowest.

b) The substitute item must not be shipped until formally authorized by the Standing Offer Authority after the Technical Authority determines the substitution is acceptable. Whether or not to accept or reject a proposed substitution is entirely within the discretion of Canada.

c) The ability to propose a substitute for a specific Call-up does not relieve the Offeror of its obligation to make delivery within the period set out in the Call-up, regardless of whether or when the proposed substitution is approved.

7.20 Product Substitutions & Alternatives

a) The Offeror may propose a substitution or alternative for an existing product listed in the Standing Offer, provided the proposed substitute or alternative meets or exceeds the

specification(s) of the existing product and the price for the substitute or alternative product does not exceed:

the firm price (or ceiling price, if applicable) for the product originally offered in the Standing Offer;

the current published list price of the substitute product, minus any applicable Government discount; or

the price at which the substitute product is generally available for purchase,

whichever is the lowest.

b) The proposed substitution/alternative may be subject to benchmark evaluation and the Offeror must pay for all costs associated with the benchmark evaluation (e.g., transportation, benchmark fee, etc.).

c) Substitute or alternative items must not be shipped until formally authorized by the Standing Offer Authority after the Technical Authority determines the substitution or alternative is acceptable. Whether or not to accept or reject a proposed substitution or alternative is entirely within the discretion of Canada. If Canada does not accept a proposed substitution or alternative, the Offeror must continue to deliver the original product. If accepted, the substitution will be documented for the administrative purposes of Canada by a revision to the Standing Offer, by removing the existing product and including the substitution instead. If accepted, the addition of any alternative product will be documented for the administrative purposes of Canada by a revision to the Standing Offer, by adding the alternative as a product under the Standing Offer. Once an alternative product has been included in the Standing Offer, Canada may purchase either product, at its option.

d) The ability to propose a substitution or alternative for any given product does not relieve the Offeror of its obligation to make delivery of the existing product when ordered within the period set out in the Standing Offer, regardless of whether or when the proposed substitution is approved.

e) No substitutions or alternatives will be included in the Standing Offer until six months after the Standing Offer is issued.

f) Discontinued Products: The Offeror must immediately notify the PWGSC Standing Offer Authority and the RCMP Technical Authority if any Product listed in this Standing Offer is discontinued or is otherwise unavailable (e.g., End of Life). The Offeror must propose a substitution, in accordance with this article, within 60 days of providing such notice. Should Canada reject the proposed substitution, Canada may apply article 7.24 - Withdrawal or Suspension of Authority to Use Standing Offer.

7.21 Equivalency of Equipment

a) The Offeror guarantees that the Products to be delivered under the Standing Offer that are listed in Pricing Table 1 are:

equivalent in form, fit, function and quality to the items listed in that table in the RFSO that resulted in the Standing Offer; and

fully compatible, interchangeable and interoperable with the existing equipment and software owned by Canada, to the extent that equipment and software are described in the Standing Offer.

b) The Offeror also guarantees that any warranties with third parties concerning the existing equipment owned by Canada will not be adversely affected by Canada's use of the Products delivered under the Standing Offer (for example, by interconnecting the Products with the existing equipment) or by any other services provided by the Offeror under the Standing Offer. If Canada determines in its sole discretion that any such warranty has been adversely affected, at Canada's sole option, the Offeror must:

pay to Canada the amount that Canada must pay to the original supplier (or an authorized reseller of that supplier) to re-certify Canada's existing equipment for warranty purposes and any other amounts paid by Canada to a third party in order to restore the equipment to full warranty status;

perform all warranty work on Canada's existing equipment in place of the original supplier; or

pay to Canada the amount that Canada must pay to the original supplier (or an authorized reseller of that supplier) to perform maintenance work on the equipment that otherwise would have been covered by the warranty.

c) The Offeror agrees that, during the Standing Offer Period, if Canada determines that any of the equipment is not equivalent in form, fit, function and quality to the existing equipment owned by Canada or is not fully compatible, interchangeable and interoperable with the existing equipment owned by Canada as described in the Standing Offer, the Offeror must immediately and entirely at its own expense take all steps necessary to ensure that the equipment satisfies these requirements (for example, by implementing any additional software or firmware), failing which Canada will have the immediate right to withdraw authority to use the Standing Offer for default.

7.22 Services – General

a) The Offeror offers to provide, as and when requested by Canada using a Call-up, professional services relating to the scope of the Standing offer.

b) In order to be able to provide these professional services on request, the Offeror must have available a team of experts, including individuals in all of the categories described in Annex A - Requirement

7.23 Internet Site for Standing Offer Products and Prices

a) The Offeror must make available to the RCMP, via secure web-based access, online access to all current OEM web sites to provide equipment configuration assistance. The site must provide the following:

1) Access to all current OEM product documentation;

2) Access to any OEM web site tools to provide equipment configuration assistance;

3) A list of all products available on the SO along with the published list price. The published; list price must be updated within the same business day of any price change; and

4) Web access to warranty and support services.

b) If there is any discrepancy between the Offeror’s website and the SO, the SO will prevail.

c) For the website, the Offeror must ensure that Canada has access to a minimum of 100 accounts. The Offeror must ensure that the website is active and meets the requirements of the Standing Offer within 30 days of Standing Offer award.

d) The website is: _____ (to be completed at issuance of the Standing Offer).

7.24 Withdrawal or Suspension of Authority to Use Standing Offer

a) Canada may, at any time, for operational reasons, withdraw authority from the RCMP to use the Standing Offer.

b) Canada may also, at any time, withdraw authority to use this Standing Offer if the Offeror breaches the terms of this Standing Offer or any Call-up, including:

1) Delivery of Products not listed in this Standing Offer, except to the extent expressly authorized by this Standing Offer;

2) Delivery of any Product that provides a lower level of performance than or does not meet the minimum specifications and requirements described in the Technical Specifications set out in Annex A - Requirement or the technical specifications of the Product approved for that Offeror, whichever is higher;

3) Substitution of any Product without prior written authorization from the Standing Offer Authority;

4) Late deliveries;

5) Poor warranty/maintenance service;

6) Distribution or publication of advertising, including information included in supplier websites, that has not been approved by the Standing Offer Authority and/or that might be interpreted as suggesting that unauthorized items are available under the Standing Offer or providing any information that conflicts with any aspect of the terms and conditions, pricing, or availability of Products currently available under this Standing Offer;

7) Failure to submit complete and accurate reports within the required time frames;

8) Breach of any of the specific terms and conditions detailed in this Standing Offer or any Call-up (e.g. failure to meet the hotline support requirements, failure to respect the Call-up limitations, etc.); and

9) Refusing a Call-up at any time or for any reason from the RCMP or the Standing Offer Authority where the Call-up is for a Product or professional services currently listed and approved under this Standing Offer.

c) If an individual Call-up made under this Standing offer is terminated, for default or otherwise, that termination will not automatically result in withdrawal of authority to use the Standing Offer. The Offeror acknowledges, however, that a default under any contract made under this Standing Offer may result in the suspension or withdrawal of authority to use this Standing Offer.

7.25 Expansion of Offerors Following Withdrawal of Authority to Use Standing Offer or Voluntary Withdrawal of Offeror

a) After permanently withdrawing authority to use the Offeror's Standing Offer, or if the Offeror voluntarily withdraws its Standing Offer, Canada may, in its sole discretion, do one or more of the following:

1) call for new Offers through the Government Electronic Tendering Service; or

2) if a withdrawal is effective within one year of issuing the Standing Offer, contact the Offeror (if any) whose offer complied with all the requirements of the Request for Standing Offer that resulted in the issuance of this Standing Offer and was “next in line” under the evaluation methodology, but who was not issued a Standing Offer.

PART 7 B - RESULTING CONTRACT CLAUSES

Note to offerors: The clauses contained in these Resulting Contract Clauses are intended to form the basis of any Call-up resulting from any Standing Offer issued as a result of this RFSO. Except where specifically set out in these Resulting Call-up clauses, acceptance by Offerors of all the clauses is a mandatory requirement of this RFSO. No modification or other terms and conditions included in the Offeror’s Offer will be applicable to any Standing Offer issued or the contracts made under any resulting Standing Offer, despite the fact that the Offeror’s Offer may become part of the Standing Offer.

Offerors submitting an offer containing statements implying that the offer is conditional on modification of these clauses or containing terms and conditions that purport to supersede these clauses will be considered non-compliant.

Offerors with concerns regarding the provisions of these Resulting Contract Clauses should raise such concerns in accordance with the Enquiries provision of this RFSO. If additional legal issues are raised by an offer, Canada reserves the right to address such issues in any Standing Offer issued as a result of this RFSO (including the Resulting Call-up clauses incorporated in that Standing Offer). If the additional provisions are unacceptable to the Offeror, the Offeror may withdraw its offer.

The following clauses and conditions apply to and form part of any contract resulting from a Call-up against the Standing Offer.

7.26 Requirement

a) The Contractor must provide the goods and services detailed in the Call-up against the Standing Offer in accordance with the term of this Contract and the Standing Offer.

b) In this RFSO, the term “Products” is used to refer to any one or more of:

1) The components for existing devices listed in Pricing Table 1; and

2) The various items available in each Device Category (which includes Hardware, Licensed Software and ancillary items), as listed in Pricing Table 2.

c) With respect to any professional services called up:

1) Once a requirement for a resource is identified by Canada and a Call-up is issued, the Offeror must make the resource available to Canada within 15 working days. This obligation applies despite any changes that Canada may have made to any hardware, software or any other aspect of the Client’s operating environment.

2) If there must be a change in a resource performing work under the Call-up (which must in any case comply with the requirements in the section of the General Conditions entitled “Replacement of Personnel”), the Offeror must make the replacement available for work within 10 working days of the departure of the existing resource (or, if Canada has requested the replacement, within 15 working days of Canada’s notice of the requirement for a replacement).

3) All resources provided by the Offeror must meet the qualifications described in the Standing Offer (including those relating to previous experience, professional designation, education, and language proficiency) and must be competent to provide the required services by any delivery dates described in the Call-up.

4) If the Offeror fails to meet any of its obligations under this sub-article (b), or fails to deliver any item or complete any task described in the Call-up on time, in addition to any other rights or remedies available to Canada under the Standing Offer or the law, Canada may notify the Offeror of the deficiency, in which case the Offeror must submit a written plan to the Technical Authority within 10 working days detailing the actions that the Offeror will undertake to remedy the deficiency. The Offeror must prepare and implement the plan at its own expense.

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

a) **General Conditions**

2030 (2011-05-16), General Conditions - Higher Complexity - Goods, apply to and form part of the Contract.

b) **Supplemental General Conditions**

1) 4001 (2010-08-16), Supplemental General Conditions - Hardware Purchase, Lease and Maintenance; and

2) 4003 (2010-08-16), Supplemental General Conditions - Licensed Software

apply to and form part of the Contract.

7.28 Personnel Security

a) The Contractor‘s Professional Services candidates must obtain Personal Security Clearance in accordance with rules of the Departmental Security Branch of the RCMP. The Contractor must ensure that any resources, any sub-Contractors or any other personnel performing work on its behalf hold the appropriate RCMP security clearances.

b) An RCMP Reliability Status (RRS) (this is not a CISD clearance and is an RCMP only clearance) is the minimum requirement for all Professional Services resources categories for Contractor personnel employed under contract with the RCMP for more than occasional access and who will have regular unescorted access to RCMP premises but not to classified/designated operational information or assets. Additional security clearances more appropriate to the level of activity, information and asset sensitivity to which Contractors need access will be required

depending on the sensitivity of the activity. Additional security clearances may be required by the RCMP for all individuals whose duties or activities require access to classified information or other assets the RCMP deems sensitive.

Note: For the purposes of this clause, “Contractor personnel employed under contract with the RCMP” means the Contractor’s resource who is working with the RCMP following a Call-up against the Standing Offer.

7.29 Period of Contract

The “Contract Period” is the entire period of time during which the Contractor is obliged to perform the Work, which:

begins on the date the Call-up is issued; and

ends on the day that the Warranty Period for the last Product delivered expires, or on the day that the final warranty work initiated during the Warranty Period is complete, or on the day that the professional services requested on a Call-up are completed, whichever is later.

When the Call-up is received, the contractor must acknowledge receipt of the Call-up as per the Call-up Procedures in the Standing Offer.

7.30 Payment

a) **Basis of Payment**

1) **Products**

(A) For the supply and delivery of the Products listed in the Call-up, Canada will pay the Contractor:

(i) Prices as listed in the Contractor's most current Published Price Lists (PPL), less the discount rate identified by the Contractor, which must be equal to or greater than the floor discount rate in Annex B, Appendix A – Financial Offer; or

(ii) Prices as listed in the Published Price List provided at the time of the Offer (ceiling prices), less the discount rate identified by the Contractor which must be equal to or greater than the floor discount rate in Annex B, Appendix A – Financial Offer.

whichever is the lowest price effective on the date of the Call-up.

(B) From the PPL(s) attached to the Standing Offer, only items listed that are not grayed out are available for purchase under the Standing Offer (items related to the 8 device categories). The PPL prices, as discounted, include all of the following:

(i) Delivery and transportation F.O.B. anywhere in the national capital region (NCR);
(ii) Customs Duty, if applicable;
(iii) Product configuration as per the Call-up;
(iv) the Hardware documentation and Licensed Software Documentation; and
(v) the Hardware Maintenance Service for all the Products as described in the Contract

Provincial Disposal Surcharge: The PPL(s) prices do not include any disposal surcharge, required to be paid by a Province in Canada, unless otherwise indicated. Any provincial disposal surcharge is extra to the price and will be paid by Canada.

2) **Professional Services**

(A) For professional services provided under the resource categories listed in Annex A - Requirement, Canada will pay the Contractor the associated per diem rates listed in Annex B, Appendix A – Financial Offer. All per diem rates represent 7.5 hours of work. Any work less than 7.5 hours will be paid at the pro-rated per diem rates.

(B) Travel:

The Contractor shall not be reimbursed for travel costs or time required for the Contractor to provide services in the NCR.

For any travel required outside of the NCR, the Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred outside of the NCR 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 (http://www.njc-cnm.gc.ca/directive/travel-voyage/index-eng.php), and with the other provisions of the directive referring to "travelers", rather than those referring to "employees".

All travel must have the prior authorization of the Standing Offer Authority. All payments are subject to government audit.

3) All prices are in Canadian dollars, Goods and Services Tax (GST)/Harmonized Sales Tax (HST) extra

b) **Limitation of Price**

SACC Manual clause C6000C (2011-05-16) Limitation of Price applies.

c) **Method of Payment**

1) **Products**

SACC Manual clause H1000C (2008-05-12) Single Payment applies.

2) **Professional Services**

SACC Manual clause H1008C (2008-05-12) Monthly Payment applies.

d) **Audit**

SACC Manual clause C0711C (2008-05-12) Time Verification applies.

e) **Payment Credits**

1) If the Contractor fails to deliver the Products or perform the professional services within 30 days from the date the Call-Up is issued or at the time specified in the Contract, whichever is latest, the Contractor must provide a credit to Canada of::

(A) 1% of the total Call-up value for late delivery or completion within 2 weeks following the initial 30 days (from when the call-up was issued) or the original completion or Delivery Date, whichever is latest; and

(B) 2% of the total Call-up value for late delivery or completion more than 2 weeks after the initial 30 days (from when the call-up was issued) or the original completion or Delivery Date, whichever is latest.

2) If any Products are not configured as required by the Call-up, Canada may provide the Contractor with an opportunity to re-configure the Products in accordance with the Call-up, but the Contractor agrees to reduce the price of the Products by 5% of the total value of the Products that are not in accordance with the configuration described in the Standing Offer or the alternative configuration described in the Call-up, in addition to the liquidated damages payable for late delivery of the Products (i.e., where the re-configured goods are delivered after the Delivery Date, the price must also be discounted as described in sub-article (1)).

3) The total amount of the liquidated damages will not exceed 15% percent of the contract price

4) **Credits represent Liquidated Damages**: The Parties agree that the credits are liquidated damages and represent their best pre-estimate of the loss to Canada in the event of the applicable failure. No credit is intended to be, nor will it be construed as, a penalty.

5) **Canada's Right to Obtain Payment**: The Parties agree that these credits are a liquidated debt. To collect the credits, Canada has the right to hold back, draw back, deduct or set off from and against any money Canada owes to the Contractor from time to time.

6) **Canada's Rights & Remedies not Limited**: The Parties agree that nothing in this Article limits any other rights or remedies to which Canada is entitled under the Contract (including the right to terminate the Contract for default) or under the law generally.

7.31 Invoicing Instructions

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

b) The Contractor's invoice must include a separate line item for each Product and service delivered

c) Each invoice for professional services must be supported by a copy of time sheets to support the time claimed. The time sheets must be filled in at the time the work is performed by the individual resource who performed the work.

d) Invoices must be distributed as follows:

The original must be forwarded to _____ *(to be completed at time of award.)* On request, the Contractor must provide a copy of any invoices to the Standing Offer Authority and the Technical Authority.

7.32 Foreign Nationals (Canadian Contractor)

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

7.33 Insurance

SACC Manual clause G1005C (2008-05-12) Insurance applies.

7.34 SACC Manual Clauses

SACC Manual clause B7500C (2006-06-16), Excess Goods; and

SACC Manual clause B9028C (2007-05-25), Access to Facilities and Equipment.

apply to and form part of the Contract.

7.35 Packaging

a) Packaging should be made of recycled materials and designed to minimize waste. When possible, bulk packaging should be used.

b) The Contractor agrees to take back the packaging for reuse, recycling or recovery, when requested by the RCMP at no additional cost to Canada.

c) The Contractor must include on the packing slip:

1) Call-up number; and

2) Any other RCMP internal tracking number provided along with the Call-up.

7.36 Delivery

a) Products must be delivered to the location(s) specified in the Call-up. All delivery locations for Products will be within the National Capital Region

b) The Contractor must deliver all items identified on the Call-up in one delivery. Multiple deliveries for one Call-up will not be accepted unless otherwise specified in the Call-up or agreed to in writing by the Call-up Coordinator.

c) Unless otherwise specified in the Call-up or the Identified User has agreed in writing to other arrangement, the Contractor must contact the Call-up Coordinator (or any individual designated as “Delivery Contact” in the Call-up) a minimum of twenty-four (24) hours prior to the delivery of any Product. Failure to make contact may result in the shipment being refused at destination; any re-shipping costs will be the Contractor’s responsibility.

d) Unless otherwise specified in the Call-up or the Call-up Coordinator has agreed in writing to other arrangements, the Contractor must provide the Call-up Coordinator with a Delivery Report detailing the delivery location and Product number of all Products delivered within 2 weeks of delivery.

e) Licensed Software:

The Products must be delivered with any software specified in the Call-up or required for the Products to function in accordance with the Technical Specifications in Annex A - Requirement. The unit price(s) include all fees and costs associated with the licenses to the Licensed Software, as well as the software maintenance and support services described in this Contract, which must be provided throughout the Hardware Maintenance Period.

The Licensed Software must be the current release and, unless otherwise specified, require no further research or development to meet the Technical Specifications (and any other functionality described in the Standing Offer or Call-up).

The Licensed Software must be supported by, and fully compatible with the Product(s) up to the limit of the Product's expansion capability (with no additional licensing fees payable). All software must be completely integrated with and fully interfaced to the Product.

This Contract grants to Canada the perpetual license (i.e., the license to use the Licensed Software is not a "demo" model and does not expire) to install, copy, deploy and use the Licensed Software with the Product(s) in accordance with the terms of this Contract (which does not include any terms or conditions contained in a shrink-wrap or click-wrap license, or other form of license delivered with the Licensed Software).

Canada acknowledges that the Licensed Software is only licensed to Canada, not sold.

f) Base Configuration: Unless specified in the Call-up, the Contractor must deliver all Products in accordance with the base configuration, as defined in Annex A - Requirement.

g) Late deliveries: If the expected Delivery Date will not be met, the Contractor must notify the Call-up Coordinator as soon as a delay is anticipated.

7.37 Limitation of Liability - Information Management/Information Technology

a) This section applies despite any other provision of the Contract and replaces the section of the general conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this section, even if it has been made aware of the potential for those damages.

b) First Party Liability:

The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to

any infringement of intellectual property rights to the extent the Contractor breaches the section of the general conditions entitled "Intellectual Property Infringement and Royalties"; and

physical injury, including death.

The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.

Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or

consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.

The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under 1) above.

Direct Damages for Goods: For all Call-ups that are solely for goods, the Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:

any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including any applicable taxes) for the goods and services affected by the breach of warranty; and

any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (B) of the greater of 0.25 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the block titled "Total Estimated Cost " or shown on each Call-up, purchase order or other document used to order goods or services under this instrument), or $2 million.

In any case, the total liability of the Contractor under paragraph 5) will not exceed the total estimated cost (as defined above) for the Contract or $2 million, whichever is more.

Direct Damages for Services: For all Call-ups that are solely for services, the Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:

any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including any applicable taxes) for the goods and services affected by the breach of warranty; and

any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (B) of the greater of 0.75 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the block titled "Total Estimated Cost " or shown on each Call-up, purchase order or other document used to order goods or services under this instrument), or $1 million.

In any case, the total liability of the Contractor under paragraph 6) will not exceed the total estimated cost (as defined above) for the Contract or $1 million, whichever is more.

Direct Damages for Combination of Goods and Services: For all Call-ups that are for a combination of goods and services, the Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:

any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including any applicable taxes) for the goods and services affected by the breach of warranty; and

any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (B) of the greater of subparagraphs 5) and 6) above.

If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

c) Third Party Claims:

Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.

If Canada is required, as a result of joint and several liability, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite paragraph 1), with respect to special, indirect, and consequential damages of third parties covered by this section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality. The Parties are only liable to one another for damages to third parties to the extent described in this paragraph c).

7.38 Hardware

With respect to the provisions of Supplemental General Conditions 4001:

Part III of 4001 applies to the Contract (Additional Conditions: Purchase)	Yes
Part IV of 4001 applies to the Contract (Additional Conditions: Lease)	No
Part V of 4001 applies to the Contract (Additional Conditions: Maintenance)	Yes
Delivery Location	As indicated in the Call-up issued against the Standing Offer, which may identify any one or more locations in the National Capital Region
Delivery Date	As set out in Supplemental General Conditions 4001 under the definition of Delivery Date (i.e., 30 days) unless another Delivery Date is specified in the Call-up. Delivery Dates specified in the Call-up could be as early as 5 business days.
Contractor must deliver Hardware Documentation	Yes. However, despite section 7(4), documentation must be provided through web access. Accounts are to be active until the end of the Contract Period or the end of the last warranty period, whichever is latest.
Contractor must update Hardware	Yes

Documentation throughout Contract Period	
Hardware Documentation must include maintenance documentation	Yes
Language of Hardware Documentation	Unless specified in the Requirement, documentation is only required to be delivered in English. If documentation is available in French and English it must be provided in both languages.
Format and Medium on which Hardware Documentation must be Delivered	Electronic web access
Special Delivery Requirements	No
Special Site Delivery or Installation Requirements	Yes
Responsibility for Special Site Delivery or Installation Requirements	As per Supplemental General Conditions 4001 (2010-08-16) section 4.2.b-d
Contractor must Install Hardware at time of Delivery	No
Contractor must Integrate and Configure Hardware at time of Installation	No, all configuration identified in the Call-up must be done prior to delivery.
Hardware is part of a System	Yes
Availability-level testing will be performed before Acceptance	No
Hardware Warranty Period	Despite 4001, the Hardware Warranty Period under Part III and Part V is 90 calendar days from the date of acceptance.
Class of Maintenance Service	Return-to-Depot Maintenance Service. Despite 4001, Section 26(2), for Return-to-Depot Maintenance Service, during the PPM throughout the Hardware Maintenance Period, the Contractor must pick up the Hardware requiring maintenance within forty-eight (48) hours of Canada requesting maintenance. Within thirty (30) working days of Canada requesting maintenance, the Contractor must deliver a replacement that meets the requirements of the Contract. Every item of Hardware requiring maintenance must be replaced rather than repaired.
Principal Period of Maintenance (PPM)	4001, Section 25(4), the PPM is 9 hours each day, from 8 a.m. to 5 p.m., Eastern Time, Monday to Friday, not including statutory holidays observed in the province of Ontario.
Toll-free Telephone Number for Maintenance Service	[to be completed with information from the Offeror at the time of award]

7.39 Hardware and Software Maintenance and Support Services

In addition to Supplemental General Conditions 4001, the following applies to the Hardware and Software Maintenance Service:

a) OEM's Warranty: If the Contractor wishes to rely on the OEM's warranty to provide the Hardware or Software Maintenance Services, the Contractor must complete all warranty registration requirements with any OEM on behalf of the Identified User. The Offeror must also notify the Identified User in writing of any requirement to register for international warranty coverage required if the end user will travel abroad with Products supplied under this Contract. Regardless of any OEM's warranty, the responsibility for providing the Hardware and Software Maintenance Services remains with the Contractor.

b) Magnetic Media: To maintain the confidentiality of information that may be recorded on magnetic media incorporated into a Product requiring Hardware Maintenance Services, the magnetic

media in all components requiring replacement (or the entire Product if the media is not removable) must remain in the possession of Canada. Faulty discs and hard drives will not be returned to the OEM.

c) Hotline Services: With respect to the hotline services required to be provided under Supplemental General Conditions 4001, the Contractor must:

Identify each reported maintenance incident via a unique warranty incident tracking number;

Confirm that the failing component is covered under the standard warranty;

Communicate regular updates to the RCMP;

Maintain an archive of maintenance incident reports and their resolutions for the duration of the Contract Period;

Make the archive of maintenance incident reports and their resolutions available to the RCMP in a CSV format when requested;

Identify date and time maintenance incident was reported; and

Identify date and time for delivery of a replacement.

d) Documented Procedures: The Contractor must document procedures for reporting and tracking warranty incidents and make them available to PWGSC and the RCMP upon request.

7.40 User-Serviceable Products

The Contractor agrees that the Identified User's technical support staff may perform maintenance and/or upgrades to the Products and replace user-replaceable or user-serviceable components without affecting the obligation of the Contractor to provide the Hardware Maintenance Services.

7.41 Safeguarding Electronic Media

a) Before using them on Canada's equipment or sending them to Canada, the Contractor must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Contractor must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.

b) If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

ANNEX A

REQUIREMENT

For

Multimedia Network Convergence
Equipment and Support Services

For

Royal Canadian Mounted Police (RCMP)

Table of Contents

1 Overview

1.1 Objective

1.1.1) Migrate Radio, Voice and Video networks to IP-based network technologies consistent with the existing RCMP data network, all the while ensuring:

a) Continuity - augment, replace or enhance the existing equipment that is currently implemented while maintaining service levels and minimizing service interruption;

b) Cost effectiveness - augmenting, replacing or enhancing existing equipment must be cost effective;

c) Ubiquitous interoperability – products must be fully interoperable with existing RCMP data network equipment and network management tools;

d) Adaptability – have available a full range of products in order to be able to configure products based on individual site requirements; and

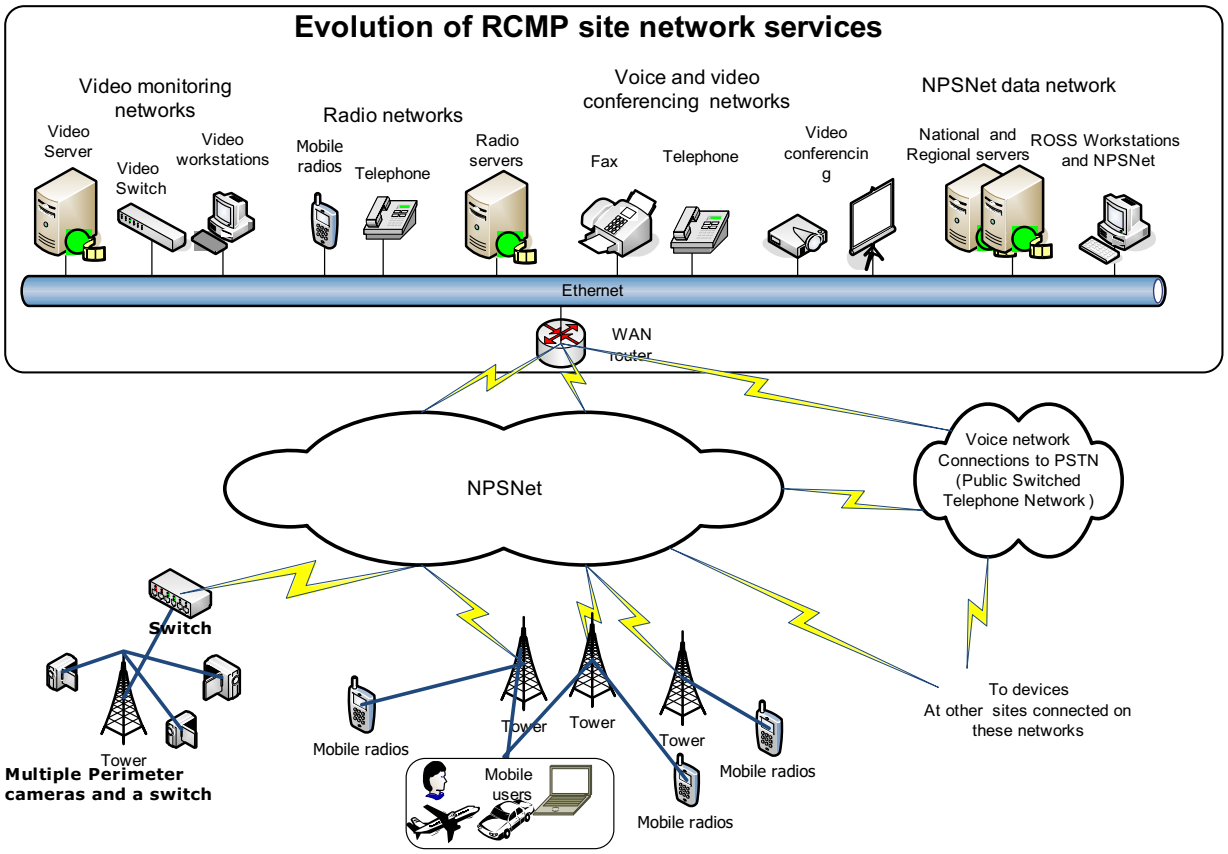
e) Expertise – have available expert resources to assist RCMP personnel in deploying and supporting the multimedia network equipment.

