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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions – TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Quebec
K1A0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

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

Issuing Office - Bureau de distribution

Informatics Professional Services Division/Division des services professionnels en informatique
Terrasses de la Chaudière 4th Floo
10 Wellington Street
Gatineau
Quebec
K1A0S5

Title - Sujet Tier 2 Informatics Professional Ser	
Solicitation No. - N° de l'invitation W6369-17P5LL/B	**Amendment No. - N° modif.** 002
Client Reference No. - N° de référence du client W6369-17P5LL	**Date** 2019-04-08
GETS Reference No. - N° de référence de SEAG PW-$IPS-004-34777	
File No. - N° de dossier 004ips.W6369-17P5LL	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2019-04-16**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☑	
Address Enquiries to: - Adresser toutes questions à: Patel, Ankoor	**Buyer Id - Id de l'acheteur** 004ips
Telephone No. - N° de téléphone (613) 858-9403 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

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

Canada

Solicitation No. – Nº de l'invitation	Amd. No – Nº de la modif.	Buyer ID – Id de l'acheteur
W6369-17P5LL/B	002	004ips
Client Ref. No. – Nº de réf. De client	**File No. – Nº du dossier**	**CCC No./ Nº CCC – FMS No/ Nº VME**
W6369-17P5LL	004ips W6369-17P5LL	

AMENDMENT NO. 002

This amendment is raised to revise the RFP and answer Bidder's questions.

RFP REVISIONS:

1. **Delete:** Document in Appendix C to Annex A – Resources Assessment Criteria and Response Table Workstream 2- Top Secret in its entirety; and

   Replace with: The document follows in PDF format

2. **Delete:** Document in Attachment 4.1 – Bid Evaluation Criteria - Workstream 2- Top Secret in its entirety; and

   Replace with: The document follows in PDF format

QUESTIONS AND ANSWERS:

Question 7:

The specific organizational environment outlined in Corporate Criteria M1 (both workstreams) limits the number of large ($5M+) Government informatics services contracts that can be referenced.

Our firm understands that the organizational environment has been included because it is critical to the services being provided. However, in order to allow for a broader range of otherwise qualified vendors to bid, we ask that the Crown amend the requirement as follows:

"For each contract identified:

1) The value must be at least $5,000,000.00 ($5M) excluding applicable taxes;

2) The duration must be at least one (1) year within the last eight (8) years from the closing date of this solicitation and cannot include option periods that have not been exercised;

3) The bidder must have provided at least eight (8) resources simultaneously for a period of at least six (6) consecutive months;"

Answer 7:

After careful review, the Crown has decided that RFP remains the same.

Question 8:

Could the Crown please clarify the security requirements?

- Do ALL resources submitted under the SECRET Workstream require NATO SECRET at the time of bid submission?
- Do ALL resources submitted under the TOP SECRET Workstream require TOP SECRET – SIGINT at the time of bid submission?

NATO SECRET and TOP SECRET – SIGINT status are not typically granted unless a resource on contract requires that level of clearance to perform their work. Therefore, asking for these security requirements at the time of bid submission drastically limits the pool of otherwise qualified candidate resources.

Answer 8:

The Crown confirms that the resources requires the proper security clearance before contract award, as stipulated in section 6.1. The process to contract award includes the time to process the FOCI requirement, as stipulated in section 7.5 f) and p), which may provide enough additional time to process the security clearance request for the resources submitted. The Crown confirms that CISD will accept this bid solicitation number as a valid reason for initiate a security clearance request for the resources submitted.

Question 9:

Ref:
Workstream 1, IT Security Design Specialist, Level 3, IEG, R3 requirement
Workstream 2, IT Security Design Specialist, Level 3, IEG, R3 requirement

The Crown assume the question related to:

WorkStream 2

C6: Information Technology Security Engineer Level 2

Specific Task Title: Information Exchange Gateway (IEG), requirement M4; and

C6: Information Technology Security Engineer Level 2

Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning, requirement M4:

"The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience engineering, designing, configuring and integrating Border Protection Service solutions."