1.1.2) The RCMP migration to a shared multimedia network will be a gradual migration from many existing networks onto a smaller number of interoperable multimedia networks.

1.1.3) Integration Objectives

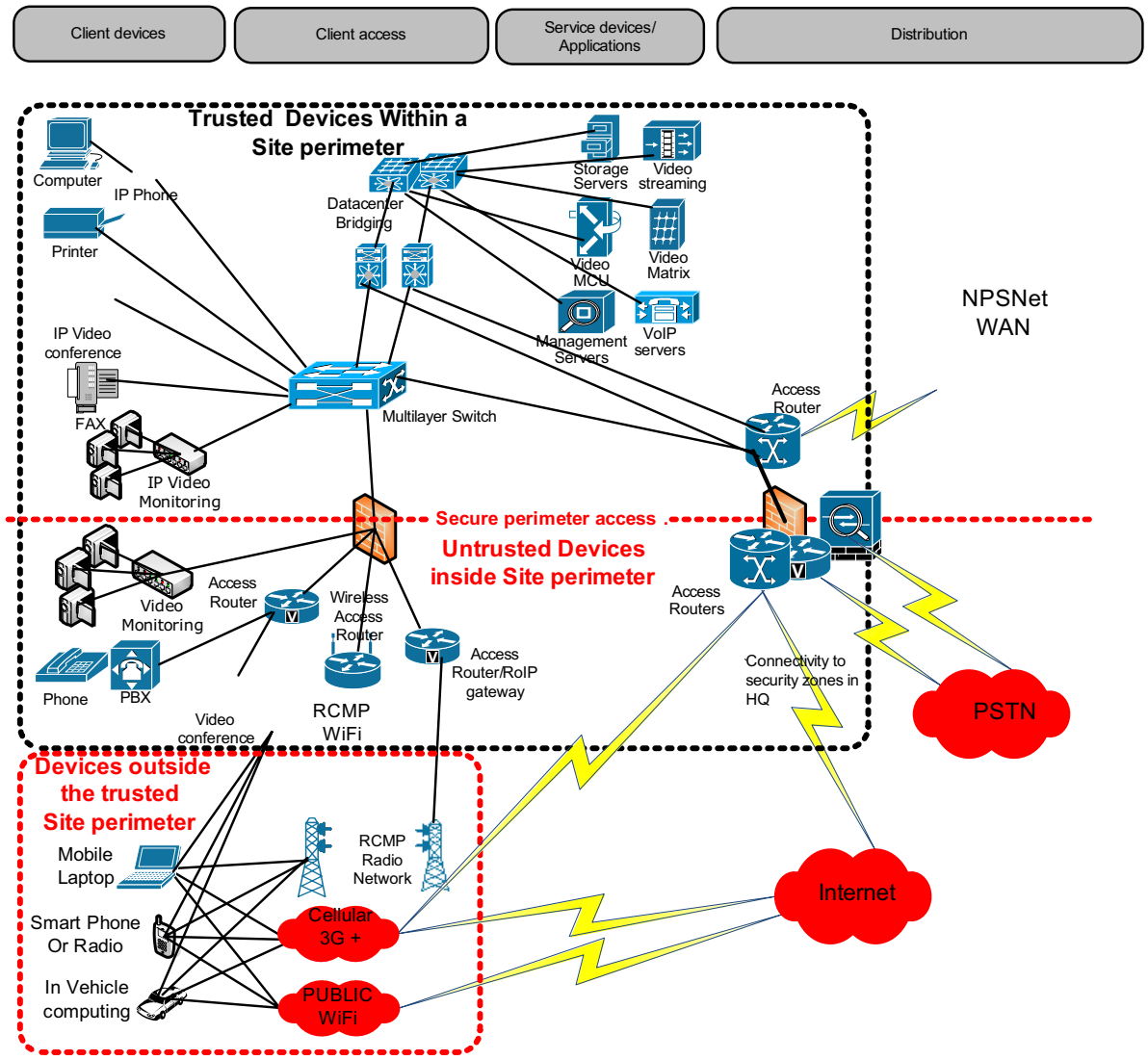
a) The migration of these multimedia requirements onto IP-based technologies creates an opportunity to consolidate some of these networks onto the RCMP's NPSNet. Some of the larger NPSNet multimedia network pilots include projects such as the National HQ VoIP, Video monitoring at the Quebec summit, Video monitoring at the Olympics and Radio over IP in Newfoundland. The RCMP will continue to leverage its NPSNet to integrate multimedia network requirements where possible. Ideally all external access could be connected to through an interoperable, highly secure, highly available and scalable network and device capable of integrating much of the RCMP multimedia network functionality.

b) Diagram of integration objectives for RCMP site deployments:

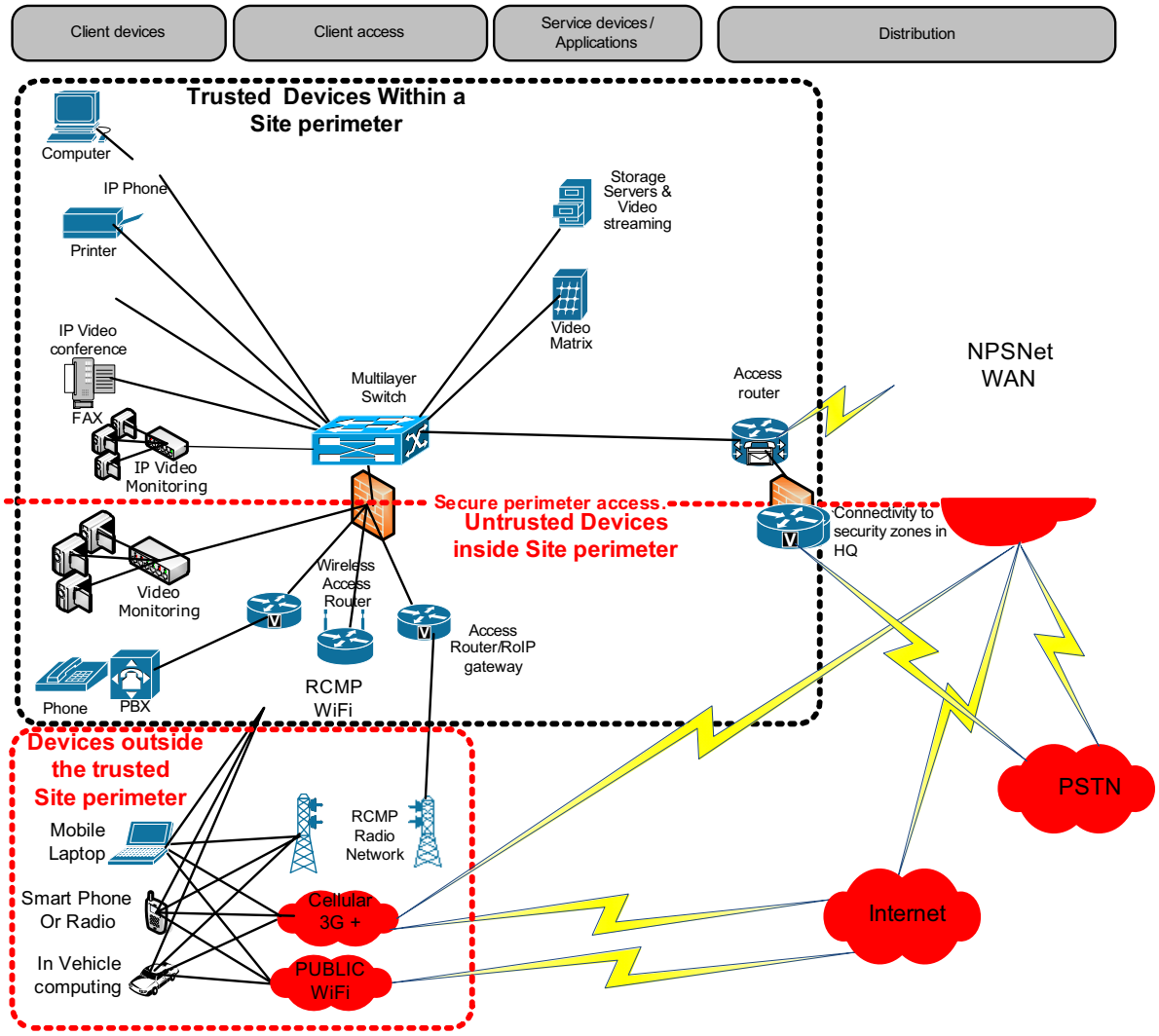


1.1.4) High Level Converged Network Architecture

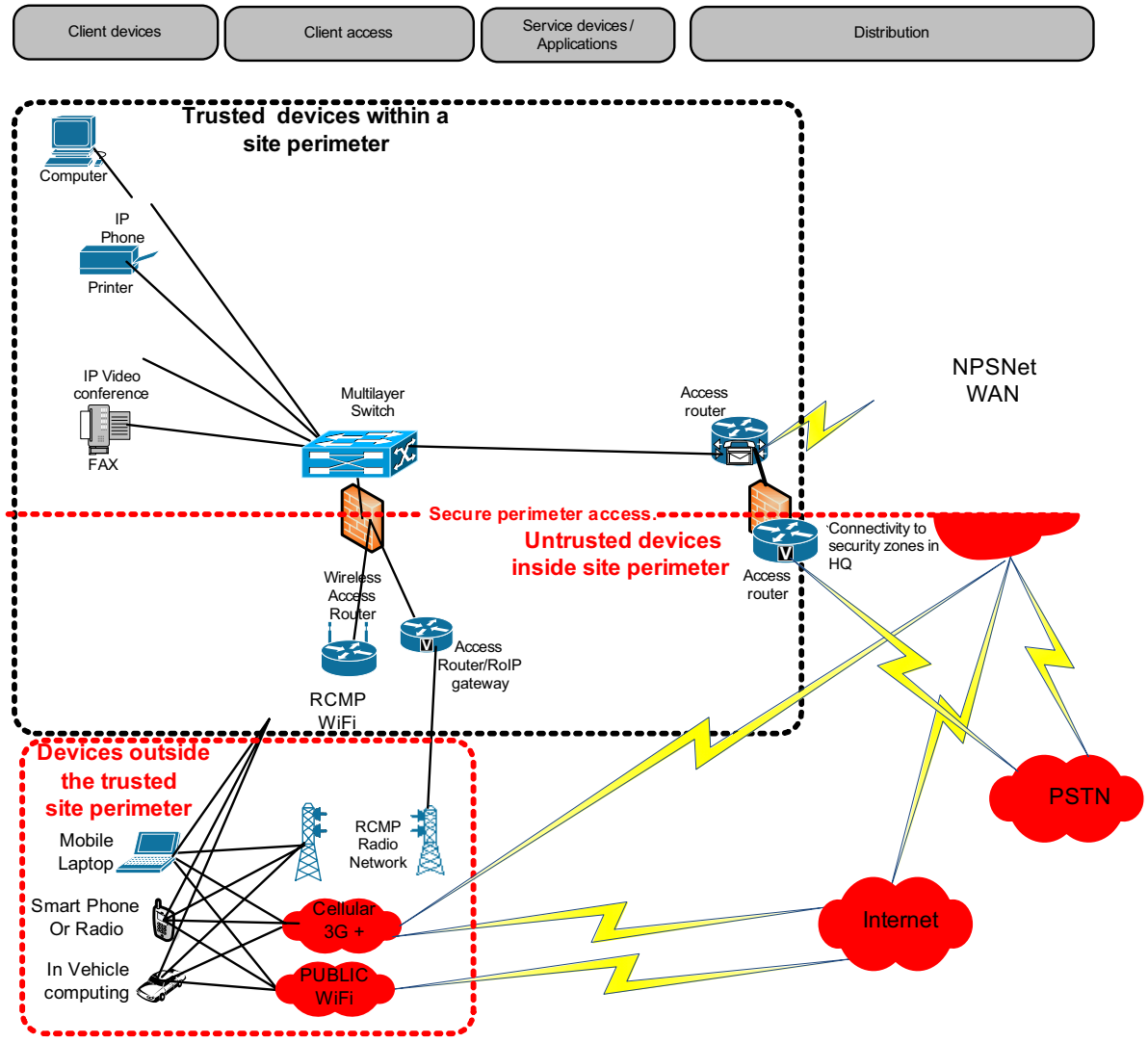
a) The figure below illustrates the objectives of the RCMP converged network equipment deployments for large sites, campus sites, and National headquarters at this time. The diagram is a conceptual categorization of the RCMP design. The individual site configurations will vary to fit more accurately with the individual site requirements. Also some device functions at sites may be combined into a single device where equipment solutions that meet the RCMP requirements exist.



b) The figure below illustrates the objectives of the RCMP network multimedia equipment deployments for medium size sites. The diagram is a conceptual categorization of the RCMP design. The individual site configurations will vary to fit accurately with the regional and individual site requirements. Also some device functions at sites may be combined into a single device where convergence solutions that meet the RCMP requirements already exist.



c) The figure below illustrates the objectives of the RCMP network multimedia equipment deployments procurements for small size sites. The diagram is a conceptual categorization of the RCMP design. The individual site configurations will vary to accurately fit the individual site requirements. Also some device functions at sites may be combined into a single device where convergence solutions meet the RCMP requirements.



1.2 Overall Requirement

1.2.1) The RCMP requires specialized multimedia network equipment and professional services to allow the RCMP to migrate different multimedia onto the RCMP IP data WAN network and the existing VoIP infrastructure. The equipment will augment the existing RCMP IP data

network to provide the capability of Radio, Voice and Video network convergence on a national scale. The Contractor must provide:

a) Network equipment and warranty services; and

b) Professional services.

1.2.2) The required equipment categories for the multimedia network convergence are:

a) Access Routers

b) Data Centre Bridging

c) Voice over IP (VoIP)

d) Radio over IP (RoIP)

e) IP Video Monitoring

f) IP Video Conferencing

g) Wireless LAN

h) Wireless IDS/IPS

1.2.3) The required professional resource categories for the multimedia network convergence are:

a) Network Architect

b) Network Project Manager

c) OEM Product Specialist

1.3 Terminology

1.3.1) Equipment Categories / Device Categories: the generic over-arching categories of equipment that are within scope of the requirement.

1.3.2) Device: Devices are standalone or clusters of standalone equipment with software that meets all the stated requirements.

1.3.3) Component: Components are cards, GBICs, software, feature licenses, servers, memory or any options that can be added to existing devices, new devices or clusters of devices to upgrade capacity and or functionality. Components could also include a device chassis or server required to upgrade the capacity and functionality for some of the existing configurations.

1.3.4) Chassis: typically a standalone framework to which the modular components of the equipment are attached to be made functional.

1.3.5) Base requirement: a mandatory requirement that must be met and is the minimum requirement that must be included in the price of the device.

1.3.6) Upgrade requirement: a mandatory requirement that is an additional capability that must be available on the device. Some upgrade requirements will include a list of requirements that collectively form the base requirements of the upgrade.

1.3.7) Type 1 Phone: a very basic phone used in common areas.

1.3.8) Type 2 Phone: a desktop phone for most RCMP users.

1.3.9) Type 3 Phone: a desktop phone for users with larger multi-line requirements.

1.3.10) Type 4 Phone: a conference room phone.

2 General Requirement

2.1 Documentation

2.1.1) Unless otherwise specified, the Contractor must deliver documents, reports, forms, and any other deliverables for the entire Contract Period, in a format that is compatible with the commercial desktop applications used by RCMP. These applications are currently as follows:

a) Microsoft Office 2010;

b) Microsoft Project 2010;

c) Microsoft Access 2010;

d) Microsoft Visio version 2010; and

e) Adobe PDF (Portable Document Format).

2.1.2) The Contractor is responsible for maintaining format compatibility with the RCMP desktop applications as they evolve, for the duration of the Contract Period.

2.1.3) Any documentation and/or deliverables provided that do not meet the requirements described above will not be accepted.

3 Services

3.1 Common Service Requirements

3.1.1) Location

Most professional services will be provided in the National Capital Region (NCR). In exceptional cases, travel outside the NCR may be required and authorized by the Standing Offer Authority.

3.2 Ongoing Services

3.2.1) The RCMP requires the following services to be provided by the Contractor on an ongoing basis and included in the price of the equipment:

a) Configuration Services:

The Contractor (or the OEM on its behalf) must work with RCMP to provide equipment configuration guidance before the placing of equipment orders, at no additional cost to the RCMP.

b) Warranty and Support Services:

Warranty and Support Services as per the resulting Standing Offer and Contract clauses.

3.3 Professional Services

3.3.1) The Contractor may be required to provide specialized services and resources for unique network requirements related to the network equipment deployments. The specialized requirements will relate to:

a) Network design;

b) Architecture, engineering and testing work for Implementation of multimedia network solutions using the equipment in this contract;

c) Solutions development;

d) Systems planning;

e) Project management of large network deployments;

f) Systems implementation;

g) Systems testing;

h) Systems upgrades;

i) Deployment of new solutions such as indoor and outdoor wireless antenna;

j) Unique Operational support functions;

k) Unique network support requirements like wireless site surveys and fibre OTDR tests;

l) Specialized onsite installation tasks;

m) Offsite staging of equipment; and

n) Onsite training for new products.

The individual requirements will be identified in each Call-up.

3.3.2) The Contractor must provide resources from the following categories:

a) Network Architect;

b) Project Manager; and

c) OEM Device Category specialists.

3.3.3) Network Architect

a) A Network Architect is a specialist with detailed knowledge of network systems and technologies in all areas of IP network services including multimedia network systems for RoIP, VoIP, video conferencing and video surveillance over IP.

b) A Network Architect must have at least 84 months of experience designing networks for multimedia network systems including VoIP or video conferencing or video surveillance over IP end-to-end and/or must have at least 36 months of experience designing networks for multimedia network systems including RoIP end-to-end. This includes, at a minimum, the requirement definition, design, installation, testing and cutover of multimedia network system.

c) The duties of a Network Architect include, but are not limited to the following:

(1) Develops technical architectures, frameworks and strategies, either for an organization or for a major application area, to meet the business and application requirements;

(2) Identifies the policies and requirements that drive a particular solution;

(3) Analyses and evaluates alternative technology solutions to meet business problems;

(4) Ensures the integration of all aspects of technology solutions;

(5) Designs and documents, in detail, all system components, their interfaces and operational environment;

(6) Designs network structures, sub-systems, modules, production monitoring procedures, testing strategy, and systems;

(7) Documents network design, concepts and facilities; presents and obtains approval of detailed system design;

(8) Writes user manual covering manual processes and operational procedures, defines user acceptance testing checklist, and obtains associated user acceptance;

(9) Identifies and documents system specific standards relating to programming, documentation and testing, covering program libraries, data dictionaries, naming conventions, etc.;

(10) Defines specific technical requirements for network acquisition, develops conversion plans and parallel operation procedures, and estimates resource and cost requirements; and

(11) Monitors industry trends to ensure that solutions fit with government and industry directions for technology.

3.3.4) Project Manager

a) A Project Manager is a senior project manager who can manage projects of high complexity and medium to high risks.

b) A Project Manager must:

(1) Have at least 5 years of experience as a project manager for projects of high complexity and risks involving the deployment of IT infrastructure; and

(2) Have a demonstrated capability of managing a team of IT specialists.

c) The duties of a Project Manager include, but are not limited to the following:

(1) Manage several Project Managers, each responsible for an element of the project and its associated project team;

(2) Manage the project during the development, implementation and operations start-up by ensuring that resources are made available and that the project is developed and is fully operational within previously agreed time, cost and performance parameters;

(3) Formulate statements of problems; establishes procedures for the development and implementation of significant, new or modified project elements to solve these problems, and obtains approval thereof;

(4) Define and document the objectives for the project; determine budgetary requirements, the composition, roles and responsibilities and terms of reference for the project team;

(5) Report progress of the project on an ongoing basis and at scheduled points in the life cycle;

(6) Meets in conference with stakeholders and other project managers and states problems in a form capable of being solved;

(7) Prepare plans, charts, tables and diagrams to assist in analyzing or displaying problems; work with a variety of project management tools; and

(8) Project sign-off.

3.3.5) OEM Product Specialist

a) An OEM Product Specialist is a resource who is a specialist in the specified device category. For instance the Contractor must be prepared to provide a resource for the Access Router device category.

b) An OEM Product Specialist must at a minimum:

(1) Have at least 36 months of experience engineering, deploying and supporting network equipment in this device category; and

(2) Have achieved the highest level of certification available from the OEM for the Device Category in question.

c) The OEM Product Specialist duties include, but are not limited to the following:

(1) Work with the RCMP technical resources to develop technical architectures, frameworks and strategies, to meet the business and application requirements;

(2) Work with the RCMP technical resources to ensure the integration of all aspects of the OEM's technology solutions;

(3) Work with the RCMP technical resources to resolve complex problems;

(4) Work with the RCMP technical resources to pass on specialized knowledge and/or train RCMP resources; and

(5) Review and validate RCMP technical architectures, frameworks and strategies.

The individual requirements for the professional services will be identified in each Call-up.

4 Products

4.1 Common Technical Requirements

The following are technical requirements that must be met by all Products provided by the Contractor:

4.1.1) Interoperability

a) Components must work with existing equipment, without any modification, and have full and complete interoperability with the RCMP's existing devices as described in the Standing Offer.

b) All equipment provided by the Contractor must have full and complete interoperability without modification or replacement of the RCMP's existing infrastructure. Any equipment provided by the Contractor must support any of the relevant protocols.

c) The existing RCMP environment is described in Appendix B

4.1.2) Environmental Requirements

Minimum environment operating and non-operating conditions applicable to all device and Product requirements, except where specific requirements within a section indicate otherwise:

a) Operating conditions:

(1) Temperature: 10 degrees to 35 degrees Celsius

(2) Relative Humidity (non-condensing): up to at least 80%

b) Non-operating conditions:

(1) Temperature: -10 degrees to 60 degrees Celsius

(2) Relative Humidity (non-condensing): up to at least 90%

4.2 Consistency of OEM Provider

4.2.1) For each of the following equipment categories, all equipment and components must be from the same OEM unless indicated otherwise within the requirements defined in the device category requirements.

a) Access Router devices;

b) Datacenter Bridging devices;

c) VoIP devices;

d) Radio over IP devices;

e) IP Video monitoring devices;

f) IP Video conferencing devices;

g) Wireless LAN devices; and

h) Wireless IDS/IPS devices.

4.3 Security

4.3.1) The physical safeguarding and integrity protection of the RCMP data systems and applications is of key importance to the RCMP. Federal laws and policies, such as the Policy on Government Security, the Access to Information Act, the Privacy Act and the Official Secrets Act, detail specific criteria for the protection of infrastructure and information. The Contractor must abide by those security requirements in addition to all other security requirements described in this Contract. The Contractor must work with the RCMP to ensure these requirements are met and the RCMP must approve any deviations before implementation.

4.3.2) The Contractor must provide equipment that allows creation, maintenance, and deletion of user profiles by authorized RCMP personnel. Any component, device or system with network management access must use authentication with unique user identifiers.

4.3.3) The Contractor must provide equipment with access controls and identification and authorization protection mechanisms to protect the systems and management systems from unauthorized access through network ports attached to the RCMP's corporate network or from ports attached to RCMP equipment. The Identification and authentication mechanisms must ensure protection from unauthorized access. Two-Factor authentication (something you have and something you know) must be used for any external access being authenticated to the equipment and components.

4.3.4) The Contractor must provide equipment with access controls that allow limits on number of unsuccessful login attempts to be set and modified by the RCMP.

4.3.5) The Contractor must provide equipment with security features that keep audit trails of logins and actions performed while logged in that can be transferred to permanent storage on the RCMP network management servers.

4.3.6) The Contractor must provide equipment with access controls that allow an inactivity limit to be set and modified by the RCMP. The inactivity limit must be activated automatically so that the account is logged out at the end of the inactivity period.

4.3.7) The Contractor must provide equipment with management software and security management software that provide security incident violation alarms, audit tracking and reporting for the detection and tracking of security violations by the RCMP.

4.3.8) The Contractor must provide equipment with access controls that provide role-based security levels that can be used to assign different access permissions to the RCMP's different organization roles and job functions.

4.4 Components for the Current Environment

4.4.1) The Contractor must provide network components to augment the existing RCMP devices. The additional hardware and software components will be required to enhance the capacity and functionality of the existing devices.

4.4.2) The list of components, which must be made available by the supplier, is attached in Annex B Appendix A Table 1. The list of Products to be delivered under this Contract are listed in the Call-up.

4.4.3) The components provided for the existing environment must be the same as or equivalent to the components listed in Annex B Appendix A Table 1.

4.5 Device Categories

The Contractor must provide network and IP equipment for specific device categories, which will migrate the RCMP multimedia onto the RCMP network on the national scale. The Device Categories are:

4.5.1) Access Routers

4.5.2) Data Centre Bridging

4.5.3) Voice over IP (VoIP)

4.5.4) Radio over IP (RoIP)

4.5.5) IP Video Monitoring

4.5.6) IP Video Conferencing

4.5.7) Wireless LAN

4.5.8) Wireless IDS/IPS

5 Device Category Technical Requirements

5.1 Reading the Requirements Tables

5.1.1) The requirements for each device category are listed in the form of a table. A cell containing an “X” represents what sub-category the requirement is for as well as whether it is a base, upgrade or option requirement.

a) Example 1: at section 5.2.2.) requirement a) (1) - Part of the Base requirement for all Access Routers be it for small, medium or large sites is that it must be rack mountable. This feature must be included in the base price.

b) Example 2: at section 5.2.2) requirement h) (2) - Part of the Base requirement for all Access Routers for medium sites only is WAN IP packet forwarding of up to 35Mbps. This feature must be included in the base price.

c) Example 3: at section 5.2.2) requirement g) (15) - An upgrade option that must be available for all Access Routers be it for small, medium or large sites is FIPS 140-2 certified VPN encryption configurations. There may be an additional charge above the base requirement when this upgrade is chosen.

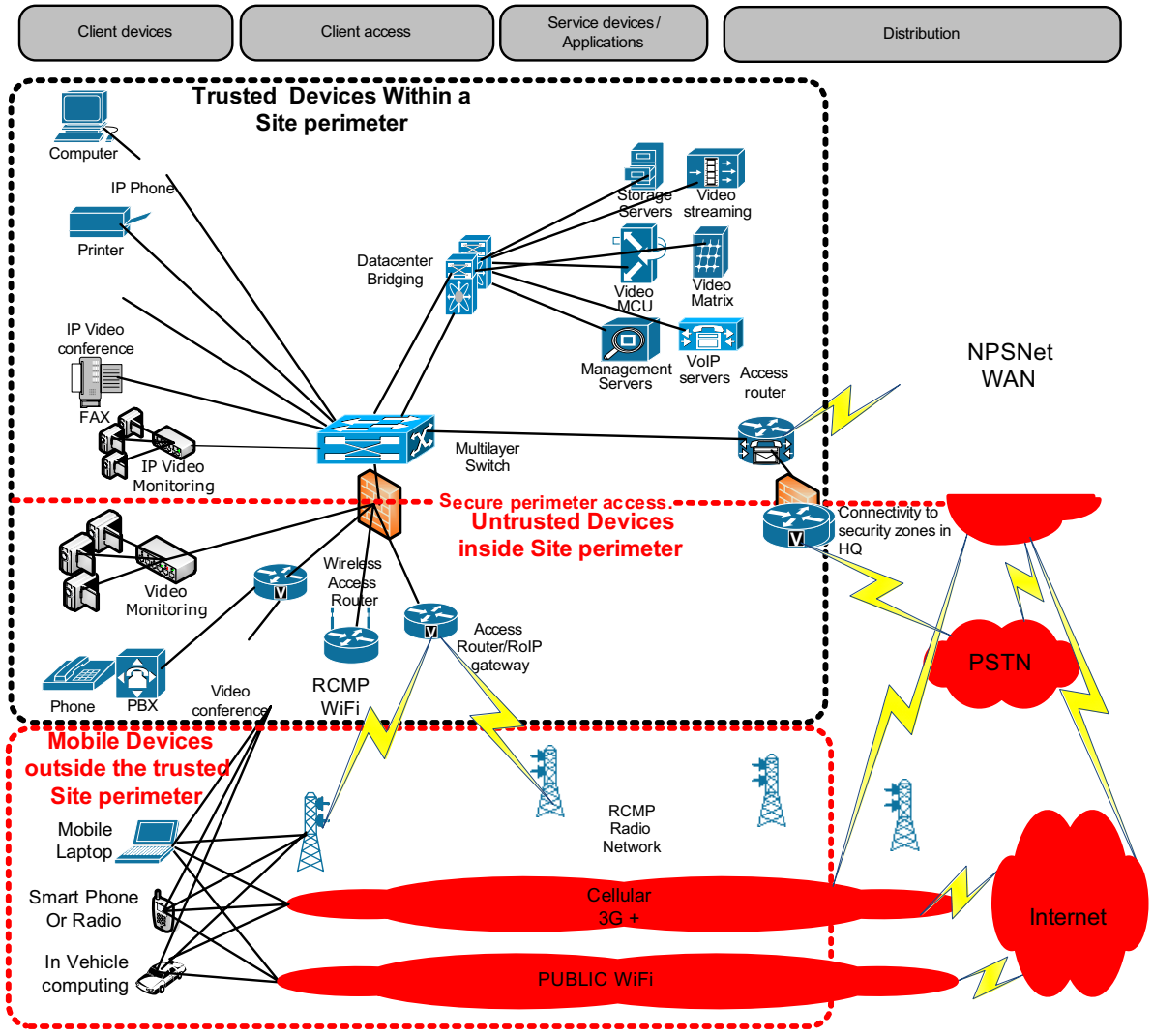
d) The requirements in the tables are minimum requirements only. Functionalities for the equipment proposed must meet and can exceed the stated requirement.