Question:

Can Canada please confirm that Border protection services are the components involved with a network perimeter or information exchange gateway, including but not limited to web proxy, email proxy, firewall, content filtering technology (standalone or as part of the proxy solution), and email message labelling (e.g. Titus).

Answer 9:

The Crown confirms that the term 'Border protection services' refers to 'the components involved with a network perimeter or information exchange gateway, including but not limited to web proxy, email proxy, firewall, content filtering technology (standalone or as part of the proxy solution), and email message labelling (e.g. Titus).'

Question 10:

Ref:

Workstream 2, IT Security Design Specialist, Level 2, CDS Transfer, M1 requirement:
"The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating High Assurance Guard technologies."

Question:

Can Canada please confirm that High Assurance Guards are a specific category of technologies used to perform secure transfer of information between classifications. Approved suppliers are US organizations and procurements are done through Foreign Military Sales. Examples include Radiant Mercury and the ISSE guard. These devices by definition operate in a classified environment because they are used to move information into and out of those environments.

Answer 10:

The Crown confirms that the term 'High Assurance Guard' refers to a 'specific category of technologies used to perform secure transfer of information between security domains of different classifications'.

Question 11:

Ref:

Workstream 1, IT Security Design Specialist, Level 3, IEG, R3 requirement
Workstream 2, IT Security Design Specialist, Level 3, IEG, R3 requirement

"….experience configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions."

Question:

Mail transfer agent (MTA) solutions are relatively simple technologies that often operate in similar manners, with the only major difference being the user interface. Given that the rest of the requirements are sufficiently stringent that you will be getting a skilled technical resource who can learn a different version of this technology, would DND modify the requirement to state experience with mail transfer agent technologies?

Answer 11:

After careful review, the Crown decides that the RFP will stay the same

---

Question 12:

Ref:

Workstream 1, IT Security Design Specialist, Level 3, IEG, R1 requirement

Workstream 2, IT Security Design Specialist, Level 3, IEG, R1 requirement

Question:

M1 for these roles requires a minimum of 2 years with Firewalls. R1 lists specific firewall technologies.

a) Can the Crown confirm if they are looking for expertise in firewall technologies that have application proxy capabilities?
b) Will rated points will be awarded only for the specific firewall technologies listed in R1, i.e. McAfee, Palo Alto, or F5 or will rated points be awarded for any firewall technologies regardless of its features?

Answer 12:

The Crown confirms that the requirement M1 refers to any firewall technologies. The crown also confirm that the rated requirement R1 refers to any firewall technologies regardless of its features.

Question 13:

Ref:

Workstream 2, C.7 IT Sec Design Specialist – Level 2 Full Packet Capture R3

Question:
As with many the technical roles in Workstream 2 that provide rated points for a CISSP, such as:

1. IT Security Engineer Level 3 IEG;
2. IT Security Engineer Level 3 Network Security Monitoring;
3. IT Sec Design Specialist Level 3 Network Security Content Inspection;
4. IT Security Design Specialist Level 3 eGRC; and
   IT Security Design Specialist NSM.

Please confirm that the CISSP certification will also be considered for points in the IT Security Design Specialist Full Packet Capture, Level 2, criterion R3?

Answer 13:

After careful review, the Crown decides that the RFP will stay the same, and the CISSP certification will not be considered for points in this context.

Question 14:

Reference:

Workstream 2, C.7 IT Sec Design Specialist – Level 3 eGRC R1

Question:

As with many the technical roles in Workstream 2 that provide rated points for a vendor-certifications as "completed specific training OR holds a current certification", such as:

1. IT Security Engineer Level 3 NSM R2;
2. Network Security Analyst Level 3 NSM R5;
3. Network Security Analyst Level 3 SIEM ISS R7; and
4. Incident Management Specialist Level 3 SIEM ISS R7).

Provided the Bidder provides proof of training, will the Crown modify IT Security Design Specialist , Enterprise eGRC, Level 3 as follows:

R1: The Contractor should demonstrate that the proposed resource completed training or holds a current certification in one or more of the following administrating IT GRC or eGRC application certifications.

Proof of training or copy of the resource's valid certification must be submitted with the bid

Answer 14:

After careful review, the Crown decides that the RFP will stay the same.

Question 15:

Reference:

Workstream 1, C.8 Network Security Analyst Level 3 NSM R7

Question:

As with the following technical grids:

1- IT Security Methodology, Policy and Procedures Analyst Level 2 STIG R8;
2- S.3 IT Security Engineer Level 3 Network Security Content R8; and
3- IT Security Design Specialist Level 2 Host R7.

Please confirm that SANS GIAC Security Essentials (GSEC) will also be included for points in the Network Security Analyst Level 3 NSM R7 criterion?

Answer 15:

After careful review, the Crown decides that the RFP will stay the same: The certifications accepted for points are those explicitly enumerated at criterion R7 of task C.8 Network Security Analyst Level 3 NSM. Consequently, the certification SANS GIAC Security Essentials (GSEC) is not accepted in this context.

Question 16:

Reference:
Workstream 2, C.7 IT Sec Design Specialist Level 3 Network Security Content Inspection R8

Question:

As with the following technical grids:

1. example IT Security Design Specialist Level 2 Full Packet Capture; and
2. IT Security Design Specialist Level 2 Host

Please confirm that the Crown will accept SANS GCIH and SANS GPEN for the referenced requirement?

Answer 16:

After careful review, the Crown decides that the RFP will stay the same: The certifications accepted for points are those explicitly enumerated at criterion R8 of task C.7 IT Sec Design Specialist Level 3 Network Security Content Inspection. Consequently, the certifications SANS GCIH and SANS GPEN are not accepted in this context.

Question 17:

Reference:

Workstream 2, C.7 IT Security Design Specialist, ICAM and PKI, Level 3, M3

Question:
DND current policies and standards (http://www.forces.gc.ca/en/about-policies-standards/dndaf.page) states "The DND/CF Architecture Framework (DNDAF) is the prescribed standard for use in all DND/CF architecture activities". The architectural frameworks currently listed at M3 essentially disqualifies any DND longstanding resources who used DNDAF. Please confirm that DNDAF will be included within this criterion to enable bidders to propose resources with years of experience within DND.

Answer 17: The Crown confirms that the DNDAF framework will be added to the list of architectural frameworks accepted in this context. Please see updated Attachment 4.1 - Workstream 2 and Appendix C to Annex A - Workstream 2.

Question 18:

Reference:
Workstream 2, IT Security Design Specialist Level 3 – Enterprise eGRC R8

Question:
Please confirm that ITIL will also be consider for points in this criterion as it is an industry recognized certification that demonstrates capacity in change management practices and an understanding for the IT development cycle that would also be a valuable attribute.

Answer 18:
After careful review, the Crown decides that the RFP will stay the same. The ITIL certification will not be considered in this context.

Question 19:

Regarding Section 3.2 Section IV Technical Bid, Previous Similar Projects (page 14), please confirm the Crown will accept corporate references by the bidder, or its wholly owned local subsidiary company as a compliant response to Mandatory Requirements – Corporate Criteria in Attachment 4.1 Bid Evaluation Criteria for Workstream 1 and Workstream 2.

Answer: 19:
The Crown confirms that it will only accept corporate references by the Bidder. In the Standard Acquisition Clauses and Conditions (SACC), ID 2003 Standard Instructions – Goods or Services – Competitive Requirements, Bidder is defined as "the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both. It does not include the parent, subsidiaries or other affiliates of the Bidder, or its subcontractors."