5.2 Access Routers

5.2.1) Access Router Environment

a) The Access Router equipment provides key integration functionality for the RCMP's access to multiple networks from a variety of multimedia devices.

Figure 1 Access Router Environment



5.2.2) Access Router Technical Requirements

Access Router Requirements	Base	Upgrade	Small Site	Medium Site	Large Site
a) Physical					
(1) Rack mountable in Standard 19" rack with standard AC 110V power	X		X	X	X
b) Ports					
(1) Minimum of 3 WAN 10/100/1000 Ethernet RJ-45 ports	X		X	X	
(2) ISDN PRI and BRI ports for PSTN connectivity		X	X	X	
(3) FXS and FXO ports for Analog phone and PBX device connectivity		X	X	X	
(4) Serial interfaces ports supporting STUN and STUN for LLC2 connections		X	X	X	
(5) E&M 2 wire and four wire inter face ports for LMR connectivity		X	X	X	
(6) 10/100/1000 Ethernet LAN ports with PoE as per IEEE 802.3af for IP phone connectivity		X	X	X	
(7) Intentionally left blank					
(8) Wireless access interface for Cellular networks supporting CDMA EV-DO Rev A and HSPA networks from Canadian cellular network providers		X	X	X	
(9) Ports with support 10 Gigabit Ethernet standards including 10GBASE-ER, 10GBASE-LR and 10GBASE-ZR interfaces		X			X
(10) Ports with Support Gigabit Ethernet standards including 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX and 1000BASE-T		X			X
(11) Ports with support for T3 interfaces with DSX3 level interface with dual female 75-ohm BNC coaxial connectors per port (separate RX and TX) supporting full duplex connectivity at DS3 rate (44.736 MHz)		X			X
c) Features					
(1) Internet Protocol as per RFC 791, 1812	X		X	X	X
(2) Ethernet prioritization and CoS as per IEEE 802.1p	X		X	X	X
(3) VLAN tagging as per IEEE 802.1q	X		X	X	X
(4) Internet Group Management Protocol IGMPv1, IGMPv2, IGMPv3	X		X	X	X
(5) NAT as per RFC1631	X		X	X	X
(6) Data Link Switching Supporting IETF RFCs 1795, 2166	X		X	X	

Access Router Requirements	Base	Upgrade	Small Site	Medium Site	Large Site
(7) Protocol Independent Multicast Supporting IETF RFCs 2337, 2362	X		X	X	X
(8) Class-Based RTP and TCP Header Compression configurable per interface	X		X	X	X
(9) LMR capability using E&M interfaces for connecting to Radio devices converting radio signals into E&M two wire and four wire signals		X	X	X	
(10) Survivable Remote Site Telephony to restore at least calling services for local VoIP phone in case of failure of connectivity to be interoperable with existing centralized VoIP IP PBX based on Cisco Call Manager V7.0		X	X	X	
(11) VoIP IP PBX including call management functionality at a minimum		X	X	X	
(12) VoIP IP PBX including messaging functionality at a minimum		X	X	X	
(13) Onboard Video surveillance storage and management		X	X	X	
(14) Onboard Wireless LAN Controller module for 802.11 a/b/g/n Wireless LAN Access points		X	X	X	
(15) Onboard voice recording capabilities		X	X	X	
(16) FAX over IP		X	X	X	
d) Management Features					
(1) CLI support	X		X	X	X
(2) Integral SNMP agent (no external proxy agents) as per RFCs 1155-1157	X		X	X	X
(3) Simple Network Management Protocol for Remote and In-band management supporting IETF RFCs 1157, 1904, 1905, 1906, 1907, 2273 and 2274	X		X	X	X
(4) Management Information Base for Network Management of TCP/IP-Based Internets supporting IETF RFC 1213	X		X	X	X
(5) Interface table as per RFC 1573	X		X	X	X
(6) Bridge MIB as per RFC 1493	X		X	X	X
(7) Ethernet MIB as per RFC 1643	X		X	X	
(8) Ethernet Repeater MIB as per RFC 1516	X		X	X	
(9) RMON as per RFC 1757	X		X	X	X
(10) RMON II as per RFC 2021	X		X	X	X
(11) TELNET as per RFC 854	X		X	X	X
(12) Secure SHell version 2	X		X	X	X
(13) Support for Authentication, Authorization and Accounting with RADIUS (Supporting IETF RFC 2865) and TACACS+ (Supporting IETF RFC 1492)	X		X	X	X

Access Router Requirements	Base	Upgrade	Small Site	Medium Site	Large Site
(14) TFTP as per RFC 783	X		X	X	X
(15) FTP as per RFC 959	X		X	X	X
(16) NTP (Network Time Protocol) as per RFC1305 Support	X		X	X	X
(17) A physical port must be provided for management and diagnostics directly on the device	X		X	X	X
(18) Device software that provides a web-based interface to perform administrative capabilities	X		X	X	X
(19) Provide a visual status of the device power and device systems status	X		X	X	X
(20) Provide a visual status of Indicators for a disabled port, an Ethernet ports link integrity, a ports Ethernet traffic, a ports duplex state, and a ports negotiated speed	X		X	X	
(21) Interoperability with Cisco Works or equivalent	X		X	X	X
(22) Cisco Discovery Protocol version 1 and 2 or equivalent	X		X	X	X
(23) SNMP version 1, 2 and 3	X		X	X	X
(24) SSH Version 2 with 3DES encryption	X		X	X	X
e) QoS and Multimedia Performance Features					
(1) IEEE 802.1q/p, CoS and DSCP marking, classification and reclassification based on incoming physical port, source and destination IP address, source and destination MAC address, and TCP and UDP port number	X		X	X	X
(2) ACL based per input port traffic shaping and rate limiting	X		X	X	X
(3) Low-Latency Queuing and Class Based WFQ	X		X	X	X
(4) Class based Weighted Random Early Detection	X		X	X	X
(5) Different Egress priority queues per port	X		X	X	X
(6) Committed Access Rate, Rate limiting by port, incoming interface, MAC source and destination address, IP source and destination address, UDP port, TCP port or Access List based criteria	X		X	X	X
(7) QoS ACLs for marking traffic on all ports with no port performance degradation	X		X	X	X
(8) Deep Packet Inspection (Layer 2-7 of the OSI model) such as Network Based Application Recognition or equivalent for validating QoS tagging and the blocking of certain security threats in the network Access Router	X		X	X	X
(9) DiffServ compliant WRED	X		X	X	X

Access Router Requirements	Base	Upgrade	Small Site	Medium Site	Large Site
(10) RSVP Protocol supporting IETF RFC 2205	X		X	X	X
(11) IP traffic Policing	X		X	X	X
(12) IP traffic Marking	X		X	X	X
(13) IP traffic Shaping	X		X	X	X
(14) Generic Traffic Shaping	X		X	X	X
(15) Hierarchical QoS	X		X	X	X
(16) Bandwidth-based multicast CAC on a per interface basis for transmission of Video multicast streams	X		X	X	X
f) IP Routing Features					
(1) IP Version 4 and Version 6 routing	X		X	X	X
(2) Inter VLAN IP routing	X		X	X	X
(3) Routing of legacy IPX traffic	X		X	X	X
(4) Static Routes	X		X	X	X
(5) RIPV2 as per RFC 1388, 1389, 2453	X		X	X	X
(6) RIP-2- MD5 Authentication as per RFC 2082	X		X	X	X
(7) BGP and BGP Route Reflector	X		X	X	X
(8) IS-IS	X		X	X	X
(9) Enhanced Interior Gateway Routing Protocol	X		X	X	X
(10) OSPF as per RFC 2178, 2328 with MD5 authentication as per RFC 2385	X		X	X	X
(11) OSPF Version 2	X		X	X	X
(12) OSPF Version 3;	X		X	X	X
(13) NBMA Next Hop Resolution Protocol Supporting IETF RFC 2332	X		X	X	X
(14) Bootstrap Protocol, DHCP Relay as per RFC 951, RFC 1541, RFC1542, RFC2131	X		X	X	X
(15) DVMRP as per RFC 1075	X		X	X	X
(16) IGMP as per RFC 1112, RFC 2236, RFC 3376	X		X	X	X
(17) PIM in both dense and sparse modes of operation as per RFC 2117, 2337and 2362	X		X	X	X
(18) Classless InterDomain Routing	X		X	X	X
(19) PBR	X		X	X	X
(20) PfR	X		X	X	X
(21) VRRP as per RFC 3768 (rfc3768), HSRP as per RFC2281 and MHSRP or VRRP that will interoperate with the VRRP in existing RCMP devices	X		X	X	X

Access Router Requirements	Base	Upgrade	Small Site	Medium Site	Large Site
g) Security Features					
(1) Port-based network access control IEEE 802.1x interoperable with RADIUS for device authentications	X		X	X	X
(2) Port-based ACLs for flexible per ports security with ACLs handled in hardware	X		X	X	X
(3) MAC address notification to management systems	X		X	X	X
(4) MAC address filtering, MAC Learning and Locking	X		X	X	X
(5) IPSec Hash function using: SHA-1 and integrity protections using HMAC	X		X	X	X
(6) IPSec encryption using AES block ciphers with key sizes of 128,192 and 256	X		X	X	X
(7) IPSec key exchange using IKEv1 as per RFC 2409 and IKEv2 as per RFC 4306	X		X	X	X
(8) Generic Router Encapsulation as per RFC 2784, 2890	X		X	X	X
(9) L2TPv3	X		X	X	X
(10) Dynamic Multipoint VPN Version 3 or equivalent that must interoperates with RCMP DMVPN deployments in spoke to spoke mode	X		X	X	X
(11) Group Encrypted Transport VPN	X		X	X	X
(12) IPSec 3DES, AES 128, AES 192, and AES 256 cryptology acceleration without consuming a hardware slot (onboard VPN Encryption and Acceleration)	X		X	X	X
(13) Support management user authentication through RADIUS and TACACS+ as per RFC1492	X		X	X	X
(14) EAL4 certified stateful firewall configuration. Firewall feature set must include: context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, java blocking and real-time alerts		X	X	X	X
(15) FIPS 140-2 certified VPN encryption configurations		X	X	X	X
(16) IPS		X	X	X	
(17) Intentionally left blank					
(18) URL filtering capabilities		X	X	X	
h) Performance and Capacity					
(1) Memory configured to support new software releases for the next 2 years	X		X	X	X
(2) WAN IP packet forwarding of up to 35Mbps	X		X		
(3) Encryption throughput for AES of 60Mbps	X		X		

Access Router Requirements	Base	Upgrade	Small Site	Medium Site	Large Site
(4) Support 500 IPSec tunnels	X		X		
(5) Support 200 simultaneous flow-through VoIP calls to the PSTN over SIP	X		X		
(6) WAN IP packet forwarding of 150Mbps	X			X	
(7) Encryption throughput of 150Mbps	X			X	
(8) Support 1,000 IPSec tunnels	X			X	
(9) Support 1000 simultaneous flow-through VoIP calls to the PSTN over SIP	X			X	
(10) 4 integrated 10/100/1000 Ethernet RJ-45 ports	X			X	
(11) 12 ports for 10 Gigabit Ethernet	X				X
(12) 96 ports for Gigabit Ethernet	X				X
(13) DS0 4096 connections using channelized DS3 interfaces	X				X
(14) IPSec tunnels: 4000	X				X
(15) Unencrypted Traffic forwarding capacity: 16Mpps	X				X
(16) Unencrypted Traffic Forwarding of unencrypted traffic: 20Gbps	X				X
(17) DMVPN encryption and forwarding capacity: 6Gbps	X				X
(18) IP Version 4 routes supported: 4,000,000	X				X
(19) IP Version 6 routes supported: 2,000,000	X				X
(20) Number of ACLs supported: 16,000	X				X
(21) Number of active voice calls supported; 15,000	X				X
(22) Number of external video teleconference sessions supported; 2,000	X				X
(23) 1+1 hardware redundancy for power, processor, traffic forwarding, management and encryption function modules, (port interfaces do not need to be duplicated)	X				X
(24) Support for Ethernet MTU of 9000 bytes with Frames of at least 9018 bytes	X				X
i) Access Router Upgrades to provide VoIP Gateway and IP Video Conferencing Gateway and IP Video Conferencing Gatekeeper functions must support		X			
(1) H.323 basic gateway and gatekeeper functionality		X	X	X	
(2) Facilitate connectivity for different VoIP and Video services from other networks using H.323-to-H.323, H.323-to-SIP, and SIP-to-SIP protocols		X	X	X	

Access Router Requirements	Base	Upgrade	Small Site	Medium Site	Large Site
(3) Support for the transparent Codec to pass supported Codec types between the originating end point and the destination end point		X	X	X	
(4) CAC		X	X	X	
(5) Audio Codecs: G.711u; G.711; G.723; G.726; G.729; G.728; and internet Low Bitrate Codec (iLBC)		X	X	X	
(6) Transmission and transcoding for Codecs G.711 (a-law and m -law), G.728, G.726 (all versions), G.723 (all versions), G.729a, G.729ab (G.729a Appendix), G.729, and G.729b (G.729-AppendixB)		X	X	X	
(7) Scalable DSP resources for transcoding, voice and video conferencing traffic		X	X	X	
(8) Video Codecs: H.261; H.263; and H.264		X	X	X	
(9) DTMF support including G.711 Inband DTMF handling as per RFC 2833		X	X	X	
(10) ENUM E.164 number support as per RFC-2916		X	X	X	
(11) Fax pass-through		X	X	X	
(12) Modem pass-through		X	X	X	
(13) T.38 fax relay (flow-through)		X	X	X	
(14) VoIP and Video flow through where originating and destinations networks are hidden from each other		X	X	X	
(15) H.323 v4Compliance;		X	X	X	
(16) H.245 version 12 compliance		X	X	X	
(17) Exchange of video and T.120 data between H.323 call legs		X	X	X	
(18) Hardware and software based echo cancellation		X	X	X	
(19) SIP V2Compliance		X	X	X	
(20) QoS remarking of media traffic using ToS and DSCP		X	X	X	
(21) Low Latency Queuing		X	X	X	
(22) Link Fragmentation Interleaving		X	X	X	
(23) IPSEC between Voice and Video end point s		X	X	X	
(24) Authentication and authorization supported using available call information (ANI or DNIS)		X	X	X	
(25) Interoperability with Cisco Unified Communications Manager 7.0		X	X	X	
(26) SIP Digest Authentication		X	X	X	

Access Router Requirements	Base	Upgrade	Small Site	Medium Site	Large Site
(27) Class of restriction on dial peers to control incoming and outgoing calls to certain destinations		X	X	X	
(28) Host name validation using FQDN to validate incoming and outgoing calls		X	X	X	
j) Upgrades for Multi-Layer Switching must support		**X**			
(1) 24 1000BASE-T ports with PoE as per IEEE 802.3af	X		X	X	
(2) Automatic QoS for issuing global configurations commands to detect IP phones, classify traffic and allow egress queue configuration	X		X	X	
(3) LACP	X		X	X	
(4) IEEE 802.1s and IEEE 802.1w Rapid Spanning Tree Protocol and Multiple Spanning Tree Protocol	X		X	X	
(5) Per-VLAN Rapid Spanning Tree Plus	X		X	X	
(6) Weighted tail drop for congestion avoidance	X		X	X	
(7) Rate limiting based on: (i) source and destination IP address; (ii) source and destination MAC address; (iii) Layer 4 TCP and UDP information; or (iv) Any combination of the fields above, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps with bandwidth guarantees in increments as low as 8 kbps.	X		X	X	
(8) Forwarding rate: .5 Mpps	X		X	X	
(9) Number of MAC addresses supported: 6000	X		X	X	
(10) Number of VLAN Configured: 512	X		X	X	
(11) Number of VLAN ID Supported: 1000	X		X	X	
(12) VTP version 3 - VTP Server mode, VTP client mode and VTP transparent mode fully interoperable with existing VTP version 3 devices in the RCMP network	X		X	X	
(13) Support for Jumbo Frames up to 9216 bytes	X		X	X	
(14) Number of Unicast routes supported: 10,000	X		X	X	
(15) Number of IGMP groups: 800	X		X	X	
(16) 8 egress priority queues per port	X		X	X	
(17) VLAN trunks can be configured on any ports	X		X	X	

Access Router Requirements	Base	Upgrade	Small Site	Medium Site	Large Site
(18) IEEE 802.1q/p, CoS and DSCP marking, classification and reclassification based on: Incoming physical port; Source and destination IP address; Source and destination MAC address; TCP and UDP port number	X		X	X	
(19) ACL entries per input port for QoS classifications	X		X	X	
(20) QoS ACLs for marking traffic on all ports with no port performance degradation	X		X	X	
(21) Cisco Discovery Protocol version 1 and 2 or equivalent	X		X	X	
(22) Port-Based Network Access Control as per IEEE 802.1x interoperable with RADIUS for device authentications	X		X	X	
(23) IEEE 802.1X port-based authentication	X		X	X	
(24) IEEE 802.1X with port security	X		X	X	
(25) IEEE 802.1X accounting	X		X	X	
(26) Port-based ACLs for flexible per port security handled within hardware	X		X	X	
(27) MAC address notification to management systems	X		X	X	
(28) MAC address filtering, MAC Learning and Locking	X		X	X	

5.3 Data Centre Bridging

5.3.1) Data Centre Bridging Environment:

a) The current datacenter network performance may be enhanced to provide better throughput and latency to the servers in the datacenter. The Datacenter network connectivity will be largely based on Ethernet with Fiber Channel.

b) The Data Centre Bridging requirements are sub-categorized as:

(1) Core Data Centre Bridges used to connect multiple Access Data Center Bridges and high-speed capable devices; and

(2) Access Data Centre Bridges used to aggregate lower-speed devices and a variety of different protocols.

5.3.2) Datacenter Bridging Technical Requirements:

Datacenter Bridging Requirements	Base	Upgrade	Access	Core
a) Physical				
(1) Rack mountable in Standard 19" rack with standard AC 110V power	X		X	X
b) Ports				
(1) 1 Gigabit Ethernet standards including 1000BASE-T, 1000BASE-SX and 1000BASE-LX and LH interfaces	X		X	X
(2) 10 Gigabit Ethernet standards including 10GBASE-ER, 10GBASE-LR and 10GBASE-ZR interfaces	X			X
(3) 10 Gigabit FCoE, T11 standards compliant with FCoE (FC-BB-5)	X		X	X
(4) Fibre Channel ports supporting 8/4/2/1-Gbps Fibre channel connections including standard port types E and F and enhanced port types SD and TE	X		X	
c) Features and functionality				
(1) Layer 2 switch ports and VLAN trunks	X		X	X
(2) IEEE 802.1Q VLAN encapsulation	X		X	X
(3) Support for up to 256 VLANs and 32 virtual SANs (VSANs) per switch	X		X	X
(4) Per-VLAN Rapid Spanning Tree Plus (PVRST+)	X		X	X
(5) MSTP (IEEE 802.1s): 64 instances	X		X	X
(6) Spanning Tree PortFast and PortFast Guard or spanning tree edge ports	X		X	X
(7) Spanning Tree UplinkFast and BackboneFast or Per-VLAN Rapid Spanning Tree Plus (PVRST+)	X		X	X
(8) Spanning Tree Root Guard	X		X	X
(9) Spanning Tree Bridge Assurance	X		X	X
(10) Ethernet NIC teaming	X		X	X
(11) IGMP Versions 1, 2, and 3 snooping	X		X	X
(12) IGMP snooping querier	X		X	X
(13) EtherChannel technology or equivalent interoperable with existing RCMP deployments	X		X	X
(14) LACP: IEEE 802.3ad	X		X	X
(15) Advanced PortChannel hashing based on Layer 2, 3, and 4 information	X		X	X
(16) Jumbo Ethernet frames on all ports: 9216 bytes	X		X	X
(17) Pause frames : IEEE 802.3x	X		X	X
(18) Storm control (Unicast, multicast, and broadcast)	X		X	X
(19) Private VLANs	X		X	X
(20) Private VLANs over trunks	X		X	X
(21) IEEE 802.1Qbb PFC (per-priority pause frame support)	X		X	X
(22) IEEE 802.1ABDCBX Protocol	X		X	X
(23) IEEE 802.1Qaz: Enhanced Transmission Selection	X		X	X
(24) Intentionally left blank				
d) Fiber channel Features including				
(1) Fiber Channel over Ethernet		X	X	
(2) 10 Gigabit Ethernet ports configurable as FCoE		X	X	

Datacenter Bridging Requirements	Base	Upgrade	Access	Core
(3) SAN administration separate from LAN administration		X	X	
(4) Fibre Channel Protocol		X	X	
(5) Fibre Channel standard port types: E, F, and NP		X	X	
(6) Fibre Channel enhanced port types: TE and VF		X	X	
(7) Direct attachment of FCoE and Fibre Channel targets		X	X	
(8) 64 buffer credits per port		X	X	
(9) VSANs		X	X	
(10) Fibre Channel (SAN) PortChannel		X	X	
(11) Native Interop Mode 2		X	X	
(12) Native Interop Mode 3		X	X	
(13) VSAN trunking		X	X	
(14) Fabric Device Management Interface		X	X	
(15) Fibre Channel ID persistence		X	X	
(16) Distributed device alias services		X	X	
(17) In-order delivery		X	X	
(18) Port tracking		X	X	
(19) N-port virtualization		X	X	
(20) N-port identifier virtualization		X	X	
(21) Fabric services: Name server, RSCN, login services, and name-server zoning		X	X	
(22) Per-VSAN fabric services		X	X	
(23) DHCHAP and Fibre Channel Security Protocol (FC-SP)		X	X	
(24) Distributing device alias services		X	X	
(25) Host-to-switch and switch-to-switch FC-SP authentication		X	X	
(26) Fabric Shortest Path First		X	X	
(27) Fabric binding for Fibre Channel		X	X	
(28) Standard zoning		X	X	
(29) Port security		X	X	
(30) Domain and port		X	X	
(31) Enhanced zoning		X	X	
(32) SAN PortChannels		X	X	
(33) Fibre Channel traceroute		X	X	
(34) Fibre Channel ping		X	X	
(35) Fibre Channel debugging		X	X	
e) Management Features must support				
(1) Switch management using 10/100/1000-Mbps management or console ports	X		X	X
(2) CLI-based console to provide detailed out-of-band management	X		X	X
(3) SSHv2	X		X	X
(4) Telnet	X		X	X
(5) AAA	X		X	X
(6) RADIUS	X		X	X
(7) TACACS+	X		X	X
(8) Syslog	X		X	X
(9) Embedded packet analyzer	X		X	X
(10) SNMP v1, v2, and v3	X		X	X

Datacenter Bridging Requirements	Base	Upgrade	Access	Core
(11) Enhanced SNMP MIB support	X		X	X
(12) XML (NETCONF) support	X		X	X
(13) Remote monitoring	X		X	X
(14) AES for management traffic	X		X	X
(15) Unified username and passwords across CLI and SNMP	X		X	X
(16) CHAP	X		X	X
(17) Digital certificates for management between switch and RADIUS server	X		X	X
(18) CDP Versions 1 and 2 or equivalent	X		X	X
(19) RBAC	X		X	X
(20) SPAN on physical, PortChannel and VLAN interfaces	X		X	X
(21) Ingress and egress packet counters per interface	X		X	X
(22) Network Time Protocol	X		X	X
(23) Power-on self-test	X		X	X
(24) Comprehensive bootup diagnostic tests	X		X	X
(25) Call Home	X		X	X
(26) Redundant switched Ethernet out-of-band channels	X			X
(27) Smart Call Home	X		X	X
(28) SPAN on Fibre Channel interfaces	X		X	
f) QoS features must support				
(1) Layer 2 IEEE 802.1p (CoS)	X		X	X
(2) 8 hardware queues per port	X		X	X
(3) Per-port QoS configuration	X		X	X
(4) CoS trust configuration	X		X	X
(5) Port-based CoS assignment	X		X	X
(6) Configuration capabilities to mapping of QoS policies to multiple interfaces	X		X	X
(7) Intentionally left blank				
(8) Policed drop	X		X	X
(9) Per-port virtual output queuing	X		X	X
(10) CoS based egress queuing	X		X	X
(11) Egress strict-priority queuing	X		X	X
(12) Egress port-based scheduling capabilities including WRR	X		X	X
g) Security features must support				
(1) Ingress ACLs (standard and extended) on Ethernet and virtual Ethernet ports	X		X	X
(2) Standard and extended Layer 2 ACLs: MAC addresses, protocol type, source addresses, destination addresses	X		X	X
(3) Standard and extended Layer 3 to 4 ACLs: IPv4 and v6 addresses, ICMP, TCP source and destination, UDP source and destination	X		X	X
(4) VLAN-based ACLs	X		X	X
(5) Port-based ACLs	X		X	X
(6) Named ACLs	X		X	X
(7) ACL logging and statistics	X		X	X
(8) Time-based ACLs	X		X	X
(9) Optimized ACL distribution	X		X	X
(10) Data path IDS for protocol conformance checks	X			X

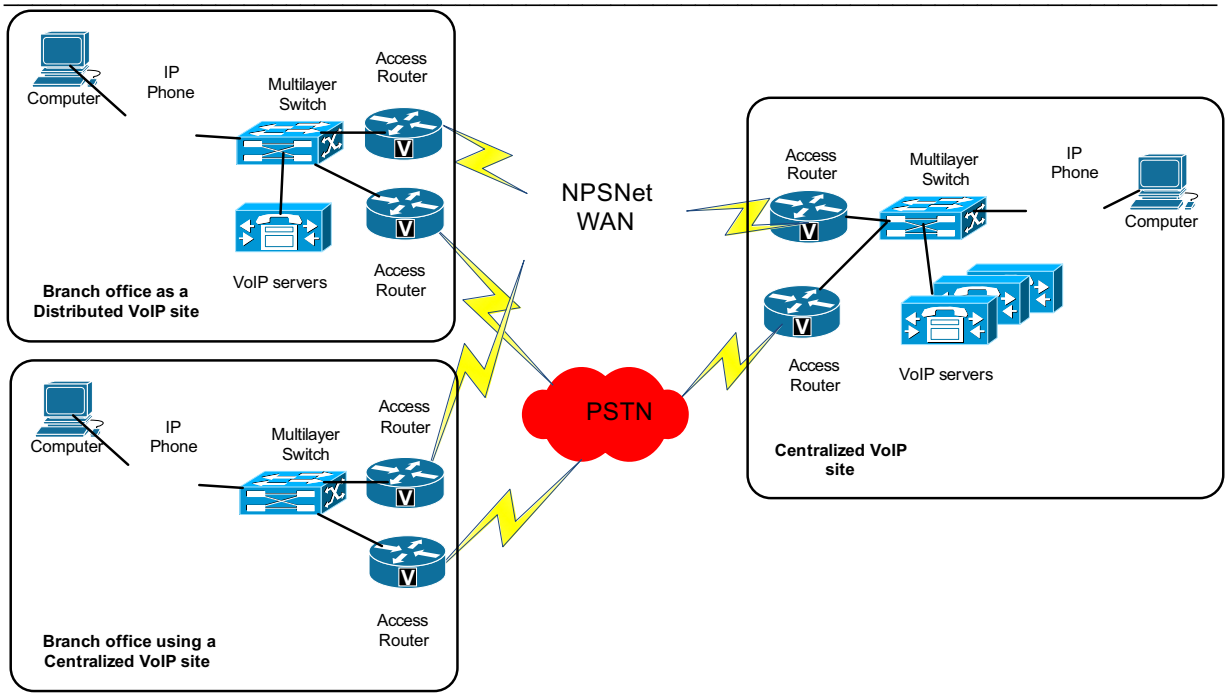
Datacenter Bridging Requirements	Base	Upgrade	Access	Core
(11) MD5 routing protocol authentication	X			X
(12) Integrated security features, DAI, DHCP Snooping, and IP Source Guard	X			X
(13) Policies based on MAC, IPv4 and IPv6 addresses supported by named ACLs (PACLs, VACLs, and RACLs)	X			X
(14) 802.1ae MAC Security on all ports		X		X
h) Routing and IP features must support				
(1) Static routing	X			X
(2) OSPF Protocol Versions 2 (IPv4) and version 3 (IPv6)	X			X
(3) Intermediate System-to-Intermediate System Protocol	X			X
(4) Border Gateway Protocol	X			X
(5) Enhanced Interior Gateway Routing Protocol	X			X
(6) Routing Information Protocol Version 2 (RIPv2)	X			X
(7) Virtual Route Forwarding	X			X
(8) DHCP Helper	X			X
(9) Unicast Reverse Path Forwarding	X			X
(10) Hot-Standby Routing Protocol	X			X
(11) Virtual Router Redundancy Protocol	X			X
(12) Gateway Load Balancing Protocol	X			X
(13) Enhanced object tracking	X			X
(14) Policy-Based Routing	X			X
(15) GRE tunneling	X			X
(16) Unicast Graceful Restart for all protocols	X			X
(17) Unicast Graceful Restart for OPSFv3 in IPv6	X			X
i) Capacity and Performance				
(1) Capacity of up to 40 ports for 10 Gigabit Ethernet;	X		X	
(2) Capacity of up to 12 ports for 10 Gigabit FCoE;	X		X	
(3) Capacity of up to 16 ports for Fibre Channel ports supporting combinations of 8/4/2/1-Gbps Fibre channel connections;	X		X	
(4) Capacity of up to 512 x 10 Gigabit Ethernet ports;	X			X
(5) Capacity of up to 768 x 1 Gigabit Ethernet ports;	X			X
(6) Capacity of up to 4 Virtual Device Contexts	X			X
(7) Virtual Port Channeling	X			X
(8) Capacity of up to 128K IPv4 forwarding entries in hardware;	X			X
(9) Capacity of up to 4,096 VLANs in hardware	X			X
(10) Scalable fabric up to at least 8 Tbps for forwarding performance	X			X
(11) Redundant, hot-pluggable power supplies and cooling fan modules	X		X	X
(12) Software and hardware support of distributed multithreaded processing on SMPs, multicore CPUs, and distributed line card processors	X		X	X
(13) Software and hardware support of offloading computationally intensive tasks to dedicated processors distributed across the line cards	X		X	X

Datacenter Bridging Requirements	Base	Upgrade	Access	Core
(14) Software and hardware support of modular processes are instantiated on demand, each in a separate protected memory space	X		X	X
(15) Online insertion and removal	X			X
(16) Subsystem In-Service Software Upgrades - allow selective system maintenance through individual patches without the need to restart the system or interrupt packet forwarding	X			X
(17) Process survivability- processes run independently; providing granular service isolation enabling independent patching and independent upgrading that does require a full device restart	X			X
(18) The capability to segment software, operating systems and hardware resources into virtual devices running as independent devices with assigned physical interfaces, routing tables, independent virtual route forwarding and independent device management	X			X

5.4 Voice Over IP (VoIP)

5.4.1) VoIP Environment

Figure 2 VoIP Environment



5.4.2) IP PBX server hardware and software that can be integrated on a single server or on multiple servers.