Question 20:

Questions related to extensions to the bid closing date

Answer 20:

After careful review, the Crown decides that the RFP will stay the same.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.
NOTE: A BID ALREADY SUBMITTED MAY BE AMENDED PRIOR TO THE CLOSING DATE. AMENDING CORRESPONDENCE MUST ADDRESS THE SOLICITATION NUMBER AND THE CLOSING DATE AND MUST BE ADDRESSED TO:
BID RECEIVING
PUBLIC WORKS AND GOVERNMENT SERVICES CANADA
PLACE DU PORTAGE, PHASE III
MAIN LOBBY, ROOM 0A1
11 LAURIER STREET
GATINEAU, QUEBEC K1A 0S5

APPENDIX C TO ANNEX A

RESOURCES ASSESSMENT CRITERIA AND RESPONSE TABLE

WORKSTREAM 2 – TOP SECRET

To facilitate resource assessment, Contractors must prepare and submit a response to a draft Task Authorization using the tables provided in this Annex. When completing the resource grids, the specific information which demonstrates the requested criteria and reference to the page number of the résumé should be incorporated so that Canada can verify this information. The tables should not contain all the project information from the resume. Only the specific answer should be provided.

RESOURCE CRITERIA

MANDATORY CRITERIA

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Configuration Management

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Configuration Management				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience planning and implementing IT security solutions.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years performing security architecture design or engineering support in the area of IT security.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the last ten (10) years, planning, developing, implementing and integrating vulnerability assessment solutions.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last eight (8) years, developing and implementing a vulnerability management program for an organization of at least 5,000 users.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience applying Government IT Security policies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience engineering, designing, configuring and integrating Border Protection Service solutions.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Cyber Security Reference Architecture

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Cyber Security Reference Architecture				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the design, planning, and/or implementation of information technology services, such as web services, database services, directory services, user access services, virtualized environments, and/or virtual desktops.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the review, design, planning, and/or implementation of security services, or security architectures for IT systems supporting more than 100 users.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience authoring technical configuration or implementation documentation.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Cross Domain Solution – Access

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Cross Domain Solution – Access				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience developing, configuring and testing of network security controls and policies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of experience designing and delivering virtual desktop services.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of experience designing, configuring and implementing role and rule-based access control models.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M6	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in designing, configuring and implementing IPSec tunneling schemes.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: Cross Domain Solution – Transfer

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: Cross Domain Solution – Transfer				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating High Assurance Guard technologies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of experience configuring and integrating Firewall technologies.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of combined experience engineering, designing, configuring and integrating e-mail content filter (such as malware prevention) and data loss prevention (such as label checking and word checking) technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience engineering, designing, configuring and integrating Border Protection Service solutions.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an IT Security Engineer.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of combined experience composing and maintaining Security Information and Event Management (SIEM) and/or Full Packet Capture (FPC) technical and engineering documentation.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in designing and implementing network security monitoring use cases in an enterprise deployment.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the last ten (10) years designing, deploying and integrating SIEM tools and/or Full Packet Capture (FPC) tools in a production environment.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Full Packet Capture

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Full Packet Capture				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years, working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years, designing, deploying, administering and troubleshooting local and wide-area network communications infrastructure components.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years performing system administration with Linux or a Linux variant.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Host Security				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years, working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of combined experience, within the last seven (7) years, designing, engineering, installing, configuring, and testing endpoint protection security software in an enterprise IT environment. Endpoint protection security software experience must include two (2) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME)			
M3	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of experience applying IT Security end-point protection policies in an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last seven (7) years developing security architecture design for a Government classified solution (SECRET and above).			
M3	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience using at least one (1) of the following architectural methods/frameworks within the past seven (7) years: • TOGAF; • US government FEAP; • Canadian government BTEP; • Zachman; • SABSA Security Architecture Framework; and/or • Department of National Defence Architecture Framework (DNDAF)			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last seven (7) years conducting detailed ICAM solution requirements analysis, design and implementation.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of experience briefing senior managers (Director level and above) on IT security implications and recommended courses of action.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following security networking technologies: • Guards and Gateways; • Firewalls; • Border Protection Services; • Data Diodes; • Web proxies; and • Mail Transfer Agent. A minimum of two years of experience is required for each of the above technologies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following IT products and infrastructure: • Microsoft Network Operating System; • IP Networks; • Applications Integration; and • Virtualization. A minimum of three years of experience is required for each of the above technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last six (6) years working with common classified networks at the Secret and/or Top Secret level.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Cross Domain Solution – Access

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Cross Domain Solution - Access				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience planning and implementing IT Security integration architectures.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of experience in the design, implementation and change management of network security controls and policies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of virtual desktop services.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of role- and rule-based access control models.			
M5	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of IPSec tunneling schemes.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M6	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Host Security				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience designing and implementing IT security solutions.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of combined experience, within the last eight (8) years, designing, engineering, installing, configuring, and testing endpoint protection security software in an enterprise IT environment. Endpoint protection security software experience must include three (3) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME)			
M3	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience in the last eight (8) years applying IT Security end-point protection policies to an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Contractor must demonstrate that the resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Network Security – Content Inspection

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Network Security – Content Inspection				
M1	The Contractor must demonstrate that the proposed resource has a minimum ten (10) years of experience within the last fifteen (15) years working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years configuring and integrating networking equipment.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last ten (10) years designing secure architectures while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience in the last eight (8) years configuring, integrating and troubleshooting Firewalls.			
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience integrating IT security solution Proof of Concepts (POCs).			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience, within the last fifteen (15) years, working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has at least two (2) years of experience, within the last five (5) years developing and implementing an Enterprise Governance, Risk, and Compliance (eGRC) solution for an organization of at least 5,000 users.			
M3	The Contractor must demonstrate that the proposed resource has at least two (2) years of experience within the last five (5) years in the assessment of applied Security Controls, the evaluation of Threats and Risks to an IT system, or the interpretation and application of Information Technology Security Guidance (ITSG) 33 Annex A.			
M4	The Contractor must demonstrate that the proposed resource has at least two (2) years of experience within the last ten (10) years defining requirements, translating business process into workflow, and engineering solutions in the definition and implementation stages of an IT Security project.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as a Network Security Analyst.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience monitoring and analysing security log files from an enterprise network of at least 500 users.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience with the collection and analysis of malicious code from hosts and network traffic.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the last eight (8) years monitoring, configuring and tuning Security Information and Event Management (SIEM) tools and/or Full Packet Capture tools in a production environment.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Security Information and Event Management (SIEM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Security Information and Event Management (SIEM)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as a Network Security Analyst			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last five (5) years configuring and providing technical support for the Security Information and Event Management (SIEM) tool ArcSight in a production environment.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience monitoring and analyzing security log files from an enterprise network of at least 500 users.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design and implementation of SIEM use cases for both servers and workstations in an enterprise deployment.			
M5	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience building, configuring, and troubleshooting Linux servers.			
	Compliant (Yes/No)?			

C.12 Incident Management Specialist – Level 3
Specific Task Title: Security Information and Event Management (SIEM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.12 Incident Management Specialist – Level 3 Specific Task Title: Security Information and Event Management (SIEM)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an Incident Management Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years implementing and providing technical support for the Security Information and Event Management (SIEM) tool ArcSight in a production environment.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design and implementation of SIEM use cases for both servers and workstations in an enterprise deployment.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience building, configuring, and troubleshooting Linux servers.			
M5	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience composing and maintaining SIEM documents or SIEM engineering deliverables.			
	Compliant (Yes/No)?			

RATED CRITERIA

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Configuration Management

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Configuration Management					
R1	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Contractor should demonstrate that the proposed resource has experience performing options analysis of IT security tools and techniques.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R3	The Contractor should demonstrate that the proposed resource has experience planning, developing, implementing and integrating IT asset discovery or configuration management database (CMDB) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Contractor should demonstrate that the proposed resource has experience in planning, developing, implementing and integrating automated configuration compliance auditing solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R5	The Contractor should demonstrate that the proposed resource has experience writing technical reports such as requirements analysis, options analysis, and technical architecture documents.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R6	The Contractor should demonstrate that the proposed resource has experience developing hardening guides for IT systems.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The proposed resource should hold one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 19 points**	**Maximum Score: 27 points**		