5.4.3) VoIP Technical Requirement is subcategorized into the following:

a) VoIP IP PBX Call Management requirements;

b) Messaging;

c) IVR (interactive voice response);

d) Music on Hold;

e) Emergency response

f) VoIP Gateway; and

g) VoIP Phones is sub-categorized based on the 4 types of IP phones.

5.4.4) VoIP IP PBX call management Technical Requirements :

VoIP IP PBX Call management Requirements	Base	Upgrade
a) General		

VoIP IP PBX Call management Requirements	Base	Upgrade
(1) Fully interoperate providing all the features and functionality of Cisco IP VoIP Manager V7.0 and the VoIP gateway functionality running on Cisco Access Routers	X	
(2) Call routing, signaling, and media control for an IP telephony deployment supporting all the functionality of the existing RCMP Cisco IP phones in the RCMP VoIP network	X	
(3) Communication systems call routing, signaling, and media control for voice conferencing and video conferencing that will interoperate with existing RCMP Cisco IP phones	X	
(4) Toll bypass to reduce or eliminate toll charges assessed by long distance and local carriers by transporting voice traffic across the enterprise intranet, LAN, metropolitan-area network (MAN), or WAN	X	
b) Must support		
(1) End-to-end interoperability with, analog phones, analog radio devices, fax machine connections, and PBX connections converted to IP VoIP traffic by existing VoIP Gateways implemented with voice-enabled CISCO access routers presently used at the RCMP	X	
(2) Marking and prioritizing traffic with advanced QoS mechanisms including RSVP, IP Precedence, and DiffServ Code Points	X	
(3) Call Control Signaling Supports: H.323 V1 and V2 and V3 and V4; MGCP 0.1 and 1.0; and SIP call control protocols	X	
(4) ITU standard voice codecs including G.711, G.729, G.729a/b, G.723.1, G.726, G.728, GSM, GSM-EFR, GSM-ER: These are standards-based technologies allowing transmission of voice across IP	X	
c) Call Management Functions must provide		
(1) Call management functions for IP phones in both centralized and distributed configurations	X	
(2) A web browser interface to perform administration tasks for IP phone users	X	
(3) Management tools to ease the mass administration of IP phones	X	
(4) Automatic re-route to PSTN when the VoIP network is congested	X	
(5) An auto-attendant	X	
(6) Reporting on Call Detail Records	X	
(7) 3-party Conference Call, Call Transfer, Call Hold, Call Forward on Busy, Call Forward on No Answer, Call Forward All Calls for IP phones	X	
(8) A PC desktop or web based user interface to access e-mail, voice, and fax messages	X	
(9) English or French user interface at the choice of the user	X	
(10) Options for text-to-speech module to read e-mail messages over the telephone	X	
(11) Web access to allow phone users to modify their own phone profiles;	X	
(12) Complementary bilingual software application (French and English) available to each licensed IP phone user that provides full control over features, outgoing calls and incoming calls for all IP phone types. Must be compatible with Windows XP, Windows Vista and Windows 7	X	
(13) Call forward to internal phones	X	

VoIP IP PBX Call management Requirements	Base	Upgrade
(14) Call forward to external phones (any PSTN number)	X	
(15) Call forward on busy	X	
(16) Call forward on no answer	X	
(17) Call forward on no answer, with variable ring count	X	
(18) Call pickup (unlimited groups)	X	
(19) Call transfer (Supervised and Blind)	X	
(20) Circular Hunt (ability to provide circular sequential hunting to the next available free line in a cluster of 3 or more lines)	X	
(21) Automatic Dial (One touch speed dial) available as either a software or hardware capability	X	
(22) Calling Line Identification on Inbound Calls	X	
(23) Call Hold - must be a system capability and available on phone	X	
(24) Option to block number display and name display on all outgoing calls (internal & external) on a per user basis	X	
(25) Ability to display information in French or English at preference of user	X	
(26) Disable outbound calls (all outbound calls)	X	
(27) Disable inbound calls (all inbound calls)	X	
d) Voice Mail user functions must support		
(1) Greetings (generic, personalized, and absence greetings)	X	
(2) Generic greeting available in both French and English	X	
(3) General voice prompts to calling party available in both French & English	X	
(4) Message copying	X	
(5) Message erasing	X	
(6) Message forwarding	X	
(7) Message listen	X	
(8) Message pause during playback	X	
(9) Message reply	X	
(10) Message review	X	
(11) Message fast forwarding and fast forward to end	X	
(12) Message fast rewinding and rewind to beginning	X	
(13) Message receipt confirmation	X	
(14) Message saving	X	
(15) Message send	X	
(16) Delayed message send (future delivery)	X	
(17) Message status (time and date stamp)	X	
(18) Message stamping (normal or urgent)	X	
(19) Name (record and search)	X	

VoIP IP PBX Call management Requirements	Base	Upgrade
(20) Visual message waiting notification to phone	X	
(21) Message notification using pager (option of all messages or priority messages only)	X	
(22) User Security code	X	
(23) Auto system backup, including all messages, personal settings	X	
(24) Notification of saved messages passing a user configurable expiration limit and mailbox full notifications	X	
(25) Voice messaging must provide the calling party the option to redirect call to an internal number (such as an attendant); if no answer, call reverts back to voice mail	X	
(26) Voice messaging must provide the option for a calling party to redirect call to an external number	X	
(27) Voice messaging must provide the ability to add and delete users and modify their profiles and features for any voice mail box	X	
(28) Voice messaging must provide the user administration the ability to set maximum minutes of recorded messages	X	
(29) Voice messaging must provide the user administration available in both French and English	X	
(30) Voice messaging must provide password activation and reactivation for individual voice mail boxes	X	
e) IP PBX must provide		
(1) A software application that allows configuration of all system functions and the attributes and settings associated with individual phones. This includes tools to manage telephone number assignments, dialing plans, voice mail box assignments, password management tools, and tools to improve the efficiency of telecom equipment and services including at a minimum: Least Cost Routing for interexchange voice services; toll denial; and NPA/NXX blocking	X	
(2) An application development suite, enabling the RCMP or 3rd parties to develop applications that can be delivered to IP phones , Type 2 and Type 3 at a minimum(phone types defined in section: Device category – VoIP – IP Phones)	X	
(3) A diagnostic tool for status information at a minimum including operational status, % utilization, alarm and event tracking for all of the VoIP server equipment and software infrastructure required to support IP telephony, excluding the IP phones	X	
(4) A diagnostic tool for view real time information about the availability of all leased and/or dedicated voice services including fiber, T1's, individual circuits, PSTN access services and 800 services.	X	
(5) Configuration and all the software options so that redundant servers can be configured to provide the ability to perform server reconfigurations while maintaining the continuous availability to receive and place new calls using the VoIP phone IP PBX	X	
(6) The capability to mark the CoS bits in the packets of IP Telephony data, to facilitate prioritization of voice and data traffic	X	

VoIP IP PBX Call management Requirements	Base	Upgrade
(7) The capability to apply DSCP bits for QoS on IP telephony traffic outbound from any given VoIP server.	X	
(8) DTMF dialing with Auto attendant, Voice mail, IVR and other CTI applications	X	
(9) Call Detail Capture (including originating and terminating phone number, time of day, date, facilities used, call duration) for PSTN and interexchange services	X	
(10) The ability to configure rules used by the systems for automatic route selection for efficient utilization of interexchange voice services, with rules that can vary according the class of service assigned to a given phone line (e.g., PSTN overflow may be denied to some users)	X	
(11) CLID supported on analog Central Office trunk lines and on ISDN PRI lines	X	
(12) A call manager server fail-over configuration that will fully restore service to all phones within 3 minutes	X	
(13) Conference Calling –3 party conferences must be supported from and to all IP phones	X	
(14) Ring Again (an internal phone encountering a busy condition on another phone, tie line or other system resource, can queue for access by dialing a code. When the busy condition ends, the system will connect to the waiting line)	X	
(15) The ability to intercept - Calls to non-working DID numbers and route to an intercept recording	X	
(16) The capability to remotely manage over an IP network. The VoIP PBX management systems must integrate or be accessible from existing VoIP PBX management systems for existing servers used at the RCMP for the existing VoIP deployment	X	
(17) Categorizing users into groups with like privileges (must be able to allow or deny access to on-net LD, off-net LD, on-net international LD, off-net international LD, operator-assisted LD, phone calling and credit card calling, Directory Assistance, and 611 repair) into Multiple Class of Service categories	X	
(18) Must fail-over to a back-up and redundant call server within 2 minutes, in the event of a call server failing. The alternate back-up and redundant call server must automatically activate with the same and complete set of operational capabilities, user preference settings and administrator settings as the failed server without requiring any user or administrator actions	X	
(19) VoIP IP PBX equipment and software must be capable of restoring full functionality to IP phones within 5 minutes, in the event of a call server fail-over without requiring any user or administrator actions	X	
(20) Uniform call distribution to a cluster of at least6 phones (ability to uniformly distribute inbound calls to a cluster of phones, where each phone has "logged-in" to system to identify it is ready to receive such calls)	X	
(21) Redundant processors and redundant AC power module for all VoIP IP PBX devices	X	
(22) Basic IVR and auto attendant system that will work in both DID environments and environments where number extensions to a single phone number may be used to identify the intended recipient	X	
(23) Voice messaging IVR must provide the ability to verbally sort through voice messages by name	X	

VoIP IP PBX Call management Requirements	Base	Upgrade
(24) Voice messaging IVR must provide the ability to respond to messages by name	X	
(25) Voice messaging must provide the ability for the creation of personal distribution lists	X	
(26) Voice messaging must provide the ability to perform user functions through a remote administration module the user can dial into	X	
(27) Voice messaging must provide real time diagnostic and utilization information on demand to the VoIP administrator	X	
(28) Voice messaging must provide alarm notifications for the failure of system components to the VoIP administrator and to the network management servers for the voice messaging servers	X	
(29) Voice messaging must provide LDAP directory integration and applications	X	
(30) Voice auto-attendant with two-tier front-end IVR menu (e.g., 1st tier for language preference (French or English), 2nd tier invites calling party, in preferred language, to dial desired extension number or alternatively, speak the name of the desired party)	X	
(31) Voice messaging must provide the ability to maintain a schedule of the availability of RCMP phone attendants, in order to avoid forwarding to an unavailable attendant	X	
***f)* VoIP IP PBX – Music On Hold component functionality must provide**		
(1) An application to provide music, from an IP connected audio source, to on-net and off-net phone calls placed on hold	X	
(2) Music to callers when their call is placed on hold, transferred, parked, or added to an ad-hoc conference	X	
(3) Music to callers connected through MGCP, SIP and H.323	X	
(4) The administrator with the ability to control content and use the on hold time to pass on messages to the audience to reduce the hang-ups	X	
(5) Accept RCMP conversion of content such as CDs and MP3 files to the MoH format 16-bit PCM WAV files	X	
(6) Support Unicast and Multicast transport s for transmitting the audio stream to the end devices	X	
(7) Separate MoH audio stream for each endpoint device when using Unicast transport	X	
(8) Integrating servers supporting MoH and Call Management requirements (for example must provide the ability to support Voice messaging and Call Management functions on same servers as MoH) with an option to deploy MoH on servers dedicated to the MoH functionality	X	
(9) The ability to generate audio streams in the following codec formats: (i) Wideband G.722 (ii) G.711 A-law or mu-law; and (iii) G.729 Annex A.	X	
(10) Support a minimum of 400 simultaneous MoH Unicast sessions with endpoints and at least 40 unique audio sources	X	
(11) Multicast sessions to at least 30,000 endpoints	X	

VoIP IP PBX Call management Requirements	Base	Upgrade
(12) A backup capability so that MoH functionality to a redundant server is maintained when the primary MoH server fails	X	
g) VoIP IP PBX – Emergency Response Functionality must provide		
(1) User configuration options for routing of VoIP emergency calls (911 calls) to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location	X	
(2) The capability to notify RCMP security personnel of an emergency call in progress and the caller's location based on Call Management Administrator configurable parameters	X	
(3) The hardware capable of supporting up to 30,000 user phones and up to 25 simultaneous (calls placed within a second) VoIP user emergency calls	X	
(4) Support the automatic location of IP phones by MAC or IP address. The Emergency Response solution must also support options for manually configuring location of IP phones by MAC or IP address	X	
(5) Route Emergency calls by location to a PSTN gateway capable of reaching the responsible PSAP for the caller's location	X	
(6) Provide a database solution to maintain street, building and floor location of every IP phone; to be managed by RCMP and capable of being linked to municipal 911 databases. The RCMP will supply the PSTN access facilities required for this capability	X	
(7) Ensure that the internal VoIP emergency calls (911 calls) are routed to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location	X	

5.4.5) VoIP Gateway Technical Requirements

VoIP Gateway Requirements	Base	Upgrade
a) General		

VoIP Gateway Requirements	Base	Upgrade
(1) The VoIP Gateway component functionality for integrating PSTN connectivity, legacy voices devices, dissimilar codecs and some form of redundancy and restoral functions must be deployable as enhancements added to the existing RCMP Access Router devices. VoIP devices will interoperate with the Access Router Device Category solutions and the existing RCMP Access Routers for providing the VoIP gateway functionality, including at minimum: (i) PSTN connectivity for IP phones to connect to external phones; (ii) Legacy voices devices for connecting legacy PBX's and phones directly to the RCMP IP network for communications with the VoIP solution; (iii) Communicating between devices using dissimilar codecs; (iv) Restoral and redundancy of local site IP Phone connectivity in case of network failure by routing calls over PSTN connections and offering Call Management capability directly on the Access Router so that IP Phones can continue to place and receive both external and external calls even when the central VoIP IP PBX is down.	X	

5.4.6) VoIP IP phone requirements

VoIP – IP Phones requirements	Base	Upgrade	Type 1 Phone	Type 2 Phone	Type 3 Phone	Type 4 Phone
a) General						
(1) SIP and/or SCCP capabilities which are fully interoperate and compatible with all the features and functionality of Cisco IP VoIP Manager V7.0 and the VoIP gateway functionality running on Cisco Access Routers	X		X	X	X	X
(2) Receiving power over the Ethernet cable from the wiring closet switch and must not require AC power at the user's office	X		X	X	X	X
(3) Phones must be IP phones. Other phone solutions with converters will not be accepted including analog or digital phones connected through TDM/IP adapters	X		X	X	X	X
(4) The administrator capability to deactivate the speaker phone feature on phones with full duplex speakerphone from a central location without installing new software or through the RCMP's existing VoIP Manager	X		X	X	X	

VoIP – IP Phones requirements	Base	Upgrade	Type 1 Phone	Type 2 Phone	Type 3 Phone	Type 4 Phone
(5) Upgrade configurations with accessibility features. These accessibility options could be from third parties that are interoperable with the OEM for the VoIP device category and do not need to be sourced from the VoIP OEM. These configuration upgrades must include at minimum equipment for: (i) Hearing-Impaired Accessibility Features; (ii) Acoustic Coupled TTY; (iii) Hearing Aid Compatible (HAC) Handset; (iv) Hearing Aid Compatible (HAC) Headset; (v) Vision-Impaired and Blind Accessibility Features; (vi) Audible voice-message indicators for phone status; (vii) Paging setup options for voice-message indications; (viii) Audible caller ID and call log; (ix) Audible access to call functions; and (x) Text to speech options		X		X	X	
(6) Name Display for calls from or on analog Central Office trunk lines and for calls from or on ISDN PRI lines	X		X	X	X	X
(7) Conference Calling - 10 parties internal & external	X		X	X	X	X
(8) Automatic station release (activates when handset is removed from cradle and call is not completed within 60 seconds; releases any common equipment and initiates a warble and howl to alert user that phone is off-hook)	X		X	X	X	X
(9) Passing the extension number in calling line ID for any internal on-net calls, regardless of whether originating phone has DID	X		X	X	X	X
(10) The capability to use a uniform 5-digit dialing plan from any RCMP IP phone to any RCMP IP phone	X		X	X	X	X
(11) The capability to use a uniform 7-digit dialing plan from any RCMP IP phone to any RCMP IP phone	X		X	X	X	X
(12) Phone device that device authentication through 802.1.x supplicant and 802.1x MD5-EAP						
(13) Capability to encode and decode traffic in conformance with the following Codecs: G.711a, G.711, G.729a, G.729b, and G.729ab	X		X	X	X	X

VoIP – IP Phones requirements	Base	Upgrade	Type 1 Phone	Type 2 Phone	Type 3 Phone	Type 4 Phone
(14) The generation of comfort noise based on configured VAD levels	X		X	X	X	X
(15) A Web-based personal assistant application that allows end users to define advanced call forwarding features (when and how they are to be contacted by calling parties), such as find-me follow-me capabilities. The Contractor must provide the Web-based personal assistant application hosted by one the VoIP servers	X		X	X	X	X
(16) Directed call pickup so that any phone will be capable of answering calls to any other phone by dialing an access code	X		X	X	X	X
(17) The Call Management administrator the ability to broadcast messages to all IP phones with LCD screens or other display screens	X		X	X	X	X
(18) The Call Management administrator the ability to configure call distribution to a cluster of at least 20 phones	X		X	X	X	X
(19) The Call Management administrator the ability for Uniform call distribution with two-tier front-end IVR menu (e.g., 1st tier for language preference (French or English); 2nd tier offers minimum 6 routing options depending on caller selection)	X		X	X	X	X
(20) The capability to display information on the phone in French or English as a user selected preference	X		X	X	X	X
(21) An electronic copy of manual for each IP phone, available in French and English	X		X	X	X	X
(22) The user the capability to block number display and name display on all outgoing calls (internal & external) on a per user basis	X		X	X	X	X
(23) The Administrator the capability to disable outbound calls (all outbound calls)	X		X	X	X	X
(24) The Administrator the capability to disable inbound calls (all inbound calls)	X		X	X	X	X
(25) The user with a Handset volume adjust capability	X		X	X	X	X
(26) Dual RJ 45 ports with Ethernet switch to allow PC to connect to LAN through the Ethernet switch in phone	X		X	X	X	
(27) The Call Management administrator the capability to disable the PC port on the Ethernet switch provided with the IP phone	X		X	X	X	

VoIP – IP Phones requirements	Base	Upgrade	Type 1 Phone	Type 2 Phone	Type 3 Phone	Type 4 Phone
(28) The capability to ensure that voice traffic from phone will not be adversely impacted by traffic from a PC connected to that phone including the ability to place Ethernet voice and data packets in separate IEEE 802.1q VLANs	X		X	X	X	X
(29) The capability to mark the Ethernet packets according to 802.1Q/p standards so that the RCMP network can prioritize the Voice traffic over the data traffic from the PC	X		X	X	X	X
(30) The capability to verify status and provide network information directly from the phones LCD display, including: (i) A display indicating model serial number; (ii) Ethernet MAC address of the device; (iii) Security configuration information; (iv) Current status of the devices and any error messages; (v) Network Quality information including: (A) Number of RTP packets received; (B) Number of RTP packets sent; (C) Average RTP packet jitter; (D) Maximum RTP packet jitter; (E) Bad RTP packets discarded by the IP Phone device; (F) RTP packets lost by the network; and (G) MOS score information.	X			X	X	X
(31) IEEE 802.3af Power over Ethernet (PoE) standards compliance and require less than 7 Watts of AC power per phone (without any upgrades installed on the phone)	X		X	X	X	
(32) Factory-installed X.509v3 certificates with the capability for the RCMP to remove the X.509v3 certificates and installing new certificates	X		X	X	X	
(33) AES-128 encryption and TLS device authentication for signaling traffic	X		X	X	X	X
(34) SRTP with AES-128 encryption for voice traffic	X		X	X	X	X

VoIP – IP Phones requirements	Base	Upgrade	Type 1 Phone	Type 2 Phone	Type 3 Phone	Type 4 Phone
(35) Capabilities for automatic configuration of IP addresses through DHCP as well options to configure a static IP address for some phones when required by the RCMP	X		X	X	X	X
(36) Auto configuration capabilities to allow the discovery of variable configuration parameters when enabled at the Ethernet switch. Presently the RCMP switches and Phones support CDP for this purpose. Auto configurations capabilities must cover the exchange of configuration information between the RCMP Ethernet Switches and the IP Phones for configurations parameters including the following: (i) IP Phone Capabilities discovery including followed by LAN speed and duplex discovery; (ii) IP Phone VLAN configuration; (iii) IP Phone Network policy; (iv) IP Phone PoE - Power discovery; (v) Support CDP or equivalent	X		X	X	X	X
(37) Personalized directories accessible from the IP Phone for each user. In addition, the IP Phone must provide options to integrate and access the corporate phone directory directly from the phone. The Call Management devices (as defined in 5.4.4 a) (1)) must provide users with a web application for configuring and storing personal contact information and phone numbers for at least 99 contacts per user. The personal directory must be accessible by users from their IP phone. The IP phone user must be capable of placing a call by using buttons on the phone to select a contact in the personal directory or in the corporate phone directory	X		X	X	X	X
(38) A phone stand with multiple positions to accommodate user preferences for positioning of IP Phone on user desktops	X		X	X	X	X
(39) Wall mounting configurations		X	X	X		
(40) A 1 phone line (one phone number) capable phone	X		X			
(41) A 2 line (2 phone number) capable phone, with LCD display, with full duplex speakerphone capability	X			X		
(42) One speed dial button	X		X	X	X	X
(43) Firmware updates as downloads to phones that can be updated by an administrator	X			X	X	X

VoIP – IP Phones requirements	Base	Upgrade	Type 1 Phone	Type 2 Phone	Type 3 Phone	Type 4 Phone
(44) An LCD screen enabling at least 6 lines of alphanumeric display	X			X	X	X
(45) A 48 character alphanumeric display, at a minimum;	X			X	X	X
(46) Visual display of the incoming caller list, logging of all calls including missed, received and placed calls to that phone accessible from the phone. The logging must provide caller id, date and time of the calls for 32 calls at a minimum.	X			X	X	X
(47) Context sensitive soft keys whose functions vary as calls are being set up or are in progress	X			X	X	X
(48) A display for Calling Name Identification on inbound calls	X			X	X	X
(49) A display for Calling Line Identification on Inbound Calls						
(50) A Query Time and Date display	X			X	X	X
(51) A visual Message Waiting Indication (could be message lamp or text message on phone)	X			X	X	X
(52) A hold button (soft or fixed key) to place calls on hold	X			X	X	X
(53) A speaker enabling on-hook dialling and handsfree listen-only mode	X			X	X	X
(54) Call Management application must provide a Web-based browser user access for user customization and configuration of IP Phone feature configurations	X			X	X	X
(55) The phone users the ability to configure vary ring volume and different ring tones	X			X	X	X
(56) A phone key to initiate connection to the Voice Message system	X			X	X	X
(57) The user the ability to call forward to internal RCMP phones	X			X	X	X
(58) The user the ability to configure the phone to call forward on busy	X			X	X	X
(59) The user the ability to configure the phone to call forward on no answer	X			X	X	X
(60) The user the ability to configure the phone to call forward on no answer, with variable ring count	X			X	X	X
(61) The user the ability to call pickup from phones in the same call group (unlimited groups)	X			X	X	X
(62) The user the ability to call transfer (Supervised and Blind)	X			X	X	X

VoIP – IP Phones requirements	Base	Upgrade	Type 1 Phone	Type 2 Phone	Type 3 Phone	Type 4 Phone
(63) The user the ability to Automatic Dial (One touch speed dial). Feature available as either a software or hardware capability	X			X	X	X
(64) A full duplex speaker phone with echo cancellation echo suppression and dynamic noise reduction to limit the impact of background room noise	X			X	X	X
(65) Support for wideband VoIP traffic conforming to the G.722 codec with adherence to TIA 920, including providing handset, headset, and speaker phone supporting wideband requirements	X			X	X	X
(66) The ability to call forward to external phones, with ability for the administrator to deny forwarding to Long Distance numbers based on configuration parameters	X			X	X	X
(67) The ability for Call Waiting with an audible alert received on a phone in use, indicating another party is calling; user has option of toggling between the current and new calling party	X			X	X	X
(68) The ability for Directed Call Park. A phone user must be able to park a call against another phone number by dialling that number plus a park code	X			X	X	X
(69) The ability to set the phone in Do Not Disturb (Make Set Busy) mode	X			X	X	X
(70) The user with the ability to setup Group Intercom calls (With an intercom line, a user can call the intercom line of another user, which auto-answers to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call. Users can use an intercom line to dial any other intercom line in the intercom partition, or the administrator can preconfigure the line to target an intercom line outside the intercom partition)	X			X	X	X
(71) The user with the ability to place a call in Consultation hold (able to place one call in a hold state, while placing another call to an internal or external party)	X			X	X	X
(72) A Last Number Redial function (allows the user to automatically redial the last party called)	X			X	X	X
(73) The ability for users and administrators to setup Call screening (selected incoming calls can be rejected or forwarded to a recording based on originator's CLID; used to screen nuisance callers)	X			X	X	X

VoIP – IP Phones requirements	Base	Upgrade	Type 1 Phone	Type 2 Phone	Type 3 Phone	Type 4 Phone
(74) Help functionality with user instruction displayed on the phone in the users language preference	X			X	X	X
(75) The ability for the setup of at least 5 Speed Dial keys on the phone when the phone is configured to support only one phone line	X			X	X	X
(76) A hearing aid compatible handset that meets the American Disabilities Act requirements		X		X	X	X
(77) A port to connect an industry standard headset jack to allow listening and speaking through a headset, without requiring removal of handset and without the need for a separate amplifier	X			X	X	X
(78) A key on the phone with the ability to Mute the microphone of the speakerphone	X			X	X	X
(79) The user the ability to access to personal and corporate directories through LCD screen	X			X	X	X
(80) Phones that interface with HTML based phone applications	X			X	X	X
(81) Phones that interface with XML applications	X			X	X	X
(82) LCD display contrast controls	X			X	X	X
(83) Automatic Hold (when user leaves one call to move to another, the original call is automatically placed on hold)	X			X	X	X
(84) A 6-line and 6 phone number capable phone, with LCD display, full duplex speakerphone, headphone capability	X				X	
(85) The ability to adding up to 24 or more additional phone lines (for a total of up to 30 or more phone lines)		X			X	
(86) The ability for the setup of at least 5 Speed Dial keys on the phone when the phone is configured to support only one phone line	X				X	
(87) Upgrade the phone with up to 24 programmable buttons at a minimum to facilitate common functions required by multiline phone attendants. This could be a separate model of Type 3 IP Phone specifically designed for attendant or could be expansion modules added to an existing Type 3 IP Phone		X			X	
(88) Multiple Call Hold capability. The IP phone display and buttons must provide visible means to know how many calls are on hold, the associated CLID and name display	X				X	
(89) Busy Line Verification capability so that an RCMP phone attendant can confirm that a given phone line is busy	X				X	

VoIP – IP Phones requirements	Base	Upgrade	Type 1 Phone	Type 2 Phone	Type 3 Phone	Type 4 Phone
(90) The ability to have a call placed on hold automatically return to the RCMP phone attendant within a pre-defined time interval specified by the administrator	X				X	
(91) The ability to place up to 5 calls on hold, where callers will hear music or other recording	X				X	
(92) The ability for Attendant Camp-On (inbound call that attendant forwards to a busy line is held on the busy line until it becomes free; the user of the busy line hears a tone to indicate a call is waiting; the user's call forward rules take precedence)	X				X	
(93) The ability to configure a cluster of multiple RCMP phone attendants, with load balancing (uniform call distribution) for incoming calls	X				X	
(94) Support for Extensible Markup Language (XML) services and Call Management XML functionality for IP Phones	X			X	X	X
(95) A conference room phone	X					X
(96) A phone handset, headset, and speaker phone supporting wideband VoIP requirements conforming to the G.722 codec with adherence to TIA 920	X			X	X	X
(97) A Mute capability to mute conversation from the conference phone for all attached microphones'	X					X
(98) Automatic Gain Control to adjust microphone sensitivity based on where participants are seated in the conference room, making conversations clearer for all participants	X					X
(99) The capability to add at least 2 additional remote microphones which can be connected to the Type 4 IP Phone up to 8 feet away		X				X
(100) At least one additional wireless remote microphone with a mute key		X				X
(101) A Mute key that flashes when Mute is active or some other visual indication on the phone whenever the Mute function is active. The Mute key, when activated must also mute any optional microphones connected to the Type 4 IP Phone	X					X
(102) Phone compatible with Ethernet devices supporting IEEE 802.3af PoE Class 3 and must support an option for a local AC-to- DC power supply	X					X

5.5 Radio over IP

5.5.1) RoIP Environment

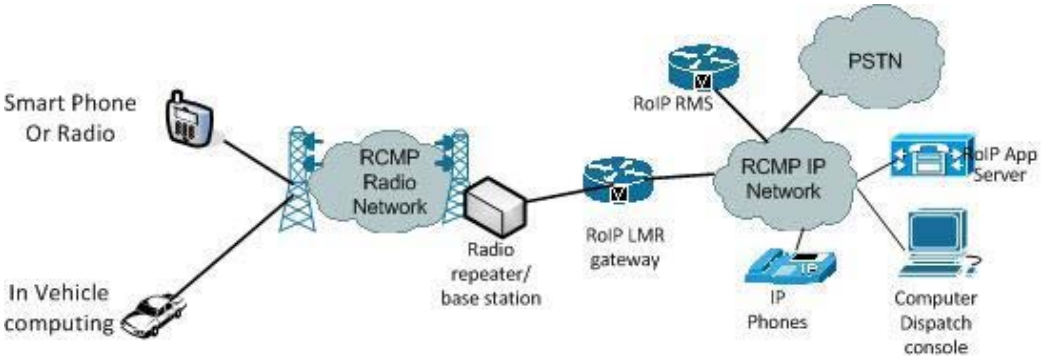
The major functional requirements of the Radio over IP environment are:

a) RoIP LMR Gateway converting transmission between the Radio networks to IP traffic for transmission on the RCMP IP network;

b) RoIP Application server managing the RoIP infrastructure including RoIP LMR gateways and RoIP Dispatch consoles; and

c) RoIP Dispatch consoles for RCMP Operational Communication Centre (OCC) Dispatch operators and other locations using RCMP radio network extensions over the RCMP IP network.