C.6 – Information Technology Security Engineer - Level 2
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 – Information Technology Security Engineer - Level 2 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing proxy solutions, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Cyber Security Reference Architecture

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Cyber Security Reference Architecture					
R1	The Contractor should demonstrate that the proposed resource has at least 6 months experience designing, or co-designing one major scale IT (Information Technology) environment for a minimum of 100 users.	IT supporting users: 3 points: 100 to 300 users. 4 points: >300 to 1000 users. 5 points: >1000 or more users.	5		
R2	The Contractor should demonstrate that the proposed resource has experience working in the application of IT Security Risk Management processes or System Security Engineering processes.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience designing or implementing and configuring IT Intrusion Detection and Protection methodologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience working with the design or implementing and configuring System Monitoring for accesses, changes or operational status.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience designing or implementing and configuring IT Enterprise Services, including directory, single sign-on, email, backup, or distributed database for an IT system supporting at least 500 users.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience designing or implementing and configuring IT Defence in Depth principles. The Contractor should also demonstrate and provide a description of how the resource applied the principles.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience working with a recognized enterprise architecture framework.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R8	The Contractor should demonstrate that the proposed resource has experience writing technical documents using desktop office-class tools, for audience at the corporate level.	1 point: 1 to 2 years of experience. 2 points: >2 to 4 years of experience. 3 points: >4 to 6 years of experience 4 points: >6 years of experience.	4		
	Total:	**Minimum Passing Score: 19 points**	**Maximum Score: 27 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Cross Domain Solution – Access

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Cross Domain Solution – Access					
R1	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.6 - Information Technology Security Engineer - Level 2
Specific Task Title: Cross Domain Solution – Transfer

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 2 Specific Task Title: Cross Domain Solution – Transfer					
R1	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.6 - Information Technology Security Engineer - Level 2
Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 2 Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning					
R1	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing proxy solutions, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Red Hat Enterprise Linux (RHEL).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R8	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 17 points**	**Maximum Score: 24 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Contractor should demonstrate that the proposed resource has experience in the last ten (10) years engineering network security monitoring solutions using at least three (3) of the following security technologies: 1) Host-based security; 2) IDS/IPS (Intrusion Prevention System); 3) Firewalls/UTMs; 4) Full Packet Capture; 5) Proxies; 6) Load Balancers; and 7) Matrix Switches/Taps.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience within the last ten (10) years designing network security monitoring solutions for the Government based on IT Security Directive (ITSD) 02 or IT Security Guidance (ITSG) 22 at the Protected B level or higher.	1 point per project up to a maximum 3 projects*† *If a Contractor provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		
R4	The Contractor should demonstrate that the proposed resource has experience providing IT security engineering services to Government departments and agencies in the form of security architecture development, advice and guidance.	1 point: 3 to 5 years of experience. 2 points: >5 to 7 years of experience. 3 points: >7 to 9 years of experience. 4 points: >9 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate the proposed resource holds one or more of the following IT security certifications: 1) International Information Systems Security Certification Consortium $(ISC)^2$ CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA) A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 16 points**		

C.7 - Information Technology Security Design Specialist - Level 2
Specific Task Title: Full Packet Capture

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 2 Specific Task Title: Full Packet Capture					
R1	The Contractor should demonstrate the proposed resource has experience within the last seven (7) years designing, planning and implementing network infrastructure of complex and highly available* environments. *Complex and highly available environments are defined as environments spanning multiple cities or countries with zero-downtime.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

R2	The Contractor should demonstrate that the proposed resource has combined experience within the last ten (10) years performing one or more of the following IT-related tasks: 1. Writing technical reports such as requirement analysis, options analysis, engineering process artefacts and/or technical architecture documents; 2. Automating the administration of Linux systems through scripting and APIs such as (but not limited to) Ruby, PHP, Bash, Perl or Python; 3. Analysis of raw network traffic capture to support troubleshooting or network forensics; 4. Deployment and administration of network forensics or traffic monitoring devices such as (but not limited to) FireEye, Solera, Sourcefire/Cisco IDS/IPS, SNORT or Netwitness (RSA Security Analytics); 5. Review alerts and packet-level data from IDS sensors/ packet capture devices;	1 point: 6 to 9 months of experience. 2 points: >9 to 12 months of experience. 3 points: >12 to 15 months of experience. 4 points: >15 months of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R2	6. Malware analysis and sandboxing with applications like (but not limited to) Netwitness Spectrum/RSA Malware, WireShark, CaptureBAT or Cuckoo Sandbox and the ability to reverse engineer and debug malware samples using tools such as (but not limited to) IDA Pro, Responder Pro or OllyDbg, including defeating anti debugging, packing and obfuscation techniques; and/or 7. Management of SAN and NAS technologies – Fibre Channel, FCOE, iSCSI, NFS, CIFS, including but not limited to the provisioning of LUNs, cabling, troubleshooting and patching. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.				

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has one or more of the following IT security certifications: 1) RSA Security Analytics Certified Administrator; 2) Any Cisco Associate level certification; 3) Any Cisco Professional level certification; 4) Any Cisco Expert level certification; 5) Any SANS GIAC certification in the Security Administration category; 6) Any Redhat Certified System Administrator, Engineer and/or architect certification; A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 or more certifications.	5		
	Total:	**Minimum Passing Score: 8 points**	**Maximum Score: 12 points**		

C.7 - Information Technology Security Design Specialist - Level 2
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 2 Specific Task Title: Host Security					
R1	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience implementing centrally managed host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience implementing McAfee, Symantec or Trend-Micro host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Contractor should demonstrate that the proposed resource has a minimum one (1) year each of experience engineering and implementing the following host-based security technologies, in an enterprise IT environment: 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; or 3) Trend-Micro Control Manager.	1 point: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 2 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 3 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	3		
R5	The Contractor should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec, or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		
R6	The Contractor should demonstrate that the proposed resource has experience evaluating various IT security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Contractor provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource has experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and 9) Other Content Inspection systems. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Contractor should demonstrate that the proposed resource holds at least one of the following IT security certifications: 1) ISC2 Certified Information System Security Professional (CISSP); 2) ISC2 Certified Cloud Security Professional (CCSP); 3) ISC2 Systems Security Certified Professional (SSCP); and/or 4) Global Information Assurance Certification (GIAC) certification (any). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 or more certifications.	5		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 26 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)					
R1	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years developing Standard Operating Procedures (SOP) on projects.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years designing and deploying PKI technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years designing and deploying Identity, Credential and Access Management (ICAM) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months experience designing IT solutions requiring interoperability with: • one or more GoC departments; and/or • one or more of the following International partners: US, UK, AUS, NZ.	1 point: demonstrated at least six (6) months of experience designing IT solutions requiring interoperability with GoC department(s). 2 points: demonstrated at least six (6) months of experience designing IT solutions requiring interoperability with International partner(s) (US, UK, AUS, NZ)	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years designing process mapping for a security architecture design.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Firewall technologies, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing proxy technologies, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP technologies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware technology.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent versions), Active Directory and Domain Name System in large (at least 1,000 users) IT networks.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Cross Domain Solution – Access