Figure 3 RoIP Environment



5.5.2) RoIP Requirement

a) The RoIP LMR devices must provide components with functionality that groups connection between Radio channels, radio broadcast channels, VoIP phones, PSTN phones and cellular Phones using the RCMP enterprise IP data network into a Channel Group so that communications from one participant is broadcast to all other participants. A Channel Group must broadcast audio conversation from any participant to all connected participants in the Channel Group. Any individual participants or endpoints in the Channel Group will be referred as a Channel regardless of the type of endpoint being used.

b) The RoIP LMR device components must all connect to the RCMP IP network using standard Ethernet cable to an IPv4 (TCP/IP) based network infrastructure.

c) The RoIP LMR devices must include functionality for encrypting and decrypting communications using the AES algorithm with a minimum bit length of 256 bits.

d) The RoIP LMR devices must include the capability to eliminate voice truncation of conversations caused by signaling in a Channel Group. This must include Channel Groups where there is a mix of Channel audio formats including analog audio, digital encrypted audio, digital unencrypted audio, conventional traffic or trunked traffic.

5.5.3) RoIP Technical requirements:

RoIP Requirements	Base	Upgrade
a) RoIP LMR - Gateway component Functionality		
(1) Provide connectivity to base stations and repeaters with a wired interface UTP connected to an E&M interface on the gateway that must: (i) Monitor for audio received from the E&M interface base stations and repeaters and convert that audio signal into VoIP traffic to be transmitted onto the RCMP IP network; (ii) Monitor VoIP traffic from the IP network to be converted to audio signals and transmitted to the base stations and repeaters over the E&M interface.	X	
(2) Convert audio received from the base stations and repeaters to a standards based VoIP codec for transmission over the RCMP IP network. The RoIP LMR gateway device must convert standards based VoIP codec from the RCMP IP network to audio signals to be transmitted to the base stations and repeaters	X	
(3) E&M Type II, III or V voice port signaling with support for both 2 wire and 4 wire connections to RCMP provided Radio base stations or repeaters supporting E&M interfaces	X	
(4) E&M voice port with audio and control signals entering and exiting the E&M port through an RJ-45 jack	X	
(5) Support for RFC 2833	X	
(6) E&M voice ports must support VAD signaling to determine when a signal is being received from the radio device and to begin sending VoIP packets on the designated multicast address	X	
(7) E&M voice ports must support configuration of the signal level thresholds in dBm to determine whether there is Radio traffic to be transmitted. When the signal level is below the noise threshold, the signal is classified as silent and no VoIP packets must be sent over the IP network. When the signal level is above or equals the noise threshold, the signal is classified as Speech or unknown and VoIP packets must be sent over the IP network	X	
(8) E&M voice ports must support COR and COS signaling	X	
(9) E&M voice ports must support tone radio control functionality. RoIP LMR Gateway device must use RFC2833 packets to send the corresponding inband tone control sequences using the configured frequencies to the Radio device connected to the E&M voice ports	X	

RoIP Requirements	Base	Upgrade
(10) Support radio communications using the following three phases of tone signaling: (i) Wakeup tone and HLGT—a tone of a specific duration and frequency that acts as a preamble to base stations to indicate that additional signaling is coming; (ii) Frequency selection (or control) tone and Function tone—one of a range of tones that is used to select a frequency (channel) for the audio; (iii) Guard tone and LLGT—A tone of a specific frequency that is maintained while there is activity on a channel. This tone indicates that the channel has been seized; and (iv) CTCSS —A tone of a specific frequency that is maintained while there is activity on a channel. This tone indicates that the channel has been seized.	X	
(11) Support the configuration of a timing delay before the voice packet is transmitted out E&M voice ports to avoid injected tone signaling from overwriting the voice packet	X	
(12) Support the configuration of signal level adjustments to properly balance audio signal levels for gain and attenuation	X	
(13) Interconnection for endpoints using IP multicast, Unicast and TDM based network connectivity	X	
(14) Support the functions required to combine two or more channel groups from RCMP IP phones and Radios including any Codec transcoding required	X	
(15) PTT interoperability with radio endpoints and any CISCO 7900 series IP phones used as endpoints	X	
(16) Configuration scaling up to a minimum of 12 E&M Interfaces	X	
(17) Interoperable with P25 and support P25 performance criteria for interoperability including at a minimum voice access times (as defined by TIA.102) of less than 480 ms	X	
(18) Be interoperable with P25 and support P25 performance criteria for interoperability including at a minimum voice access times (as defined by TIA.102) of less than 480 ms	X	
b) LMR - Application Server Component Functionality		
(1) Administrative functions including configuration authentication and security services for the integration of communications from RCMP IP phones and Radios over the IP network	X	
(2) Support RBAC user accounts	X	

RoIP Requirements	Base	Upgrade
(3) Support different security levels corresponding to different user roles. The server must support configuration of security levels for the following roles at a minimum: (i) The administrator security level has the ability for installing and setting up resources, such as servers, routers, multicast addresses, locations, and Channel Groups and has the ability to manage, monitor the activity logs, set up and manage users and user groups, granting access, assigning user channels, creating policies, managing policies and all the functionality of the dispatcher level; (ii) The dispatcher security level has the ability to set up channel groups, activating channel groups to begin conferences, and adding or removing participants in Channel Groups templates and active Channel Groups. This user level also monitors active Channel Groups and events and can mute and unmute users.	X	
(4) User accounts must be stored locally on the server	X	
(5) Configurable using a Web based GUI, which can be accessed remotely using HTTP or HTTPS	X	
(6) Intentionally left blank		
(7) Configuration file or directory that contains the entire RoIP solutions configuration in a single location.	X	
(8) Allow user, read, write and execute access to the configuration file or directory that stores the entire system configuration	X	
(9) Support RoIP system configuration file or directory being restored from a backup. The RoIP Application Server must resume operations based on the configurations settings contained in that file and directory after being restored	X	
(10) Redundancy in an active standby configuration. The redundant components must not share any of the loads and it must start operating only if active components fail. The active standby component must automatically switch over to active status within 5 seconds, should a failure of active unit occur. The RoIP Application Server must be able to support manual failover initiated by commands to switch from the active configuration to the standby configuration	X	
(11) No interruptions or communication degradation for users already connected through a RoIP Dispatch Console, should a RoIP Application Server failover occur	X	
(12) Recover to original operating state on a power cycle	X	
(13) Support access through a web based application using Internet Explorer release 6 or higher to perform all configuration requirements for enabling communications from RCMP IP phones and radios over the IP network	X	
(14) Configure, store, manage and operate the attributes of the RoIP configurations for the communications between the existing RCMP Radio networks, the RCMP IP network and the RCMP phones	X	
(15) Support adding, deleting, changing, enabling, disabling, viewing, and associating the different RoIP component attributes managed by the RoIP Application Server and required for the communications between the existing RCMP IP network and the RCMP IP phones	X	

RoIP Requirements	Base	Upgrade
(16) Store and manage information on the RoIP configurations for the following attributes: (i) Managing Channel Groups: (A) Channel Group details including Channel Group name; (B) Channel Group and Channel text description; (C) Channel Group and Channel security information; (D) Which users are allowed to use this channel; (E) Whether PTT Channel Groups can use this channel; (F) The status of the channel, the type of channel; (G) The location of the channel; (H) The multicast IP address and port to be used; (I) The codec to be used; (J) The Radio device to be used; (K) The channel selector for certain radio types; and (L) Status. (ii) Managing Radio configuration details including: (A) The name of the radio; (B) Radio text description; (C) The location; (D) The multicast address and port; (E) The codec; (F) The security associated with this radio configuration (G) The radio's descriptors; (H) The radio's tone control; (I) The voice delay also configured on the RoIP LMR Gateway; (J) The hangover time also configured of RoIP LMR Gateway;	X	

RoIP Requirements	Base	Upgrade
(K) The radio's serial control; (L) The radio's frequency channels; (M) The radio's channel selectors and control sequences with tone control; (N) The radio's channel selectors and control functions with serial control; and (O) Status. (iii) Managing Radio Descriptor configuration details including; (A) Predefined radio descriptor files in XML format; (B) Radio type name field; (C) Descriptor file name; (D) Descriptor type; and (E) Status information including file size, last update. (iv) Managing IP address Multicast Pool and any Multicast domains; (A) Managing parts of the RoIP LMR Gateway configuration information required for integration and interoperability; (B) Managing Client and device Licenses associated with the RoIP deployment; (C) Managing RoIP Dispatch Console configuration information; (D) Managing Media convergence resources; (E) Managing Active Users and Activity Logs; (F) Managing PTT setups; and (G) Managing security and privileges of users and clients.		
(17) Manage the RoIP Dispatch Consoles deployment and related tasks, such as installation, upgrade, display look&feel, and RoIP Dispatch Consoles configuration update activities over the IP network	X	
(18) Support the functions required to combine two or more Channel Groups in a PTT conversation	X	

RoIP Requirements	Base	Upgrade
(19) Reconfiguration, reboot, and software upgrade must not cause outages to operational RoIP RCMP systems or other network connected systems. An outage is considered to be any event that slows down, impedes the performance or renders ineffective the normal operation of RCMP systems that will share a common infrastructure with the system	X	
(20) Able to function in a primarily IP Unicast network environment with isolated IP Multicast island domains	X	
(21) Inter-connects to RoIP LMR Gateways through IP Unicast and/or multicast LANs and WAN	X	
(22) VoIP integration that will interoperate with the existing RCMP VOIP infrastructure which is Cisco Unified Call Manager	X	
(23) VoIP integration that will interoperate with the existing RCMP IP Phones which are Cisco model series 7900 phones, to call a device, to connect to channels and Channel Groups. This functionality must include the ability to receive and transmit voice data onto those Channels and Channel Groups through a PTT function	X	
(24) Intentionally left blank		
(25) VoIP integration application supporting H.323 and SIP protocols	X	
(26) Support G.729 CODEC algorithm for audio compression and decompression	X	
(27) Support G.711 CODEC algorithm for audio compression and decompression	X	
(28) Support IP Multicast technology	X	
(29) Able to connect to a variety of interoperable communication devices and systems through RoIP LMR Gateway including at a minimum the existing RCMP RoIP LMR Gateways implemented using a Cisco router equipped with E/M analog port module card such as a VIC3-2E/M	X	
(30) Support 500 concurrently active Channels	X	
(31) Support 50 concurrently active Channel Groups with up to 4 Channels per group	X	
(32) Support 50 concurrently active RoIP Dispatch Console sessions	X	
(33) Able to group together multiple Channels into one Channel Group where communications from a Channel is broadcast to all active Channels in the group	X	
(34) Support temporary Channel Groupings, created by an operator from the RoIP Dispatch Console application	X	
(35) Support the configuration of permanent Channel Groups, created by a system administrator from the system's management GUI	X	
(36) Remote access for management purposes through a TCP/IP network connection	X	
(37) Support a user initiating a connection by performing a PTT function on a device (radio or RoIP Dispatch Console) before the user's voice is transmitted on any channel or channel grouping	X	
(38) Interface synchronize the system time clock to an external GPS time reference and an external NTP time reference	X	

RoIP Requirements	Base	Upgrade
(39) Telephony interface that allows user dial-in system access from the PSTN. This telephony interface must require the use to enter a password	X	
(40) Support dial-in user options to choose any channel and channel groupings based on user's profile permissions	X	
(41) Support 20 concurrent dial-in telephone sessions	X	
(42) Capability to interface to a P25 ISSI system built by a different manufacturer	X	
(43) Support Reporting and Recording Requirements providing: (i) Real-time Channel Group status & presence reporting; (ii) Real-time status & presence reporting of all system users; (iii) Centralized archival and playback of system-wide recordings or must provide interface to inter-connect to a Centralized archival and playback system for system-wide recordings; and (iv) A log of system events and user activity.	X	
c) LMR Device – Application server Logging functionality		
(1) The RoIP Application Server must provide RoIP Logging Recording component functionality provided as part of the RoIP Application Server or as a separate device provided with every RoIP Application server	X	
(2) Real-time channel/channel grouping status & presence reporting	X	
(3) Real-time status & presence reporting of all users defined to the RoIP Application server	X	
(4) Interface to a centralized archival and playback of recordings	X	
(5) Keep a log of system events and user activity of all users and Dispatch consoles defined to the RoIP Application server	X	
(6) Able to report alarms based on classifications of minor, major and critical based on configurable severity for alarms. Alarms can be but not limited to Link Failed, Loss Of Signal, Power Failure.	X	
(7) Able to clear alarms	X	
(8) Able to monitor traffic end to end and provide logs	X	
(9) Capable of capturing traps and software errors with proper time stamps in such a way that they can be collected and analyzed by the RCMP	X	
(10) Method of logging all audio paths in unencrypted digital format on multiple hard drives simultaneously for the purpose of redundancy	X	
(11) Support 200 radio Channels.	X	
(12) Support 40 PBX and PSTN Channels.	X	
(13) Instant replays of any recorded conversations within five seconds.	X	
(14) Ability to create administrative user accounts that control access to RoIP Logging Recording functions.	X	
(15) Security functions must allow channel-specific security privileges.	X	
(16) Ability for any workstation client on the network with proper security privileges to play back audio or modify configuration of the RoIP Logging Recording device.	X	

RoIP Requirements	Base	Upgrade
(17) User interface with the ability to view and select recordings for playback according to date, start time, channel number and name, talkgroup alias, call type, call duration and call notations (capable of being edited).	X	
(18) User ability to search for calls across all archiving devices on the network	X	
(19) User ability to mix audio data from as many as eight Channels during playback	X	
(20) User with the following audio controls during voice playback: (i) Stop. (ii) Pause. (iii) Rewind. (iv) Fast Forward. (v) Restart.	X	
(21) User ability to create a repeatable loop inside a call segment	X	
(22) User ability to make a copy of the original recordings in wave format that can be played back or edited on standard, multi-media devices	X	
(23) User ability to configure each channel individually with any combination of the following record triggers: (i) Ring detect (ii) Off hook detect (iii) Activity detect (iv) VOX (v) Contact closure (vi) Continuous record	X	
(24) For keeping records of the dates and times of silent periods for non-event verification, the RoIP Logging Recording device must be able to represent silence in the original recordings in a form that does not consume space for silent audio	X	
(25) A naming convention for recordings that incorporates the date, time and channel number into the file name	X	
(26) Capability to interface with existing RCMP standard voice recording equipment for external permanent or archive storage including at minimum the Eventide VR778, VR725 and VR615	X	
(27) Permanent or archive storage that must be on a removable storage disk media	X	
(28) Method to allow the data to be exported to an external database	X	
(29) Automatic recovery and restoral at the last operating state after a power failure	X	
(30) Ability for multiple users to access calls simultaneously from a single recorder	X	

RoIP Requirements	Base	Upgrade
(31) The recording of radio Channel Group audio data must be stamped with all available P25 information pertinent to the transmission including: (i) Radio talkgroup ID and Alias; (ii) Time stamp; (iii) Date stamp; (iv) Duration; (v) Call Type; (vi) Unit ID and Alias; (vii) Console ID and Alias;	X	
(32) The recording of telephone audio data must be stamped with all available information pertinent to the communication including: (i) Time stamp; (ii) Date stamp; (iii) Duration; (iv) Call Type; (v) Incoming ANI and Automatic Location Information (ALI) information; (vi) Outgoing DTMF information; (vii) Trunk ID; (viii) Console ID and Alias.	X	
(33) Hard disk capacity to store at least 500 hours of voice and its associated data	X	
(34) Hard disk must be provided in a raid configuration and allow for hot swappable exchange of defective hard drives	X	
d) LMR Device - Dispatch Console component requirement functionality		
(1) Provide the interface that allows PTT audio communications. End-users, dispatch personnel, and administrators using the RoIP Dispatch Consoles must be able to simultaneously monitor and participate in one or more PTT Channels or Channel Groups at the same time	X	
(2) Support options for downloading the software for installation from a network connected server	X	
(3) Support up to 36 active Channels simultaneously on a Contractor provided Windows XP SP2, Windows Vista or Windows 7 professional editions network connected PC system with: (i) 3.2GHz Pentium 4 processor; (ii) 2 GB of RAM; and (iii) 1 GB of free hard drive disk space.	X	
(4) Support downloading RoIP configurations and information stored on the RoIP Application Server device to be used for managing the RoIP configuration assigned to this RoIP Dispatch Console login.	X	
(5) A display simulating the functions of handheld radios, buttons and screen user interfaces.	X	

RoIP Requirements	Base	Upgrade
(6) Must display the following controls and status indicators: (i) A PTT channel display button to click with your mouse and hold it to talk. When you are done talking, release the left mouse button to return to listen-only mode; (ii) A PTT channel button with status for Receive Indicator and Latch Indicator; (iii) A PTT channel button to indicate when RoIP Dispatch Console is in transmission mode; (iv) A display for initiating voice replay functionality to play back buffered voice transmissions and to view graphical representation of this functionality; (v) A button to increase or decrease the volume on the channel; (vi) A display to indicate current volume level on the channel in a graphical format; (vii) A connectivity indicator that specifies RoIP Dispatch Console connectivity status with the server; (viii) Online help functionality; (ix) A button to allow All Talk functionality to simultaneously talk on all of the Channels that RoIP Dispatch Console has selected; (x) Buttons to play out alert tones on one or more Channels selected; (xi) Buttons to activate and deactivate channels with indicators for active and inactive channel; (xii) Access to different radio views; (xiii) The ability to simultaneously monitor status of multiple Channels; (xiv) Buttons to interact and control the session with the RoIP Application Server; (xv) Using the PTT latch functionality, if you have user permissions configured in the server to simultaneously talk on several Channels.	X	
(7) Users must login to the RoIP Application Server which manages the login requests. The RoIP Application Server then must create a unique session identification that the RoIP Dispatch Console must use as its Identification	X	
(8) User must continue to operate in offline mode as long as the user has made one successful login to the RoIP Application Server even if the RoIP Application Server becomes unavailable. The RoIP Dispatch Console user must be able to log in to an alternate server.	X	
(9) When the RoIP Dispatch Console logs in to the RoIP Application Server, the server must download all of the currently available Channels that can be displayed for a particular RoIP Dispatch Console user to the consoles device according to the profile for that RoIP Dispatch Console log in. The RoIP Dispatch Console must receive configuration updates from the RoIP Application Server during the session.	X	

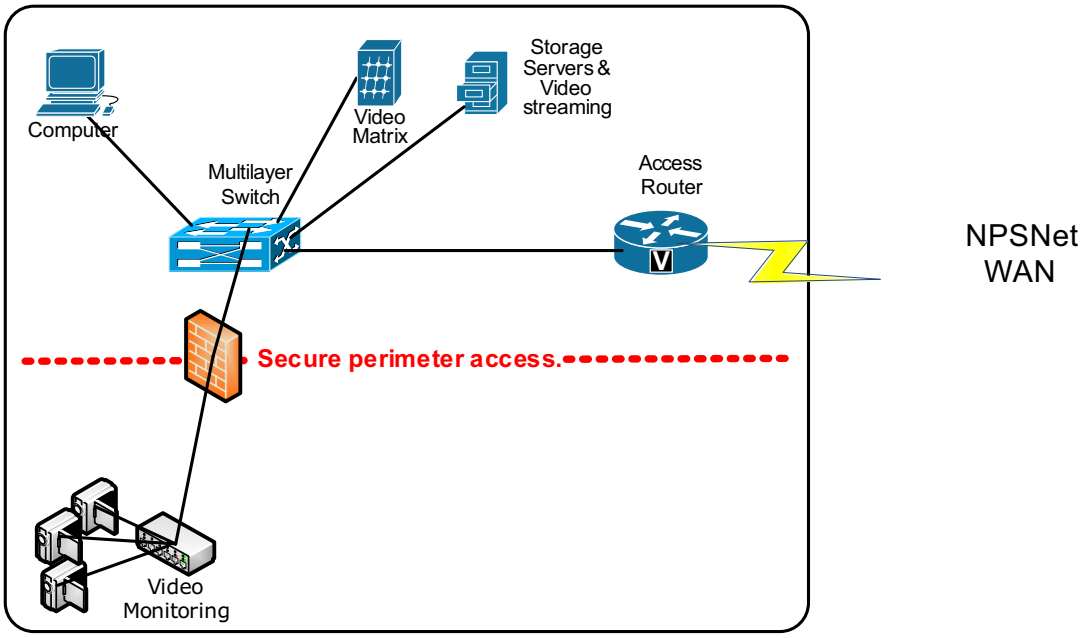
RoIP Requirements	Base	Upgrade
(10) Support sending RFC 2198 and RFC 2833 packets on a per-channel basis compatible with the RoIP gateway. The RoIP LMR Gateway must be able to understand the packet sent by RoIP Dispatch Console and convert them into audible tones and output to the physical radio through the E&M interface configured on the RoIP LMR Gateway.	X	
(11) Instant playback capability of the last 30 seconds of the last active conversation.	X	
(12) Channel and Channel Grouping traffic activity, through graphical indicators	X	
(13) Intentionally left blank		
(14) Capable of radio dispatching and telephone interconnect functions through the RCMP VoIP PSTN and PBX connected phones	X	
(15) Current PC based systems capable of connecting to the RCMP IP network through Ethernet	X	
(16) Operate independently of other RoIP Dispatch Consoles and must not be affected by the failure of other RoIP Dispatch Consoles.	X	
(17) Capable of both: external speaker and microphone operation; and headset earphone and microphone operation.	X	
(18) Support two Plantronics headsets (Model PLNH141) or an equivalent replacement with each device	X	
(19) Ability to connect two headset jacks to each RoIP Dispatch Console	X	
(20) Separate “operate” and “monitor” external speakers with individual volume controls with each dispatch console workstation	X	
(21) Route “operate” speaker audio to the headset earphone, during headset operation	X	
(22) Display must have a visual indicator on the display showing microphone audio being transmitted by the dispatcher	X	
(23) Display must show traffic activity on a channel or channel grouping, with graphical indicators. For example, a receive indicator that blinks green when traffic is received on a channel and channel grouping	X	
(24) Circuitry associated with microphone audio must provide headset microphone sensitivity level control to provide a steady transmit output level with microphone input variations that may range from nominal levels to 15 dB below nominal levels	X	
(25) Headset volume must be controlled independently from the speaker volume and include microphone side tone at a level of approximately 20dB below the receive audio for all microphone talk audio	X	
(26) Headset audio must not be capable of exceeding damaging sound pressure levels of 90 dBA in compliance with Canada Labour Code section 2	X	
(27) Foot and hand operated PTT switch		X
(28) Headset transmit microphone audio must only be routed to a dispatch console workstation radio resource when there is an active PTT	X	
(29) Audio circuitry must maintain a full duplex audio path to all connected radio resources, while maintaining an active PTT	X	
(30) Headset microphone and earphone audio must be connected in a full duplex manner without requiring an active PTT	X	

RoIP Requirements	Base	Upgrade
(31) Intentionally left blank		
(32) Able to monitor all Channels assigned to the workstation	X	
(33) Intentionally left blank		
(34) Display multiple pre-configured Channel groupings in a separate area of the dispatch console screen	X	
(35) Capable of creating new Channel Groups	X	
(36) Capable of removing Channel Groups	X	
(37) Support interfacing to 2 analogue phone lines that can be used for inbound and outbound dialing through the PSTN	X	
(38) Capable of activating and de-activating pre-configured Channel Groups based on operator necessity	X	
(39) Display with a graphical indicator to distinguish between active and inactive pre-configured Channel Groups	X	
(40) Capable of patching multiple Channels together and operating the new channel groupings as a single channel. The newly formed group channel will remain active until manually ungrouped by the operator	X	
(41) Capable of linking the visibility of predefined channel groupings to the RF channels that are currently on the main display		X
(42) Re-transmit, all inbound communications activity on a channel associated with a group channel, outbound to all the other Channels forming the group	X	
(43) Intentionally left blank		
(44) Intentionally left blank		
(45) Intentionally left blank		
(46) Intentionally left blank		
(47) Intentionally left blank		
(48) Intentionally left blank		
(49) Intentionally left blank		
(50) Support SSL Certificate or manual loading of encryption keys		X
(51) Support integration with the SSL Certificate or Tait Key Management Facility for AES 256 Key system programming		X
(52) Directory of phone numbers that are readily available to the operator or directory support within the pre-existing CUCM server platform.	X	

5.6 IP Video Monitoring

5.6.1) IP Video Monitoring Environment

Figure 4 IP Video Monitoring Environment



5.6.2) IP Video Monitoring Requirement:

IP Video Monitoring Device Requirements	Base	Upgrade
a) IP Video Monitoring Device Functionality		
(1) Real-time viewing and camera control	X	
(2) Support for the IP communications protocol	X	
(3) Multivendor interoperability (such as the use of multiple codecs and PTZ camera control)	X	
(4) Support video archiving to external servers	X	
(5) Video archiving at multiple locations (distributed and centralized models), frame rates, and durations	X	
(6) Disk compression for video files	X	
(7) Video monitor switching controlling video outputs to displays with software customizable triggers for security incident response	X	
(8) Bandwidth management approaches that reduce band integrate with the RCMP WAN	X	
(9) Provide IP Video Operations Center capability including: (i) Playback of local or remotely stored video archives (ii) Video archives capable of storing 2 terabytes of recorded video, at a minimum; (iii) Simultaneous local and remote live monitoring, recording, and viewing across multiple sites (iv) Local and remote control of IP Video Camera devices.	X	

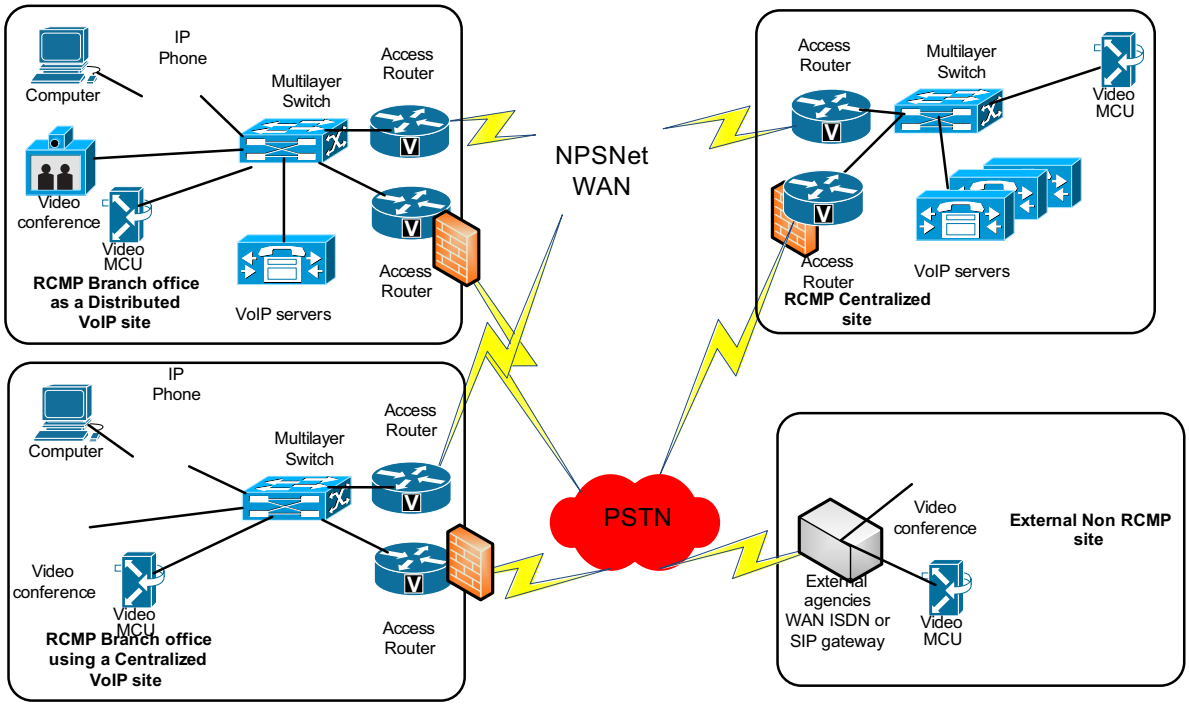
IP Video Monitoring Device Requirements	Base	Upgrade
(10) Support options for External cameras and connectivity capable of monitoring in many different external environments including options for monitoring in temperatures ranging from -30 Celsius up to 55 Celsius.		X
b) IP Video Monitoring Device Functionality		
(1) IP Camera devices providing, internal and external, PTZ and fixed camera devices designed to be used with the RCMP's complete end-to-end IP Video monitoring	X	
(2) An IP Video Operations Center capability which is a highly scalable solution allowing control of the centralized and distributed components enabling local and simultaneous remote monitoring, recording viewing and playback across multiple sites, regardless of geographical location	X	
(3) IP-Analog Transmitter and Receiver Integration solutions capable of providing conversion of Analog PTZ and fixed cameras to MPEG-4 and H.264 technology at a choice of resolutions for applications such as surveillance, identification and high speed movement	X	
(4) IP-Analog Alarm Panel Integration devices providing positive and/or negative triggered inputs which can generate events on the IP network to be used by Control Center solution to display video from specific cameras, move cameras to preset PTZ positions and dispatch emergency personnel	X	
(5) IP-Analog Alarm Panel Integration devices integrating external alarms and monitoring systems at a minimum supporting fire alarms, temperature alarms, intrusion alarms, motion alarms, door alarms	X	
(6) Mobile IP Video device/solutions for video monitoring and storage with mobile network connectivity for uploading stored video or live feeds using wireless network options when available	X	
(7) IP Cameras must include a suite of cameras with models to meet all requirements, including at a minimum	X	
(8) Indoor and outdoor PTZ cameras with the following resolutions (i) 1920 x 1080 (ii) 1280 x 720 (iii) 720 x 480/576 (iv) 704 x 480/576 (v) 352 x 240/288	X	
(9) Local and remote control of IP Video Camera devices	X	
(10) Pan, tilt, and optical zoom Camera devices		X
(11) PoE and capacity to power the camera from an electrical outlet	X	
(12) The wireless IP camera model must provide 1 X 2 MIMO communications. The wireless IP camera must provide strong wireless security using Wi-Fi Protected Access (WPA)/WPA2 and support various network protocols for 802.1x authentication	X	
(13) Automatic alerts, including video clips or still images, sent whenever motion is detected on the premises	X	
(14) The ability to view live video feeds from any Internet-connected PC or mobile phone	X	
(15) The ability to integrate alarms, door sensors, motion detectors, and other security systems	X	
(16) Support for low- and no-light environments	X	

IP Video Monitoring Device Requirements	Base	Upgrade
(17) An embedded microphone and speaker for two-way audio	X	
(18) Embedded security and networking with the camera providing 802.1X authentication and hardware-based AES	X	
(19) IP Multicast support for enhanced bandwidth management	X	
(20) Support True HD video	X	
(21) H.264 compression, streaming up to 30 frames per second at 1080p (1920 x 1080) resolution	X	
(22) Capture each frame at its entire resolution using progressive scan rather than interfaced video capture	X	
(23) Day/night functionality that includes an IR filter that automatically switches to night mode in low light scenes	X	
(24) Cameras that can be installed with a fixed mount	X	
(25) Cameras that can be installed with a an external pan/tilt mount and motorized zoom lens		X
(26) Minimum Illumination F1.4 @ 0.4 lux	X	
(27) Day and night operation cameras	X	
(28) Video Compression including H.264 and MJPEG	X	
(29) Audio Compression G.711 A-Law, G.711 U-Law	X	
(30) Video frame rates up to 30 fps at a minimum	X	
(31) Traffic prioritization through DSCP marking and 802.1p/q marking	X	
(32) User-definable detection areas with configurable sensitivities and thresholds to trigger e-mail alerts and FTP uploading of captured video or JPEG snapshots when a motion alert is generated	X	
(33) Variable Bit Rate settings for transmission	X	
(34) IP filtering	X	
(35) Graphical User interface for simplified access to captured videos and stills	X	
(36) Surveillance and management software	X	
(37) Browser based configuration management interface	X	

5.7 IP Video Conferencing

5.7.1) IP Video Conferencing Environment

Figure 5 IP Video Conferencing Environment



5.7.2) IP Video Conferencing Requirement

a) The Contractor must provide IP Video conferencing devices that will be interoperable with existing RCMP legacy video conferencing solutions and with the RCMP IP network technologies

b) The IP Video Conferencing devices must provide an ITU H.323 video conferencing solution. The H.323 functional elements will be referred to as:

c) IP Video Conferencing MCUs functionality responsible for actually connecting all video conference participants to the same conference;

d) IP Video Conferencing Gateways gateway functionality provides connectivity and translation services for older ISDN H.320 video conferencing endpoints so that they can join the same conferences as IP-based H.323, SIP endpoints;

e) IP Video Conferencing Gatekeepers providing the H.323 network a number of connection services for terminals, gatekeepers, and MCU devices; and

f) IP Video Conferencing terminals.

5.7.3) IP Video Conferencing Technical Requirements:

IP Video Conferencing device Requirements	Base	Upgrade
a) IP Video Conferencing Support		
(1) H.225 RAS, which is used between an H.323 endpoint and a Gatekeeper to provide address resolution and admission control services	X	
(2) H.225 Call Signaling, which is used between any two H.323 entities in order to establish communication	X	
(3) H.245 control protocol for multimedia communication, which describes the messages and procedures used for capability exchange, opening and closing logical Channels for audio, video and data, control and indications	X	
(4) RTP and the RTCP which is used for sending or receiving multimedia information (voice, video, or text) between any two H.323 entities	X	
(5) H.460 series which defines optional extensions that might be implemented by an endpoint or a Gatekeeper, including ITU-T Recommendations H.460.17, H.460.18, and H.460.19 for NAT and Firewall traversal	X	
(6) The H.239 standard that allows conference participants to share content in real time	X	
(7) Audio codecs: G.711 A-law and μ-law, G.729 (including G.729a), G.722, G.728	X	
(8) Video codecs: H.261 QCIF, H.263 (4CIF and 16CIF), H.264	X	
(9) IP Video telephony from desktops or laptops with the software and hardware required	X	
(10) Video communication systems based on the ITU, H.320 standard defining ISDN connection-based video communication and the ITU H.323 standard for packet-based multimedia communications over TCP/IP	X	
b) IP Video Conferencing Functionalities		
(1) Providing video conferencing for rooms ranging from 1 to 30 people.	X	
(2) Point-to-point using a single video terminal calling and another video terminal and point-to-multipoint using multiple terminals and multiple protocols (such as ISDN and IP, codecs G.711 and G.729).	X	
(3) Directory capable of dynamically adding terminals and other endpoints.	X	
(4) Centralized management systems providing management and monitoring for all IP connected end points including: (i) Terminals; (ii) MCUs; (iii) Gateways; and (iv) Gatekeepers.	X	

IP Video Conferencing device Requirements	Base	Upgrade
(5) Centralized management systems with the following functionalities: (i) View conference list and number of participants, participant information including name, number, IP address, video and audio codecs in use, and time joined the conference; (ii) Create a new conference and assign a conference password; (iii) Terminate a video conference; (iv) Add or drop participants in a conference; (v) Lock the video on a location to be viewed by all participants in a conference; (vi) Mute audio from a selected participant; (vii) Scheduling and call detail records of meetings; and (viii) On-screen menu for meeting selection.	X	
(6) Multiprotocol Support including H.323, SIP and H.320.	X	
(7) Connections between HD 1080p or 720p video terminals and Standard Definition video terminals end points.	X	
(8) Configuration options for transcoding and transrating for video codecs and connections between terminals connected at different speeds.	X	
(9) QoS support with DiffServ, ToS, and IP Precedence settings used to prioritize IP traffic.	X	
(10) Scale to support 200 video terminals, with 20 simultaneous conferences with 10 to 20 terminals in a conference.	X	

5.8 Wireless LAN

5.8.1) Wireless LAN Requirement

a) Requirements for wireless network access is divided in subcategories meeting the requirements for

(1) Wireless LAN access points for linking laptops and LAN devices; and

(2) Wireless controller for solutions with centralized security and management of wireless LANs;

b) Wireless LAN devices proposed must provide the RCMP with the unlimited right to copy the client side security supplicant onto all RCMP laptops.

5.8.2) Wireless LAN access points technical requirements

Wireless LAN Access Point Requirements	Base	upgrade
a) Device Wireless LAN Access Point Configurations must support		
(1) Flexible installation configurations models with options to provide Access point with any of the following installation types: (i) Wall; (ii) Ceiling; (iii) Above ceiling; (iv) Plenum; and (v) Intentionally left blank	X	
(2) CAPWAP or LWAPP	X	
(3) Wireless LAN Access Points must be compatible with the Wireless LAN Controller except for optional Standalone autonomous APs.	X	
(4) PoE support as per IEEE 802.3af	X	
(5) Integrated antennas for the 2.4GHz and 5 GHz bands	X	
(6) When running 802.11a/g provide connectivity at a bandwidth of 54Mbps with receive signal of -77dBm or better	X	
(7) When running 802.11n provide connectivity at a bandwidth of 300Mbps with receive signal of -68dBm or better	X	
(8) Dual Band Radios or dual band Access Points	X	
b) Features and Standards		
(1) 10/100/1000BASE-T as per IEE 802.3	X	
(2) Standards IEEE 802.11a, IEEE 802.11g and IEEE 802.11n	X	
(3) MSDU aggregation and MPDU aggregation	X	
(4) Multicast to Unicast conversion at the Wireless LAN Access Point for multimedia traffic	X	
(5) Obtains address from DHCP server as per RFC 2131	X	
(6) Radio certification compliant with RSS-210	X	
(7) Operating Frequency bands: (i) 2.412 to 2.462 GHz with 11 channels (ii) 5.18 to 5.32 GHz with 8 channels (iii) 5.5 to 5.75 GHz with 8 channels (iv) 5.745 to 5.825 GHz with 5 channels	X	
(8) Spectrum and transmit power management as per IEEE 802.11h	X	
(9) Adjustable transmit power settings	X	
(10) Intentionally left blank		
(11) Wireless operation in additional regulatory domains per IEEE 802.11d	X	
(12) VLAN support as per IEEE 802.1q	X	
(13) QoS support	X	
(14) MAC based	X	
(15) IEEE 802.1q/p based	X	

Wireless LAN Access Point Requirements	Base	upgrade
(16) WMM certification including WMM queue enforcement and Dynamic WMM Q management or standard WI-FI Alliance WMM certification	X	
(17) Voice Call Admission	X	
(18) Automatic Voice Prioritization	X	
(19) Intentionally left blank		
(20) DHCP support	X	
(21) Intentionally left blank		
c) Performance and Capacity		
(1) Setting Transmit power up to 100mW	X	
(2) Variable transmit power	X	
(3) 4x4 MIMO AP capable of 450Mbps at MCS23 and capable of 21 channels in the 5GHz spectrum.	X	
(4) 21 non overlapping channels	X	
(5) AP must be capable of supporting 200 MAC addresses for devices to be simultaneously associated and connected to an AP	X	
d) Security Features		
(1) WPA2	X	
(2) EAP TLS	X	
(3) Protected EAP	X	
(4) EAP TTLS	X	
(5) AES encryption	X	
(6) MAC address filtering	X	
(7) Compliant with IEEE 802.11i, including CCMP mode using AES	X	
(8) IEEE 802.1x.	X	
(9) AP Ethernet port must be configurable to use 802.1 x supplicants to authenticate to an existing Ethernet switch configured for 802.1x	X	
(10) Must provide the RCMP a client side security supplicant that supports the use of Entrust for the key management that runs on Windows 7, Windows XP and Windows 2000	X	
(11) Configuration with FIPS 140-2 certification or registered with NIST and in the process of being certified	X	
e) Management Features		
(1) Visual status of: (i) Device operating status; (ii) Ethernet port status and activity; (iii) Radio status and activity.	X	
(2) RJ45 Console port	X	
(3) TELNET as per RFC 854	X	
(4) Intentionally left blank		
(5) Intentionally left blank		
(6) Intentionally left blank		

Wireless LAN Access Point Requirements	Base	upgrade
(7) Intentionally left blank		
(8) Intentionally left blank		
(9) Authentications of 802.11 management traffic using digital signatures	X	
(10) Certifications including: (i) Safety - CSA 22.2 No.60950-1; (ii) EMI - ICES-003 Class A; (iii) RSS-210; (iv) UL 60950-1; (v) UL 2043.	X	

5.8.3) Wireless LAN Controller technical requirements

Wireless LAN Controller Requirements	Base	Options
a) Architecture Configurations		
(1) Dynamic channel assignment for downstream AP's	X	
(2) Dynamic downstream AP transmit power control	X	
(3) Radio interference management and avoidance	X	
(4) WLAN traffic load balancing – dynamically balances radio traffic between APs	X	
(5) QoS support	X	
(6) MAC based	X	
(7) IEEE 802.1q/p based	X	
(8) Seamless roaming	X	
(9) Seamless connectivity for users roaming across access points for both Layer 2 and layer 3 connected controllers	X	
b) Features and Standards		
(1) 10BASE-T as per IEEE 802.3	X	
(2) 100BASE-TX as per IEEE 802.3	X	
(3) Gigabit Ethernet 1000BASE-T/SX/LX as per IEEE 802.3		X
(4) Auto-negotiation of speed and duplex mode as per IEEE 802.3	X	
(5) Manual setting for speed and duplex mode as per IEEE 802.3	X	
(6) Full duplex mode, flow control as per IEEE 802.3	X	
(7) Ethernet prioritization and CoS as per IEEE 802.1q, IEEE 802.1p	X	
(8) VLAN Tagging as per IEEE 802.1q	X	
(9) Intentionally left blank		
(10) IP as per RFC 791	X	
c) Intentionally left blank		
d) Security Features	X	
(1) Security as per IEEE 802.1x	X	
(2) IEEE 802.11i compliance, including CCMP mode using AES	X	
(3) Intentionally left blank;		

Wireless LAN Controller Requirements	Base	Options
(4) Wireless LAN Controller based WIDS/WIPS must be able to detect and mitigate the following threats: (i) Rogue AP; (ii) Rogue client; (iii) Wireless ad-hoc network; (iv) 802.11 Dos; (v) RF interference	X	
e) Management Features		
(1) SNMP agent without using external proxy agents	X	
(2) Web based HTTP and HTTPS access	X	
(3) TELNET access	X	
(4) TFTP access	X	
(5) FTP access as per RFC 959	X	
(6) LED status indicators		
(7) CLI support	X	
(8) Wireless LAN management with a WLAN network management and planning system providing : (i) Centralized management of controllers and thousands of access points; (ii) Planning and design tools for optimizing AP location; (iii) Real time assessment and status of Wireless LAN infrastructure; (iv) Automated alarms; (v) AP wired port authentications with 802.11x; (vi) Displays interference from Wireless LAN devices and other devices; (vii) RF statistics; and (viii) Voice deployment monitoring tools for VoIP deployment over the Wireless LAN solution.	X	

5.9 Wireless IDS/IPS

5.9.1) Wireless IDS/IPS Requirement

a) Requirements for Wireless IDS/IPS are divided into 2 subcategories:

(1) Wireless IDS/IPS Sensors for passively observing Wireless LAN traffic and collecting forensics data about the wireless LAN transmissions; and

(2) Wireless IDS/IPS servers for centralized management and analysis of the observations and forensics data collected by the wireless IDS/IPS sensors.

5.9.2) Wireless IDS/IPS sensor requirements:

Requirement for Wireless IDS/IPS Sensor	Base	Options
a) Architecture		

Requirement for Wireless IDS/IPS Sensor	Base	Options
(1) Flexible installation options (mounting hardware for requested configuration included): (i) Ceiling; (ii) Above ceiling; (iii) Plenum; (iv) Outdoor, with or without the use of a supplier provided enclosure	X	
(2) Wireless LAN Sensor devices compatible with the Wireless IDS/IPS server	X	
(3) PoE support as per IEEE 802.3af,	X	
(4) Intentionally left blank		
(5) Integrated antennas for the 2.4GHz and 5 GHz bands: (i) When running 802.11a/g supporting connectivity at a bandwidth of 54Mbps with receive signal of -78dBm or better; (ii) When running 802.11n supporting connectivity at a bandwidth of 300Mbps with receive signal of -68dBm or better;	X	
(6) Dual Band Radios or Dual Band Access Points to support: both Wireless IPS/IDS Sensor and AP mode; or Wireless IPS/IDS Sensor only mode	X	
(7) Intentionally left blank		
b) Features and Standards		
(1) 10/100/1000BASE-T as per IEE 802.3	X	
(2) Standards IEEE 802.11a, IEEE 802.11g and IEEE 802.11n	X	
(3) Obtains address from DHCP server as per RFC 2131	X	
(4) Operating Frequency bands: (i) 2.412 to 2.462 GHz with 11 channels; (ii) 5.18 to 5.32 GHz with 8 channels; (iii) 5.5 to 5.75 GHz with 8 channels; (iv) 5.745 to 5.825 GHz with 5 channels.	X	
(5) Spectrum and transmit power management as per IEEE 802.11h	X	
(6) IP as per RFC 791	X	
(7) Wireless operation in additional regulatory domains per IEEE 802.11d	X	
(8) Intentionally left blank		
(9) Intentionally left blank		
(10) Intentionally left blank		
(11) Intentionally left blank		
(12) Intentionally left blank		
(13) DHCP support	X	
(14) Interface ports for connecting external antennas	X	
(15) Intentionally left blank		
(16) In Sensor mode must support detection of interference to Wi-Fi frequencies from other wireless devices including at a minimum cordless phones, Bluetooth headsets, wireless cameras and Microwaves.	X	
c) Performance and Capacity		
(1) Transmit power up to 23dBm	X	
(2) Bandwidth of 54Mbps up to 100 feet away and at –70dBm	X	
(3) 21 non overlapping channels	X	

Requirement for Wireless IDS/IPS Sensor	Base	Options
(4) Capable of supporting 200 MAC addresses for devices to be simultaneously associated and connected to an observed by the Wireless IDS/IPS sensor.	X	
d) Security Features		
(1) WPA2	X	
(2) EAP TLS	X	
(3) Protected EAP	X	
(4) EAP TTLS	X	
(5) AES encryption	X	
(6) Intentionally left blank		
(7) Compliant with IEEE 802.11i, including CCMP mode using AES	X	
(8) IEEE 802.1x	X	
(9) Intentionally left blank		
(10) Intentionally left blank		
e) Management Features		
(1) TELNET as per RFC 854	X	
(2) Intentionally left blank		
(3) Intentionally left blank		
(4) Intentionally left blank		
(5) Intentionally left blank		
(6) Intentionally left blank		
(7) Certifications including: (i) Safety - CSA 22.2 No.60950-1; (ii) EMI - ICES-003 Class A; (iii) UL 60950-1; (iv) UL 2043 or plenum rated certifications.	X	
(8) Visual status for the device operating status, Ethernet port status, Ethernet port activity, Radio status and Radioactivity	X	

5.9.3) Wireless IDS/IPS server requirements:

Requirements for Wireless IDS/IPS Server	Base	Options
a) Architecture		
(1) Full time wireless monitoring capabilities	X	
(2) Centralized management console	X	
(3) Hot-failover	X	
(4) Intentionally left blank		
(5) Forensic capabilities including: (i) Keep minute by minute logs of all connectivity that can be reviewed and searched; (ii) Intentionally left blank (iii) Options to allow full IP packet capture of connected devices.	X	
b) Management Features		
(1) Reports in PDF, HTML, CSV	X	

Requirements for Wireless IDS/IPS Server	Base	Options
(2) Ability to customize reports and provide the most common report types including Sarbanes Oxley, PCI, HIPAA	X	

ANNEX A Appendix A - Glossary of Technical Terms and Definitions

Term or Acronym	Definition
720P	720P is a category of HDTV. The number 720 represents 720 lines of vertical resolution
1080P	1080p is a category of HDTV. The number 1080 represents 1080 lines of vertical resolution and is sometimes referred to as full HD or true HD
1000BASE-SX/LX	Fibre optic gigabit Ethernet standards as per IEEE 802.3z
1000BASE-T	Gigabit Ethernet over copper wire as per IEEE 802.3ab
100BASE-TX	Fast Ethernet as per IEEE 802.3u
100V	100 volt AC
10BASE-T	Ethernet as per IEEE 802.3
10GBASE-LR/SR	Fibre optic 10 gigabit Ethernet standards as per IEEE 802.3ae
3DES	Triple Data encryption standard
3-wire (2PH+G)	AC power cord
AAA	AAA stands for authentication, authorization and accounting protocol
AC	Alternating current
Acceptance	The formal written acceptance by RCMP for Contractor deliverables (documents, demonstrations, equipment implementation, tasks, etc.)
Access Point	A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations
ACL	Access Control List
ActiveX	Microsoft-based technology was built to link desktop applications to the World Wide Web
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ANI	automatic number identification
AP	Access Point
ARP	Address Resolution Protocol
AVR	Automatic Voltage Regulation
BGP	Border Gateway Protocol
BNC	BNC (Bayonet Neill-Concelman) connector is a very common type of RF connector used for terminating coaxial cable
BOOTP	Boot Protocol A protocol used for the static assignment of IP addresses to devices on the network
BRI	Basic Rate Interface (BRI, 2B+D, 2B1D) is an Integrated Services Digital Network (ISDN) configuration
Business days	Monday through Friday not including statutory holidays
Business hours	Business hours will be 8:00am to 5:00pm in each time zone Monday to Friday
CA	Certificate Authority
CAC	Connection Admission Control
Call Park	Call park is a feature of telephone systems that allows a person to put a call on hold at one telephone set and continue the conversation from any other telephone set.

Term or Acronym	Definition
CAPWAP	The intent of the Control And Provisioning of Wireless Access Points (CAPWAP) protocol is to facilitate control, management and provisioning of WLAN Termination Points (WTPs) specifying the services, functions and resources relating to 802.11 WLAN Termination Points.
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code protocol
CDMA	Code division multiple access
CDP	Cisco Discovery Protocol
Channel	A participant in a Channel Group
Channel Group	Group connections between Radio channels, radio broadcast channels, VoIP phones, PSTN phones and cellular Phones into a Channel Group so that communications from one participant is broadcast to all other participants.
CHAP	Challenge Handshake Authentication Protocol
Chassis	The equipment's chassis is typically a standalone framework to which the modular components of the equipment are attached to be made functional by providing power, component communication, some status indicators and some management interfaces.
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CMP	Certificate Management Protocol
Codecs	Coder and DECoder algorithms. Standards for encoding and decoding digital streams and signals defined in different ITU standards for telecommunications such as G.7xx standards define packetized voice with different compressions and SNR optimization algorithms and H.2xx standards that define Video codecs.
Component	A related functional subset or part of the device that maybe made up of sub components itself.
Contractor	Any potential Contractor or Contractor that is submitting a proposal in response to this RFP.
COR	Carrier Operated Relay
CoS	Class of Service
COS	Carrier Operated Squelch
CSA	Canadian Standards Association
CSV	Comma separated variables
CTCSS	Continuous Tone-Coded Squelch System
Data Centre	Any site with data processing servers The two Enterprise Data Centres in Ottawa support RCMP mainframes, and are the main network concentration points for most of RCMP's remote site access requirement at this time
dBm	A ratio of decibels per milliwatt
dB	Decibels A unit for measuring relative power ratios in terms of gain or loss Units are expressed in terms of the logarithm to base 10 of a ratio and typically are expressed in watts
DES	Data Encryption Standard
DHCHAP	Diffie-Hellman Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DHTML	Dynamic HTML
Dictionary attack	A dictionary attack uses a targeted technique of successively trying all the words in an exhaustive list called a dictionary for defeating a cipher or authentication mechanism.
DiffServ	Differentiated Services
DLSw	Data Link Switching
DMVPN	Dynamic Multipoint Virtual Private Network
DN	Distinguished Name
DNIS	Dialed Number Identification Service
DNS	Domain Name System
DoS	Denial of Service. A type of network attack in which the goal is to render a network service unavailable

Term or Acronym	Definition
DS0	basic digital signaling rate of 64 Kbit/s
DS3	Digital Signal 3 (DS3) is a digital signal level 3 T-carrier sometimes referred to as a T3 with a data rate of 44.736Mbps.
DSCP	Differentiated Services Code Point
DSP	Digital Signal Processor
DSL	Digital subscriber line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances.
DSX3	DS3 cross connect
DTMF	Dual-tone multi-frequency signaling
DVMRP	Distance Vector Multicasting Routing Protocol
DWDM	Dense Wavelength Division Multiplexing (fibre optic communications)
E&M	Ear & Mouth is a type of supervisory line signaling that uses DC signals on separate leads, called the "E" lead and "M" lead, traditionally used in the telephone networks for voice transmission and signaling.
EAL-4	Evaluation Assurance Level – level 4 certification from a Common Criteria security evaluation
EAP	Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
Eastern Time	Eastern Standard or Eastern Daylight Savings Time in North America
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Electromagnetic Interference
EOL	End Of Life product life cycle
EOS	End Of Sale product life cycle
ESCON	Enterprise System Connection (IBM)
ESCON XDF	Enterprise System Connection (IBM) Extended Distance Feature
ESP	Encapsulating Security Payload. An IPSec protocol,
EtherChannel	Link aggregation providing
ETR/CLO	External timer reference/control link oscillator
EV-DO	Evolution-Data Optimized
Extended ACL	Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL
F1.4(F number)	For cameras, the focal length of the lens divided by the "effective" aperture diameter
FC 100	Fibre Channel at the rate of 100MBytes per second (1.0625Gbps)
FC 200	Fibre Channel at the rate of 200MBytes per second (2.025Gbps)
FCID	Fibre Channel ID
FCoE	Fibre Channel over Ethernet fault-tolerance and high-speed links between switches, routers and servers
FCP	Fibre Channel Protocol
FC-SP	Fibre Channel Security Protocol
FDMI	Fibre Device Management Interface
FECC	Far End Camera Control
FICON	Fibre Connectivity is a high-speed input/output (I/O) interface for mainframe computer connections to storage devices
FIPS-140-2	Federal Information Processing Standard 140-2(FIPS 140-2) is a standard that describes US Federal government requirements that IT products should meet for Sensitive, but Unclassified (SBU) use.

Term or Acronym	Definition
FOB	Under the terms of "FOB to destination", the title of the goods passes to the buyer when the goods arrive at their destination and the Contractors pays for the shipping costs of the merchandise.
FQDN	Fully Qualified Domain Name
FSPF	Fabric Shortest Path First
FTP	File Transfer Protocol
Fuzzing Attack	Attacks attempting to crash a device by sending it invalid messages.
FXO	Foreign eXchange Office
FXS	Foreign eXchange Subscriber/Station
G.*xxx*	ITU-T standards
GBIC	Gigabit Interface Converter that converts serial electric signals to serial optical signals and vice versa.
Gbps	Stands for billions of bits per second
GBytes	Stands for billions of bytes per second
GET	Group Encrypted Transport
GHz	Gigahertz. One billion cycles per second. A unit of measure for frequency
GLBP	Gateway Load Balancing Protocol
GOC	Government Of Canada
GRE	Generic Routing Encapsulation is a tunneling protocol
GTS	Generic traffic shaping
GUI	Graphical User Interface
H.*xxx*	ITU-T standards
H.323	ITU-T standard to address call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences on a packet network.
H.323 SIP	H.323 allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs, call set up and negotiating procedures, and basic data transport methods.
HD	High Definition
Help Desk	The Contractor’s first level technical support for reporting warranty of incidents.
HIDS	Host Intrusion Detection System
HLGT	High Level Guard Tone
HP OpenView	HP OpenView (a product from HP) is a tool RCMP uses to manage the network
HQ	Headquarters
HSPA	A collection of two cellular telephony protocols
HSRP	Hot Standby Router Protocol.
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTP GET	A Hypertext Transfer Protocol method
HTTP HEAD	A Hypertext Transfer Protocol method
HTTPS	Hypertext Transfer Protocol with Secure Sockets Layer (SSL)
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE 802.###	IEEE 802 refers to a family of IEEE standards about networking. IEEE stands for Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
ILMI	Integrated Local Management Interface
IMAP	Internet Message Access Protocol

Term or Acronym	Definition
Incident ticket	A record in the Contractor incident management system used by the Help Desk to track and record network equipment warranty incidents, any replacements and people involved in the investigations.
IP	Internet Protocol
IPComp	IP Payload Compression Protocol
IPS	Intrusion Prevention System
IPSec	Short for IP Security, sets of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement Virtual Private Networks (VPNs).
IPv4	IPv4 is version 4 of the Internet Protocol (IP) and it is the first version of the Internet Protocol to be widely deployed
IPX	Internetwork Packet Exchange
ISAKMP	Internet Security Association and Key Management Protocol (ISAKMP) is a cryptographic protocol which forms the basis of the IKE key exchange protocol
ISC, ISC-2, ISC-3	IBM's Intersystem channel protocol
ISDN	Integrated Services Digital Network
Isotropic	An antenna that radiates its signal 360 degrees both vertically and horizontally in a perfect sphere.
IS-IS	Intermediate system to intermediate system
ITU-T	International Telecommunication Union (ITU) Telecommunication standardization sector
IVR	Interactive Voice Response
JPEG	Joint Photographic Experts Group image compression
L2	OSI Layer 2
L2F	Layer Two Forwarding
L2TP	Layer 2 Tunneling Protocol
L2TPv3	Layer 2 Tunneling Protocol version 3
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	A light-emitting diode (LED) is a semiconductor device that emits incoherent narrow-spectrum light when electrically biased in the forward direction. LEDs are used as informative indicators in various types of systems
LLC	Logical Link Control (LLC) is the upper sublayer of the OSI data link layer
LLC2	Logical Link Control type 2
LLGT	Low Level Guard Tone
LMR	Land Mobile Radio
LOS	Line Of Sight
LQDR	Large Quantity Discount Request
Lux	Unit measure of illuminance and luminous emittance
LWAPP	LightWeight Access Point Protocol are specifications drafted by the IETF to create a standard protocol to be used by switches or routers controlling a group of IEEE 802.11 WLAN access points.
MAC	Media Access Control
MAN	Metropolitan Area Network
MITM(Man in the Middle) attack	Is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.
May	An action, which is discretionary.
Mbps	A megabit per second (Mbps or Mbit/s)

Term or Acronym	Definition
MCU	Multipoint Control Unit is a device commonly used to bridge videoconferencing connections.
MD5	MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function.
Metro	Metropolitan Area
MGCP	Media Gateway Control Protocol
MHSRP	Multigroup Hot Standby Router protocol
MIB	Management Information Base
MJPEG	Motion JPEG(Joint Photographic Experts Group) compression for images
MPEG-Audio& video	Moving Picture Experts Group or MPEG is a working group of ISO/IEC charged with the development of video and audio encoding standards
MPDU	Message Protocol Data Unit
MPLS	Multi Protocol Label Switching
MPOA	Multiprotocol over ATM
Mpps	On Million packets per second usually measured with 64 byte packets
MSDU	MAC Service Data Unit
MSTP	Multiple Spanning Tree Protocol
NAT	Network Address Translation
NBMA	non-broadcast multiple access
NCC	Network Communications access point in each building
NCR	Nation Capital Region (Ottawa)
NEBS	NEBS is the most common set of safety, spatial and environmental design guidelines applied to telecommunications equipment.
NEMA	National Electrical Manufacturers Association
NETBIOS	Network Basic Input/Output System
NETCONF	Is an IETF working group network management protocol -Network Configuration Protocol specified in RFC 4741
NetFlow	A set of applications to collect network statistics and export the data, perform data volume reduction, post-processing, and provide to end-user applications easy access to network statistics data
NFS,	Network File System
NHRP	Next Hop Resolution Protocol
NIC	network interface controller
NIPS	Network based Intrusion Prevention System
NNTP	Network News Transfer Protocol
NPIV	N-Port Identification Virtualization
NPSNet	RCMP National Police Services data network
NPV	N-Port Virtualization
NTP	Network Time Protocol
NVRAM	Non Virtual Random Access Memory
OEM	Original Equipment Manufacturer
OIR	Online Insertion and Removal
OSPF	Open Shortest Path First (protocol)
P25	Project 25 (P25) is a set of standards produced through the joint efforts of the Association of Public Safety Communications Officials International (APCO), the National Association of State Telecommunications Directors (NASTD), selected Federal Agencies and the National Communications System (NCS), and standardized under the Telecommunications Industry Association (TIA). The P25 suite of standards is to address interoperable solutions for digital Land Mobile Radio (LMR) services for communications between local, state/provincial and national (federal) public safety organizations and agencies.
PACL	Port-Based ACL
PAT	Port Address Translation

Term or Acronym	Definition
PBR	Policy Based Routing
PBX	Private Branch Exchange is a telephone exchange that serves a particular business or office
PC	Personal computer
PfR	Performance based routing
PIM	Protocol Independent Multicasting
Plenum	Enclosed spaces (in buildings) used for heating, ventilating, and/or air-conditioning airflow. Because ordinary cabling and equipment introduces a toxic hazard in the event of fire, special plenum equipment and cabling maybe required in plenum areas to meet safety standards.
PoE	Power over Ethernet technology is to transmit power along with data over standard network cables
POST	Power-On Self-Test
PPL	Product Price List
PPPoE	Point-to-point protocol over Ethernet is a network protocol for encapsulating PPP frames in Ethernet frames. It is used mainly with DSL services
PPTP	The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks.
PSTN	Public Switched Telephone Network
PTT	PTT (Push To Talk) is a method of conversing on half-duplex communication lines, including two-way radio, using a momentary button to switch from voice reception mode to transmit mode.
PTZ	Pan tilt zoom
Push To Talk	Push-to-talk , also known as Press-to-Transmit, is a method of conversing on half-duplex communication lines, including two-way radio, using a momentary button to switch from voice reception mode to transmit mode.
PVC	The permanent virtual circuit (or permanent virtual connection) is an ATM and Frame Relay terminology
PVRST+	Per VLAN Rapid Spanning Tree Plus
QoS	Quality of Service
RACL	Router-based ACL
RADIUS	Remote Authentication Dial-In User Service
Range	A linear measure of the distance that a transmitter can send a signal.
RAS	Registration, Admission and Status
RBAC	Role Based Access Control
RCMP	Royal Canadian Mounted Police
RCMP site	Any location where RCMP or partners employees are stationed and conduct business This is interchangeable with RCMP or partners premises and RCMP or partners controlled premises RCMP or partners does not necessarily own the building identified as the RCMP site
RCMP Technical Authority	The RCMP Information Technology Branch representative that is overall responsible for the technical aspects of the contract. This also includes any RCMP staff designated by the RCMP Technical Authority to act on its behalf
Ready For Use	The testing and verification of the equipment and services before they are used to carry RCMP's production data.
Receiver Sensitivity	A measurement of the weakest signal a receiver can receive and still correctly translate it into data.
RF	Radio frequency. A generic term for radio-based technology.
RFC####	A series of numbered Internet informational documents and standards
RFP	Request For Proposal

Term or Acronym	Definition
RIP	Routing Information Protocol
RIPv1	Routing Information Protocol version 1
RIPv2	Routing Information Protocol version 2
RJ-45	RJ-45 is used most commonly to refer to Ethernet-type connectors but also refers to the pin assignments defined in the wiring standard TIA/EIA-568-B used by a variety of electronic equipment.
RMON	Stands for Remote Monitoring. It is a standard used in telecommunications equipment
RMON-II	Stands for Remote Monitoring. It is an extension of RMON a standard used in telecommunications equipment
RPC	Remote Procedure Call
ROC	Requisition on Contract - A requisition or a request for delivery which is forwarded directly to a Contractor to obtain delivery of materiel from a previously negotiated contract
RoIP	Radio over IP
ROSS workstation	ROSS - RCMP Office Software System is the name of the platform for the computers that the RCMP has developed for its members based on the Novell LAN operating system.
RRS	RCMP Reliability Status
RSA	RSA is an algorithm for public-key encryption
RSCN	Registered State Change Notification
RSPAN	RSPAN stands for Remote Switched Port Analyzer
RSS-210	Radio Standards Specification (RSS) sets out requirements for the certification of licence-exempt (i.e. unlicensed) low-power radio communication devices.
RSS-Gen	General Requirements and Information for the Certification of Radio communication Equipment
RSSI	Received Signal Strength Indication
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource ReservationProtocol
RTCP	Part of the RTP Control Protocol
RTP	Real-time Transport Protocol
RX	Receive
SAA	Service Assurance Agent
SAN	Storage Area Network
SAP	A client/server enterprise application software company commonly used.
SCCP	Skinny Call Control Protocol
SCP	A protocol and the associated program for transferring files securely
SDLC	Synchronous Data Link Control
Session hijacking	The exploitation of a valid computer session to gain unauthorized access to information or services in a computer system by an unauthorized user taking over a session after some authentication has been completed with the appropriate permissions by a valid user.
SFP	Small Form Factor Pluggable interface for optical connections
SHA-1	A set of related cryptographic hash functions.
SIP	Session Initiation Protocol SIP equips platforms to signal the set-up of voice and multimedia calls over IP networks.
SIP	Session Initiation Protocol
SM	Single-Mode fibre
SMP	symmetric multiprocessors
SMTP	Simple Mail Transfer Protocol is the de facto standard for e-mail transmission across the Internet
SNA	IBM’s System Network Architecture
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SQL	Structured Query Language

Term or Acronym	Definition
SSH	Secure Shell or SSH is both a computer program and an associated network protocol designed for logging into and executing commands on a networked computer
SSH HELLO	Part of the Secure Shell protocol
SSL	Secure Sockets Layer
Standard ACL	Standard ACLs control traffic by the comparison of the source address of the IP packets to the addresses configured in the ACL.
STP	Spanning Tree Protocol
STUN	Serial tunneling
Supplicant	Part of the 802.1x architecture, - Software that runs on the PC / other devices attaching to the wireless network.
SYN flooding	A form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system
Syslog	Syslog is a de facto standard protocol for forwarding log messages in an IP network
T1	T-carrier is the generic designator for any of several digitally multiplexed telecommunications carrier systems. T1 represents a first level carrier with bandwidth of 1.544 Mbps (DS1) (24 DS0 Channels)
T3	T-carrier is the generic designator for any of several digitally multiplexed telecommunications carrier systems. T3 represents a third level carrier with bandwidth of 44.736 Mbps (DS3) (672 Channels)
TACACS	Terminal Access Controller Access Control System,
TACACS+	Terminal Access Controller Access Control System Plus
Tbps	Terabits per second (10^{12} bits per second)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TELNET	A protocol typically used to provide user oriented command line login sessions between hosts on the Internet. The name is derived from the words telephone network, since the program is designed to emulate a single terminal attached to the other computer.
TFTP	Trivial File Transfer Protocol
TimeServer	A timeserver is a computer networking device that reads the actual time from a reference clock and distributes this information to its clients using a computer network
TKIP	TKIP (Temporal Key Integrity Protocol, also known as WEP key hashing) defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key.
TLS	A cryptographic protocol which provides secure communications on the Internet
TN3270e	Is the remote-login protocol used by software that emulates the IBM 3270 model of mainframe computer terminals
ToS	Type of Service in the Internet Protocol Suite
Transmit Power	The power level of the radio transmission
TTR	Time to Resolve/repair an incident or equipment failure
TX	Transmit
UDP	The User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite
UNI	User-Network Interface is a demarcation point between the responsibility of the service provider and the responsibility of the subscriber
UNIX	Is a computer operating system
UPS	Uninterruptible Power Supply

Term or Acronym	Definition
URL	A Uniform Resource Locator (URL or, less formally, Web address) is a sequence of characters conforming to a standardized format, used for referring to resources (such as documents and images on the Internet) by their location, which is usually shown in the address bar at the top of a browser
uRPF	Unicast Reverse Path Forwarding
VA	Apparent power is conventionally expressed in volt-amperes (VA) since it is the simple multiple of voltage and current.
VACL	VLAN-based ACL
VAD	Voice Activation Detection
VCAT	Virtual concatenation is an inverse multiplexing technique used to split SONET/SDH bandwidth into logical groups, which may be transported or routed independently
VLAN	Virtual Local Area Network is a logically independent network. Several VLANs can co-exist on a single physical switch and cable
VoIP	Voice over Internet Protocol is the routing of voice conversations over the Internet or any other IP-based network
VOX	Voice operated transmit detection
VPC	Virtual Port Channel
VPN	Virtual Private Network is a private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
VSAN	virtual storage area network
WAN	Wide Area Network is a computer network covering a wide geographical area, involving a vast array of computers
WAP	Wireless Application Protocol (WAP) is an open international standard for applications that use wireless communication
WEP 128 bit	Wired Equivalent Privacy (WEP) is a scheme to secure wireless networks (Wi-Fi)
WFQ	Weighted fair queuing
Wi-Fi	A class of wireless local area network (WLAN) devices based on the IEEE 802.11 standards
WINS	Short for Windows Internet Naming Service, a system that determines the IP address associated with a particular network computer. This is called name resolution
WLAN	A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier: the last link with the users is wireless
WPA	Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi) computer networks
WPA2	Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi) computer networks
WRED	Weighted random early detection (WRED) is a queue management algorithm with congestion avoidance capabilities
WRR	Weighted Round Robin
WTD	Weighted tail drop
xDSL	Is a family of digital subscriber line technologies that provide digital data transmission over the wires used in the "last mile" of a local telephone network
XML	The Extensible Markup Language (XML) is a W3C-recommended general-purpose Markup language for creating special-purpose Markup languages, capable of describing many different kinds of data
XWindow	The X Window System (commonly X11 or X) provides windowing for bitmap displays. It provides the standard toolkit and protocol to build graphical user interfaces on Unix

ANNEX A Appendix B – Current Environment

1 Overview of Current Network

a) The RCMP existing data network called NPSNet (National Police Services Network) provides mostly data network connectivity to:

i) Over 1400 RCMP sites throughout Canada;
ii) Various other government agencies in support of GOC (Government of Canada) security;
iii) Security services at various locations throughout Canada (including embassies of other countries); and
iv) Online access to RCMP services for other police and security organizations.

b) The RCMP presently has other smaller more regional networks offering Radio, Voice and other more specialized network connectivity requirements that have traditionally not been suited to the RCMP NPSNet data network architecture. The RCMP plans are to converge these smaller networks into the RCMP NPSNet network as these smaller networks convert to IP based technologies.

c) The RCMP NPSNet network is centrally engineered and managed.

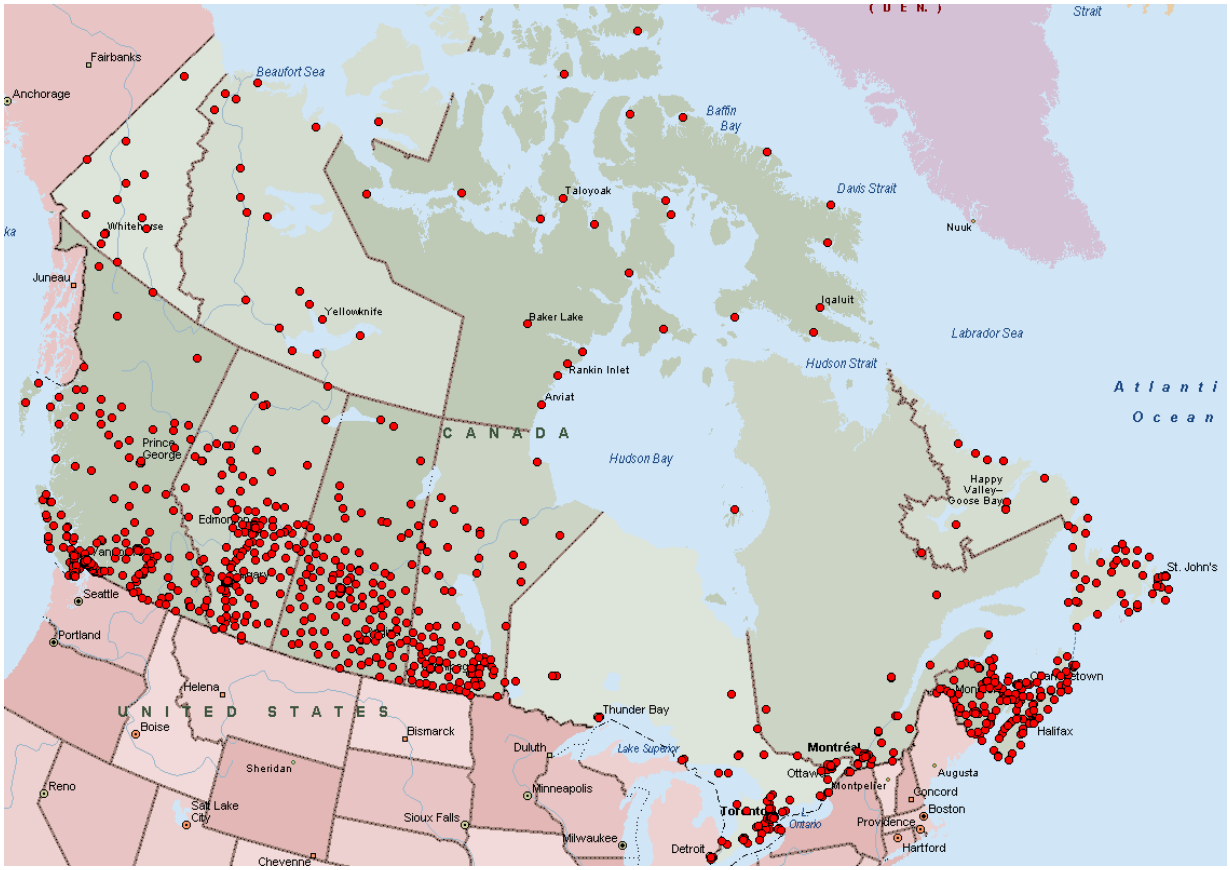
d) The RCMP's network infrastructure has been developed and improved over a number of years. Several networking protocols have been evaluated, standardized and implemented throughout the network equipment.

2 Current NPSNet Network

a) NPSNet consists of approximately 1,400 sites connecting mostly to the National HQ and a Divisional HQ within the same division.

b) NPSNet delivers principally a TCP/IP-based network for the National Police Services national data applications. The newer communications technologies deployed in NPSNet will support any site to any site networking with the capability to scale up to multimedia networking requirements. Certain locations and projects have already deployed Radio, Voice and Video over NPSNet as prototype projects. However presently most of RCMP Radio, Voice and Video requirements are deployed on networks that are independent of the existing NPSNet data network.

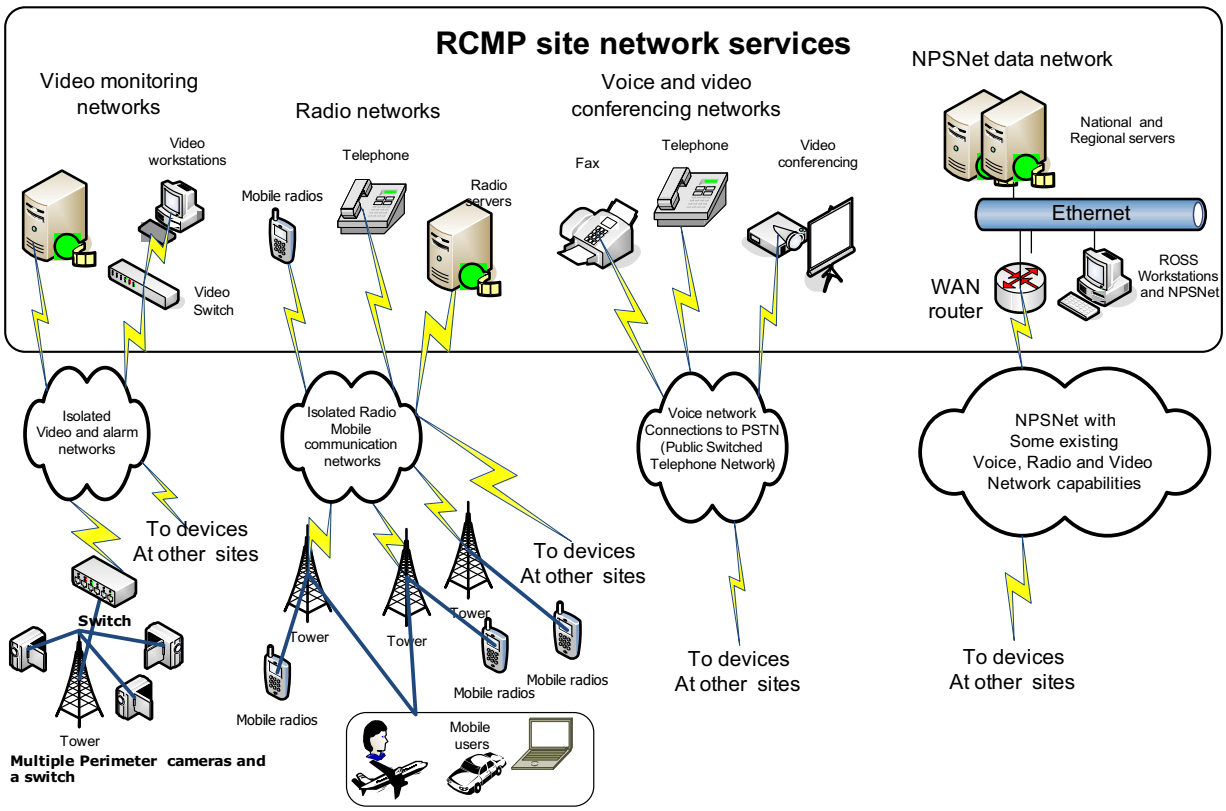
c) NPSNet Domestic Site Diagram:



3 **Current RCMP Site Networks**

a) Many RCMP sites presently have a disparate mix of multiple multimedia networks that are for the most part incompatible with the other networks at a site. These networks historically used technologies that were not interoperable and RCMP network integration opportunities' were limited.

b) Current RCMP site deployment diagram:



4 Current Access Router Environment

a) Small site routers

Approximately 1700 small site routers using mostly Cisco 2800 & 2900 models routers who are almost all at this point HSEC/K9 configurations. Software levels being run include the CISCO IOS's:

i) Advanced IP Services with crypto supporting AES encryption at level 12.4 or above; and

ii) Advanced Enterprise Services with crypto supporting AES encryption at level 12.4 or above.

b) Medium site routers

Approximately 100 medium site routers, models 3845 with HSEC/K9, VPN3/K9 and SRST/K9 configurations. Software levels being run include the CISCO IOS's:

i) Advanced IP Services with crypto supporting AES encryption at level 12.4 or above; and

ii) Advanced Enterprise Services with crypto supporting AES encryption at level 12.4 or above.

c) Large site routers

Approximately 80 large site routers using CISCO models including ASR 1000, ASR1002, 7604, 6509-E and 6513. Software levels being run include the CISCO IOS's:

i) Advanced IP Services with crypto supporting AES encryption at level 12.2 or above; and
ii) Advanced Enterprise Services with crypto supporting AES encryption at level 12.2 or above.

5 **Current VoIP Environment**

a) The table below indicates the servers supporting the RCMP's VoIP implementation.

Qty	Model Number	Description
1	MCS-7815I-2.0-EVV1	Cisco Call Manager PUB HW Only MCS-78151-2000 with P4 2.0 512MB RAM 40G HD
1	MCS-7815I-2.0-EVV1/S	Cisco Call Manager SUB HW Only MCS-78151-2000 with P4 2.0 512MB RAM 40G HD
1	MCS-7825H-2.4-ECS2	Cisco Emergency Responder MCS-7825 P4 2.266 1GB SDRAM 40GB ATA
3	MCS-7825H3-IPC1	Cisco Emergency Responder Server
1	MCS-7845H-2.2-CC1	Cisco Voice Mail Server MCS 7845-HP; UM-4HDD; RACK; 1GB; RAID 1 (2) DUAL C
7	MCS-7845-H2-CCX2	Cisco Call Centre server with 4GB RAM and four 72GB SAS HD
5	MCS-7845H2-K9-CMA2	Cisco Unified Communication Manager Subscriber
4	MCS-7845H2-K9-UCA1	Cisco Unity Connection Voice Mail Server

b) The software releases presently implemented include:

i) Cisco Emergency Responder 7.0
ii) Cisco Contact Centre Enterprise 7.0
iii) Cisco Unified IP Queue Manager 2.7
iv) Cisco Work Force Management 8.3.3
v) Cisco Unified E-Mail Interaction Manager 4.3.3
vi) Cisco Unified Communication Manager 7.1.3
vii) Cisco Unity Connection Voice Mail Server 7.1.3

c) Presently 3500 IP phones are implemented with server capacity, software and licenses to provide service to more than of 10,000 IP Phones.

d) Presently the VoIP for the National Headquarters pilot is running on multiple 3845s with an SRST/K9 configuration.

6 **WAN service conversion to MPLS**

a) Existing RCMP sites connected to the NPSNet will be converted to an MPLS network service to meet RCMP bandwidth upgrade and multimedia convergence requirements for:
   i) Upgrading bandwidth at Remote sites using a range MPLS access technologies including T1, xDSL and some Internet based broadband solutions;
   ii) Upgrading bandwidth for sites in core cities with computing requirements exceeding a T1's capacity; and
   iii) Sites with multimedia convergence requirements for Voice, Video, and Radio services will implement the appropriate IP MPLS services.

b) The new IP MPLS network services are deployed with the NPSNet network solutions, including:
   i) An IP Virtual Private Network (VPN) service for selected RCMP sites. The IP VPN is created through a Contractor provided IP Multi-Protocol Label Switching (IP MPLS) core network with scalable access technologies for the different site capacity requirements;
   ii) RCMP is deploying an RCMP managed router at each location to connect to the Contractor's IP MPLS through Ethernet and provide RCMP managed encryption using the Dynamic Multipoint VPN technology to encrypt all RCMP data being transmitted over the IP MPLS WAN; and
   iii) Additional network diversity is being implemented for high availability at the RCMP datacenters, divisional HQ sites and some large sites. RCMP routers are configured to use OSPF, BGP, EIGRP, MHSRP and NHRP routing to interface with the RCMP's NPSNet services and with other networks to provide the route diversity to all RCMP computing sites.

ANNEX B

EVALUATION AND BASIS OF SELECTION

For

Multimedia Network Convergence
Equipment and Support Services

For

Royal Canadian Mounted Police (RCMP)

Table of Contents

List of tables

1 General Information

1.1 Evaluation Procedures

a) Offers will be assessed in accordance with the entire requirement of the Request for Standing Offers including the technical and financial evaluation criteria. There are several steps in the evaluation process, which are described below. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Offeror has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel. Once Canada has determined that an offer is non-responsive, Canada may set aside that offer at any time during the evaluation process.

b) An evaluation team composed of representatives of Canada will evaluate the offers.

c) The evaluation team will determine whether each offer includes a valid Certification relating to the Set-aside Program for Aboriginal Business (Annex E - Offer Forms). Offers that do not include a valid Certification will be set aside.

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

e) Any elements of the RFSO with the words “must” or “mandatory” are mandatory requirements. Offers that do not comply with each and every mandatory requirement will be considered non-responsive and be disqualified. Offerors who fail to submit complete offers with all the information requested by this RFSO will be evaluated accordingly.

f) The evaluation process is subdivided into 5 phases:

1) Phase 1: Technical Evaluation;

2) Phase 2: Financial Evaluation;

3) Phase 3: Offeror Ranking;

4) Phase 4: Demonstration and Submission of Sample; and

5) Phase 5: Offeror selection.

g) In addition to any other time periods established in the Request for Standing Offers:

1) Requests for Clarifications: If Canada seeks clarification or verification from the Offeror about its offer, the Offeror will have 3 working days (or a longer period if specified in writing by the Standing Offer Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the offer being declared non-responsive.

2) Extension of Time: If additional time is required by the Offeror, the Standing Offer Authority may grant an extension at his or her sole discretion.

h) During evaluation, Canada will review the Bid Submission Form, the Joint Venture Offer Form and the OEM Certification Form and ensure they are complete (Annex E – Offer Forms).

2 Evaluation Phase 1 - Technical Evaluation

For convenience, the results of the evaluation of sections 2.2 - Technical Evaluation of Offeror Experience and Product Functionality and 2.3 – Technical Evaluation of Product Strategy will be rolled up by the evaluators using Tables 2 and 3. Tables 2 and 3 do not need to be filled out by Offerors – they will be used only by the evaluators. They do not contain any information that is not already set out in Tables 4 through 10.

2.1 Technical Evaluation of Products

a) The completed Substantiation of Technical Compliance Form (Annex E – Offer Forms), together with the completed Financial Tables without prices (Annex B Appendix A), both of which must be submitted with each offer, will be evaluated to determine whether they substantiate the responsiveness of the Products being offered with the mandatory requirements of this RFSO. With respect to the Substantiation of Technical Compliance Form, only the substantiation of compliance with the specific articles listed in that form will be evaluated.

b) The completed Pricing Table 1 – Components for Existing Products, together with the supporting documentation included in the offer, will be evaluated to determine whether:

1) the offeror has offered the Products listed in Pricing Table 1 – Components for Existing Products, in which case the offer will be technically compliant; or

2) the offer substantiates that each component for which a substitute has been offered is equivalent, in accordance with the requirements of this RFSO. The Offeror's offer will be deemed non-responsive if Canada determines that any component substitutions are not equivalent. The Offeror's offer will be deemed non-responsive if Canada determines that documentation provided is insufficient to determine that any substitution is equivalent to the required component.

c) Claims in an offer that a future upgrade or release of a product included in the offer will meet the mandatory requirements of the Request for Standing Offers, where the upgrade or release is not available on the closing date for submitting offers, will not be considered.

2.2 Technical Evaluation of Offeror Experience and Product Functionality

a) Canada has provided the Offerors with a series of tables concerning each Offeror's previous experience as well as end-user proof of the product's functionality. Canada will evaluate the completed tables submitted by each Offeror according to the scoring methodology set out in each table. Some requirements are mandatory and some requirements are rated.

b) Canada will evaluate the Offeror's previous experience working with OEMs in Table 4 of this Annex B. The Offeror must include a contact person employed with the OEM who can verify the information provided by the Offeror.

c) Canada will evaluate the functionality of the Products in similar end-user environments as the RCMP's in Tables 5 through 9 of this Annex B. The Offeror must include a contact person from the end-user who can verify the information provided by the Offeror. Where the requirement is for the end-user to have used the proposed Product, the Product does not have to be the exact product (same component identifier in the financial offer) offered but must be from the same Product Line (as defined in the RFSO under Extension of Existing Product Line). Canada reserves the right to determine whether an End-User's Product is from the same Product Line as the Product offered. For example, where the Product offered is the 4th generation of Product X, and the product in the End-User's environment is the 2nd generation of Product X, this falls within the definition of "same product line" and therefore the end-user reference will be accepted.

d) Even though it is the Offeror's responsibility to complete and submit the tables with its Offer, Canada may, at its discretion, verify any or all of the information provided in any of the tables with the contact person. Where Canada verifies any of the information, it will email a copy of the completed table and any required product information to the contact person at the OEM or end-user and verify any or all of the information with that contact person by e-mail (however, Canada may also, at its discretion, telephone a contact person,

if Canada determines that it will be easier to communicate in that way.) For verification, Canada will not award any points regarding the relevant table associated with that contact unless Canada receives the contact's response within 5 working days. On the third working day after sending out the email, if Canada has not received a response, Canada will notify the Offeror by e-mail, to allow the Offeror to contact its reference directly to ensure that it responds to Canada within the prescribed 5 day response time. Wherever information provided by a reference differs from the information supplied by the Offeror, the information supplied by the reference will be the information evaluated. Crown references will be accepted. Canada may contact references after receiving their responses to ensure they have properly understood the responses (and this follow-up does not need to occur within the 5 working days); however, if any reference does not respond to a follow-up within a reasonable period of time, Canada may contact the Offeror with a deadline for receiving a response from the reference.

e) In some cases, the Offeror can rely on several OEMs or end-users, by submitting one table for each. The maximum number that can be submitted is shown below. Submitting the maximum number is desirable, because it allows an Offeror to be awarded more points. Canada will evaluate the references in the order in which they appear in the offer, up to and including the maximum number of references as indicated in Table 2 (Evaluation Summary Table) of this Annex B. Any additional references will be disregarded. For example, if the Offeror provides information about 6 OEMs with whom it has worked for the first category below, only the first four will be evaluated.

f) Where more than one table is submitted for evaluation, each one must relate to a different OEM or a different end-user, as the case may be. "Different" means that the OEMs or end-users deal with one another at arm's length, and they are not affiliates or otherwise related entities. For example, for Table 5 (Access Router experience) of this Annex B, two tables can be submitted, for two different end-users. If an offeror submits one table about ABC Co.'s network and another table about ABC Co.'s parent corporation's network, only one of them will be evaluated, because they are not "different" end-users for the purposes of this requirement.

g) The following categories of experience will be evaluated:

1) Working with OEMs (Table 4 of this Annex B– Maximum of 4 can be submitted, each for a different OEM): The Offeror must demonstrate previous experience working with one or more OEMs in order to provide networking equipment to one or more customer(s). Offerors score more points if they:

A) have worked with multiple OEMs, increasing the breadth of their experience;

B) have more years of experience working with an OEM; and

C) have more experience in terms of a greater value of the OEM's products sold.

2) Access Router (Table 5 of this Annex B – maximum of 2 will be evaluated, each for a different end-user): The Offeror must demonstrate that the proposed OEM access router devices have been previously used in other end-user environments.

Points are awarded based on the characteristics of the end-user's network in which the Product was used. For the purposes of this table, it is not mandatory that the Offeror be the one who supplied or integrated the product to the end-user.

3) VoIP (Table 6 of this Annex B – maximum of 4 will be evaluated, each for a different end-user): The Offeror must demonstrate that the proposed OEM VoIP devices have been previously used in other end-user environments. Points are awarded based on the characteristics of the end-user's network in which the Product was used. For the purposes of this table, it is not mandatory that the Offeror be the one who supplied or integrated the product to the end-user.

h) RoIP (Table 7 of this Annex B – maximum of 2 will be evaluated, each for a different end-user): The Offeror must demonstrate that the proposed OEM RoIP devices have been previously used in other end-user environments. Points are awarded based on the characteristics of the end-user's network in which the Product was used. For the purposes of this table, it is not mandatory that the Offeror be the one who supplied or integrated the product to the end-user.

i) Video Monitoring (Table 8 of this Annex B – maximum of 2 will be evaluated, each for a different end-user): The Offeror must demonstrate that the proposed OEM Video Monitoring devices have been previously used in other end-user environments. Points are awarded based on the characteristics of the end-user's network in which the Product was used. For the purposes of this table, it is not mandatory that the Offeror be the one who supplied or integrated the product to the end-user.

j) Video Conferencing (Table 9 of this Annex B – maximum of 1 will be evaluated, each for a different end-user): The Offeror must demonstrate that the proposed OEM Video Conferencing devices have been previously used in other end-user environments. Points are awarded based on the characteristics of the end-user's network in which the Product was used. For the purposes of this table, it is not mandatory that the Offeror be the one who supplied or integrated the product to the end-user.

2.3 Technical Evaluation of Product Strategy

As set out in the RFSO, it is mandatory that Offerors propose only one OEM for each Device Category. However, in order to reduce interoperability and interconnection issues, Canada considers it desirable for the Offeror to offer all the Products (for all the Device Categories) from a single OEM. That is, Canada considers it desirable that the OEM whose equipment is proposed to be supplied for each of the Device Categories be the same, or that there be as few OEMs represented as possible. Offerors will be rated based on the strategy they adopt in terms of how many different OEMs' Products are proposed. The way in which this will be scored is set out in Table 10 of this Annex B.

3 Evaluation Phase 2 - Financial Evaluation

3.1 Financial Evaluation

a) SACC Manual Clause A0220T (2007-05-25), Evaluation of Price

b) The Financial Evaluation will be conducted by calculating the Total Offer Price using the Financial Evaluation Tables in Annex B, Appendix A - Financial Offer completed by Offerors. Instructions on how to complete the tables are included in Annex B, Appendix A – Financial Offer. Failure to provide complete pricing information as specified could result in the Offeror's offer being declared non-responsive.

c) If the pricing tables provided to offerors include any formulae, Canada may re-input the prices provided by offerors into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by an offeror.

4 Evaluation Phase 3 – Basis of Selection

4.1 Ranking of the Offerors

a) To be declared responsive, an offer must:

1) comply with all the requirements of the RFSO; and

2) meet all mandatory criteria

Offers not meeting 1) and 2) will be declared non-responsive.

b) The rating is performed on a scale of 3100 points.

c) The evaluation will be based on the highest responsive combined rating of technical merit and price. The ratio will be 25% for the technical merit and 75% for the price.

d) To establish the technical merit score, each responsive offer will be prorated against the highest evaluated technical points and the ratio of 25%.

e) To establish the pricing score, each responsive offer will be prorated against the lowest evaluated price and the ratio of 75%.

f) For each responsive offer, the technical merit score and the pricing score will be added to determine its combined rating.

g) To complete the calculation in c) through f) above, the following formula is used:

$$\frac{\text{Offeror's evaluated technical points}}{\text{Highest responsive evaluated technical points}} \times 25 = \text{(Total 1)}$$

$$\frac{\text{Lowest responsive evaluated price}}{\text{Offeror's evaluated price}} \times 75 = \text{(Total 2)}$$

(Total 1) + (Total 2) = Combined rating of technical merit and price

h) Neither the responsive offer obtaining the highest technical score nor the one with the lowest evaluated price will necessarily be accepted. The responsive offer with the highest combined rating of technical merit and price will be recommended for issuance of the Standing Offer.

i) The table below illustrates an example where all three offers are responsive and the selection of the supplier is determined by a 25/75 ratio of technical merit and price, respectively. The highest evaluated technical points equals 2,750 and the lowest evaluated price is $20,000,000 (20).

Table 1 Sample Calculation

Basis of Selection - Highest Combined Rating Technical Merit (25%) and Price (75%)			
	Offeror		
	Offeror 1	**Offeror 2**	**Offeror 3**
Overall Technical Score	1000	2600	2750
Offer Evaluated Price	$20M	$23M	$30M
	Calculations		
Technical Merit Score	1000/2750*25 = 9.09	2600/2750*25 = 23.64	2750/2750 *25 = 25.00
Pricing Score	20/20 * 75 = 75.00	20/23*75 = 65.22	20/30*75 = 50.00
Combined Rating	84.09	88.86	75.00
Overall Rating	**2nd**	**1st**	**3rd**

j) If an Offeror submits more than one responsive offer, only the highest-ranked offer will be considered for Phase 4 and Phase 5 of the evaluation.

k) If more than one Offeror is ranked first because of identical overall scores, then the Offeror with the best pricing score will become the top-ranked Offeror.

5 Evaluation Phase 4 - Demonstration and Submission of Sample

5.1 Demonstration

a) Canada may, but will have no obligation, to require that any of the 2 top-ranked offerors (identified after the financial evaluation) demonstrate any features, functionality and capabilities described in this RFSO or in its offer (including the requirements with respect to equivalency for certain components), in order to verify compliance with the requirements of this RFSO. The demonstration can include any of the requirements in Annex A, and is not limited to the ones identified in the Substantiation of Compliance Form. If required, the demonstration must be conducted, at no cost to Canada, at a location in Canada agreed to by the Standing Offer Authority. The Standing Offer Authority will provide no fewer than 10 working days of notice before the scheduled date for the demonstration. Once the demonstration has begun, it must be completed within 10 working days. Canada will pay its own travel and salary costs associated with any demonstration. Despite the written offer, if the Canada determines during a demonstration that the Offeror's proposed Product(s) does not meet the mandatory requirements of this RFSO (including the requirements with respect to equivalency for certain components), the offer will be declared non-responsive. Canada may, as a result of a demonstration, reduce the score of the Offeror on any rated requirement, if the demonstration indicates that the score provided to the Offeror on the basis of its written offer is not validated by the demonstration. The Offeror's score will not be increased as a result of any demonstration.

5.2 Sample

a) Canada may, but will have no obligation to, require that the top-ranked Offeror (identified after the financial evaluation) provide a sample of the goods that it has offered, to allow Canada to verify compliance of the Product(s) with any of the requirements of this RFSO or described in the offer (including the requirements with respect to equivalency for certain components.) If required, the sample must be delivered, at no cost to Canada, to a location specified by Canada, within 10 working days of the Standing Offer Authority's request. Despite the written offer, if Canada determines as a result of examining the sample that the Offeror's proposed product or solution does not meet the mandatory requirements of this RFSO (including the requirements with respect to equivalency for certain components), the offer will be declared non-responsive. The evaluation of the sample can include any of the requirements in Annex A, and is not limited to the ones identified in the Substantiation of Compliance Form. Canada may, as a result of examining the sample, reduce the score of the Offeror on any rated requirement, if the examination of the sample indicates that the score provided to the Offeror on the basis of its written offer is not validated by the examination. The Offeror's score will not be increased as a result of examining any sample.

6 Evaluation Phase 5 – Supplier Selection

6.1 Standing Offer Award Process

a) In order to be considered for award, an offer must:

1) comply with all the mandatory requirements of the RFSO; and

2) meet all the mandatory technical evaluation criteria; and

3) if requested, pass all of the requirements following the Demonstration of Proposal and submission of samples.

4) Offers not meeting 1), 2) or 3) will be declared non-responsive.

b) The Offeror that submits the compliant proposal that represents the highest responsive combined rating of technical merit and price will be recommended for Standing Offer award.

c) Whether any offeror is recommended for Standing Offer award depends on all the provisions of this RFSO (for example, the vendor performance provisions of the Standard Instructions would affect whether an otherwise responsive offer were recommended for award, as would factors such as financial capability.) Offerors must note that all Standing Offer awards are subject to Canada's internal approvals process, which includes a requirement to approve funding in the amount of any proposed Standing Offer. Despite the fact that the Offeror may have been recommended for Standing Offer award, a Standing Offer will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no Standing Offer will be awarded.

7 Technical Evaluation Tables

Table 2 Evaluation Summary Table

Evaluation Criteria	Min # of references required	Max # of references to be evaluated	Maximum points possible per reference	Total Maximum points possible	Total Marks Obtained
Mandatory Criteria (Table 3)	N/A	N/A	N/A	Pass or Fail	
OEM Reference (Table 4)	1	4	50	200	
Access Router Reference (Table 5)	1	2	200	400	
VoIP Reference (Table 6)	1	4	150	600	
RoIP Reference (Table 7)	1	2	500	1000	
Video Monitoring Reference (table 8)	1	2	50	100	
Video Conferencing Reference (Table 9)	1	1	200	200	
Total Number of Proposed OEMs (Table 10)	N/A	N/A	N/A	600	
TOTAL	**6**	**15**	**N/A**	**3100**	

Table 3 Mandatory Requirements

Mandatory Requirement	Met	Not Met	Page/Ref Number
1- Minimum number of references provided for each reference category as per Table 2 Evaluation Summary Table			
2- At least one of the Offeror's OEM references has previously contracted with the Offeror for at least two of the network equipment Device Categories defined in Annex A – Requirement (Table 4)			
3- The Offeror has been providing equipment from at least one OEM reference for a minimum of 1 year in the last 10 calendar years (since 2001) (Table 4)			
4-For at least one OEM reference, Offeror's annual sales, for a minimum of one out of the last ten calendar years (since 2001), must have attained $1Million. (Table 4)			

Table 4 Offeror OEM Reference Rated Requirements

OEM REFERENCE #: ____ **OEM REFERENCE Name:_____**			
General Information			
a) OEM Reference Information	Contact Name:		
	Telephone Number:		
	Email Address:		
b) Type(s) of network equipment from the OEM that is provided by the Offeror			
c) Name and Number of Device Categories defined in Annex A – Requirement (8 device categories) for which the OEM has previously contracted with the Offeror.	2+ categories – category names: _____ _____ _____ 1 category – category name: _____ 0		
Rated Requirements			
Description	**OEM Reference**	**Score**	**Ref page**
d) Number of years the Offeror has been providing equipment from the reference OEM in the last 10 calendar years (since 2001) (mandatory minimum of 1 yr)	Equal to or greater than 3 years	25	
	Equal to or greater than 2 years and less than 3 years	10	
	Greater than 1 year but less than 2 years	5	
	1 year	0	
e) Total annual sales value of reference OEM equipment sold by the Offeror (mandatory minimum of $1Million once in the last ten years)	Calendar year: _____		
	Equal to or greater than $3 Million annually	25	
	Equal to or greater than $2 Million and less than $3 Million annually	10	
	Greater than $1 million and less than $2 Million annually	5	
	$1 million	0	
TOTAL SCORE FOR OEM REFERENCE			

TOTAL POSSIBLE SCORE PER REFERENCE		**50**

Table 5 Access Routers Reference Rated Requirements

ACCESS ROUTER - END-USER REFERENCE #:____ **ACCESS ROUTER - END-USER REFERENCE Name:_____**			
General Information			
a) Access Router Reference Information:	Contact Name:		
	Telephone Number:		
	Email Address:		
Rated Requirements			
Description - The End-User reference attests that it:	**End-User Reference**	**Score**	**Page #**
b) Uses the proposed Access Router OEM devices in a secure DMVPN network and that the product integrates with Cisco 2800 or 2900 and 3800 or 3900 routers in a network with at least 200 routers.	Yes No	75 0	
c) Uses the VoIP OEM devices with the Access Router OEM devices proposed including at a minimum the VoIP ISDN PSTN access or SIP based PSTN access with a Cisco Call manager 7.0 VoIP infrastructure with voice messaging, IVR, emergency response and Music on hold for at least 6000 IP phones.	Yes No	50 0	
d) Uses the Video conferencing OEM devices – integrated with any POLYCOM or Tandberg video conferencing infrastructure with at least 80 conference rooms.	Yes No	15 0	
e) Uses Panasonic Perimeter monitoring infrastructure with at least1000 HD cameras transmitting with real time local and remote recording and viewing of camera images.	Yes No	10 0	
f) Uses a minimum of two of the RoIP OEM devices with the proposed Access Router OEM devices with LMR P25 radio equipment from Motorola or Daniels or PlantCML(EADS) or Harris or EF Johnson.	Yes No	50 0	
TOTAL SCORE FOR END-USER REFERENCE			
TOTAL POSSIBLE SCORE PER REFERENCE	**200**		

Table 6 VoIP Reference Rated Requirements

VoIP - END-USER REFERENCE #:____ **VoIP - END-USER REFERENCE Name:_____**			
General Information			
a) VoIP Reference Information:	Contact Name:		
	Telephone Number:		
	Email Address:		
Rated Requirements			
Description - The End-User reference attests that it:	**End-User Reference**	**Score**	**Page #**
b) Connects CISCO VoIP IP phones with the proposed VoIP IP PBX device providing Call management, messaging, and Emergency response	Yes No	30 0	
c) Has a VoIP network that uses Cisco 2800 or 2900 and 3800 or 3900 routers or larger Cisco routers for PSTN gateway functionality to allow: incoming and outgoing calls between any VoIP IP Phone and any PSTN connected phone with these devices providing either ISDN or SIP based PSTN connectivity; Communications between devices using dissimilar codecs; and Restoral and redundancy of local site IP Phone connectivity in case of network failure by routing calls over PSTN connections and offering some local site Call management capability directly on the Access Router.	Yes No	60 0	
d) Has CISCO 3750 switches or 3560 switches or any switching modules integrated into the CISCO routers providing connectivity and power to the proposed OEMs VoIP IP Phone devices.	Yes No	10 0	
e) Has a VoIP network that uses the proposed VoIP OEM devices with at least 24000 IP Phones with voice messaging, IVR, emergency response and Music on hold for all IP phones.	Yes No	50 0	
TOTAL SCORE FOR END-USER REFERENCE			
TOTAL POSSIBLE SCORE PER REFERENCE	**150**		

Table 7 RoIP Integration Reference Rated Requirements

RoIP - END-USER REFERENCE #:____ **RoIP - END-USER REFERENCE Name:_____**			
General Information			
a) RoIP Reference Information:	Contact Name:		
	Telephone Number:		
	Email Address:		
Rated Requirements			
Description - The End-User reference attests that it:	**End-User Reference**	**Score**	**Page #**
c) Uses the proposed RoIP Device Category devices, providing interoperability between legacy/analog Radio devices with the proposed RoIP devices for LMR P25 radio and Cisco 2800 or 2900 and 3800 or 3900 routers for IP networking.	Yes No	25 0	
d) Uses the proposed RoIP Device Category devices withinteroperability between a Cisco VoIP network with Radio PTT so that VoIP IP phones could participate in conferences and conversations with Radios connected to the IP network.	Yes No	25 0	
e) Uses the proposed OEM's RoIP devices to interoperate with LMR with Radio equipment from Motorola.	Yes No	50 0	
f) Uses the proposed OEM's RoIP devices to interoperate with LMR with Radio equipment from Daniels.	Yes No	50 0	
e) Uses the proposed OEM's RoIP devices to interoperate with LMR with Radio equipment from PlantCML(EADS).	Yes No	50 0	
e) Uses the proposed OEM's RoIP devices to interoperate with LMR with Radio equipment from Harris.	Yes No	50 0	
e) Uses the proposed OEM's RoIP devices to interoperate with LMR with Radio equipment from EF Johnson.	Yes No	50 0	
f) Has a network that supports at least 200 radio tower/transmitter receiver/base stations and more than 1000 radios integrated with the proposed Access Router OEM and the proposed OEM for VoIP for Radio to IP phones connectivity.	Yes No	150 0	

RoIP - END-USER REFERENCE #:____ **RoIP - END-USER REFERENCE Name:_____**			
g) Uses OEM devices proposed for the Radio over IP category, integrated with: • A data network with routers including Cisco 2800 or 2900 and 3800 or 3900 routers for IP networking with at least 1000 routers	Yes No	50 0	
TOTAL SCORE FOR END-USER REFERENCE			
TOTAL POSSIBLE SCORE PER REFERENCE	**500**		

Table 8 Video Monitoring Integration Reference Rated Requirements

VIDEO MONITORING - END-USER REFERENCE #:____ **VIDEO MONITORING - END-USER REFERENCE Name:_____**			
General Information			
a) IP Video Monitoring Reference Information:	Contact Name:		
	Telephone Number:		
	Email Address:		
Rated Requirements			
Description - The End-User reference attests that it:	**End-User Reference**	**Score**	**Page #**
b) Uses the proposed Video Monitoring OEM devices with Cisco 2800 or 2900 or 3800 or 3900 routers for connecting at least 200 sites to the WAN and with at least 30 sites supporting 10 or more HD cameras with remote monitoring, video recording and distribution sites;	Yes No	50 0	
TOTAL SCORE FOR END-USER REFERENCE			
TOTAL POSSIBLE SCORE PER REFERENCE	**50**		

Table 9 Video Conferencing Reference Rated Requirements

VIDEO CONFERENCING - END-USER REFERENCE #:____ **VIDEO CONFERENCING - END-USER REFERENCE Name:_____**			
General Information			
a) VoIP Reference Information:	Contact Name:		
	Telephone Number:		
	Email Address:		
Rated Requirements			
Description - The End-User reference attests that it:	**End-User Reference**	**Score**	**Page #**
b) Uses the proposed IP Video Conferencing Monitoring OEM devices with Cisco 2800 or 2900 or 3800 or 3900 routers for connecting sites on the WAN;	Yes No	25 0	
c) Uses the proposed IP Video Conferencing Monitoring OEM devices with a Cisco Call Manager VoIP network;	Yes No	25 0	
d) Uses the proposed IP Video Conferencing Monitoring OEM devices with POLYCOM or Tandberg video conferencing solution;	Yes No	25 0	
e) Uses the proposed IP Video Conferencing Monitoring OEM devices in a network of at least 80 video conferencing rooms.	Yes No	125 0	
TOTAL SCORE FOR END-USER REFERENCE			
TOTAL POSSIBLE SCORE PER REFERENCE	**200**		

Table 10 Proposed OEMs Rated Requirements

General Information	
Device Category	**Name of Proposed OEM**
1. Access Routers	
2. Data Centre Bridging	
3. Voice over IP	
4. Radio over IP	
5. IP Video Monitoring	
6. IP Video Conferencing	
7. Wireless LAN	
8. Wireless IDS/IPS	

Rated Requirements	
Description	**Score**
The same OEM proposed for all 8 Device Categories	600
The same OEM proposed for 7 Device Categories	500
Largest number of Device Categories proposed from the same OEM is 4,5, or 6 out of 8	150
Largest number of Device Categories proposed from the same OEM is 2 or 3 out of 8	50
TOTAL SCORE FOR NUMBER OF PROPOSED OEMs	
TOTAL POSSIBLE SCORE	**600**

ANNEX C

REPORT FORMATS

For

Multimedia Network Convergence
Equipment and Support Services

For

Royal Canadian Mounted Police (RCMP)

C-1 STANDING OFFER USAGE REPORT

STANDING OFFER NUMBER M9010-09-1080

Cumulative Number of Invoices To Date		**Cumulative Number of Call-Ups To Date:**		**Cumulative Invoiced To Date (taxes included):**	$ XX.XX	**Start Reporting Period:**	
Total Number of Invoices for Current Reporting Period		**Total Number of Call-ups for Current Reporting Period:**		**Total for current Reporting Period (taxes included):**	$ XX.XX	**End Reporting Period:**	

Invoice/Credit Memo number	Invoice Date	Call-up Number	Amendment Number (if applicable)	Call-up/Amendment Date	Delivery Date	Category (Device category or Resource Category)	Item ID	Quantity	Unit Price	Total Item Value (Taxes Excluded)	Total Item Value (Taxes Included)

C-2 STANDING OFFER USAGE REPORT

STANDING OFFER NUMBER M9010-09-1080

Cumulative Deliveries Delayed To Date:		**Cumulative Credits To Date:**		**Start Reporting Period:**	
Total Delayed Deliveries for Current Reporting Period:		**Total Credits for Current Reporting Period:**		**End Reporting Period:**	

Call-up Number	RCMP Call-up Coordinator Name	Item ID (of the item delivered late)	Original Delivery Date	Actual Delivery Date	Number of Calendar Days Delayed	Destionation	Reason for Delay	Applicable Credit ($)

C-3 STANDING OFFER WARRANTY INCIDENTS REPORT

STANDING OFFER NUMBER M9010-09-1080

Cumulative Warranty Incidents To Date:	
Total Warranty Incidents for Current Reporting Period:	

Start Reporting Period:	
End Reporting Period:	

Incident Number Assigned to the Warranty Call	Date of Warranty Call	Date Warranty Call Was/Will be Resolved	Device Category Related to Warranty Call	Number of Components Replaced Due to Warranty Call	Comments

ANNEX D

SRCL

For

Multimedia Network Convergence
Equipment and Support Services

For

Royal Canadian Mounted Police (RCMP)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
M9010-091080
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	2. Branch or Directorate / Direction générale ou Direction
Royal Canadian Mounted Police	Network Service Branch
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

RCMP requires a procurement arrangement for specialized multimedia network equipment used to converge different multimedia services on to the RCMP IP data WAN network including Voice, video and radion requirements.(excluding professional services)

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

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

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No Non	☑ Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No Non	☐ Yes Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?	☑ No Non	☐ Yes Oui

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

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐

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

No release restrictions Aucune restriction relative à la diffusion ☑	All NATO countries Tous les pays de l'OTAN ☐	No release restrictions Aucune restriction relative à la diffusion ☐
Not releasable À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

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

PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☐	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
UNCLASSIFIED

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
M9010-091080
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? ☑ No ☐ Yes
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? ☑ Non ☐ Oui
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

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

if anything higher than R.R.S is required. another SRCL will be needed. /dl

Special comments:
Commentaires spéciaux : Tasks requiring additional security levels and clearances will be identified through Task authorizations

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

10. b) May unscreened personnel be used for portions of the work? ☑ No ☐ Yes
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? ☑ Non ☐ Oui
If Yes, will unscreened personnel be escorted? ☐ No ☐ Yes
Dans l'affirmative, le personnel en question sera-t-il escorté? ☐ Non ☐ 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? ☑ No ☐ Yes
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? ☑ Non ☐ Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets? ☑ No ☐ Yes
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC? ☑ Non ☐ 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? ☑ No ☐ Yes
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? ☑ Non ☐ 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? ☑ No ☐ Yes
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? ☑ Non ☐ Oui

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
M9010-091080
Security Classification / Classification de sécurité
UNCLASSIFIED

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE? ☑ No / Non ☐ Yes / Oui

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

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE? ☑ No / Non ☐ Yes / Oui

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