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Cross Domain Solution – Access					
R1	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has combined experience performing at least three (3) the following IT Security tasks: 1) Analysis of IT Security tools and techniques; 2) Analysis of security data and provision of advisories and reports; 3) Writing technical reports including requirements analysis, options analysis, technical architecture documents and mathematical risk modeling; 4) Security architecture design and engineering support; and 5) Data security classification studies. A minimum of six (6) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent versions) Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience in design, implementation and change management of VMWare technologies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource holds one or more of the following architecture certifications: 1) Certification in The Open Group Architecture Framework (TOGAF); 2) Certification in Information Technology Service Management (ITSM); 3) Certification in Enterprise Architecture Center of Excellence (EACOE); 4) Certification in Microsoft Certified Architect (MCA); and/or 5) Certification in VMWare Certified Design Expert (VCDX). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Host Security					
R1	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience implementing centrally managed host-based endpoint security policies in an enterprise IT environment.	1 point: 2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience implementing McAfee host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Contractor should demonstrate that the proposed resource has a minimum one (1) year each of experience engineering and implementing the following host-based security technologies, on an enterprise IT environment: 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; or 3) Trend-Micro Control Manager.	1 point: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 2 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 3 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	3		
R5	The Contractor should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec, or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		
R6	The Contractor should demonstrate that the proposed resource has experience evaluating various security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Contractor provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource has experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and 9) Other Content Inspection systems. A minimum of six (6) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Network Security – Content Inspection

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Network Security – Content Inspection					
R1	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco technologies including Routers, and/or Nexus and Catalyst Series Switches.	1 point: 5 to 6 years of experience. 2 points: >6 to 7 years of experience. 3 points: >7 to 8 years of experience. 4 points: >8 years of experience.	4		
R2	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and troubleshooting Palo Alto firewalls.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience working with application aware traffic generators.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience working with Intrusion Detection Systems (IDS).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience working with VMWare.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning F5 load balancers.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience working with inline network encryption technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Contractor should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 25 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Enterprise Governance, Risk, and Compliance (eGRC)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Enterprise Governance, Risk, and Compliance (eGRC)					
R1	The Contractor should demonstrate that the proposed resource holds one or more of the following administrating IT GRC or eGRC application certifications: 1) RSA Archer Certified Administrator 2) IBM OpenPages Administrator 3) MetricStream GRC Certified Administrator A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
R2	The Contractor should demonstrate that the proposed resource has combined experience within the last five (5) years authoring XML data transformation and/or translation scripts.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience with IT Security Design projects within an eGRC implementation environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years writing technical reports such as options analysis, and/or implementation plans.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has combined experience within the last five (5) years accrediting an IT system using the Security Assessment and Authorization (SA&A) process and/or the Certification and Accreditation (C&A) program.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years developing network security architectures (Level II or higher) based on IT Security Directives (ITSD) and /or IT Security Guidance (ITSG).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Contractor should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications	3		
	Total:	**Minimum Passing Score: 16 points**	**Maximum Score: 23 points**		

C.8 – Network Security Analyst - Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 – Network Security Analyst - Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Contractor should demonstrate that the proposed resource has experience in the last ten (10) years performing network security monitoring and log analysis to detect malicious activity.	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and optimizing production Security Information and Event Management System (SIEM) and/or Full Packet Capture solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience providing IT security incident detection, analysis and handling services using automated Security Information and Event Management System (SIEM) tool(s).	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience operating and configuring all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of experience reviewing, developing and implementing incident handling and escalation process flows in an IM/IT project.	1 point = 1 project. 2 points = 2 projects. 3 points = 3 or more projects. A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) International Information System Security Certification Consortium (ISC)2 CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE); A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 14 points**	**Maximum Score: 20 points**		

C.8 – Network Security Analyst - Level 3
Specific Task Title: Security Information and Event Management (SIEM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 – Network Security Analyst - Level 3 Specific Task Title: Security Information and Event Management (SIEM)					
R1	The Contractor should demonstrate that the proposed resource has experience in the last seven (7) years performing network security monitoring and log analysis to detect malicious activity.	1 point: 2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and maintaining production SIEM solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years providing technical support to at least three (3) of the following network security technologies: 1) Host-based security 2) IDS/IPS (Intrusion Prevention System) 3) Firewalls/UTMs 4) Proxies 5) Load Balancers 6) Matrix Switches/Taps	1 point: 2 to 5 months of experience. 2 points: >5 months of experience.	2		
R4	The Contractor should demonstrate that the proposed resource has experience deploying and operating all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience tuning and configuring SIEM components to improve efficiency, accuracy, and performance.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Contractor should demonstrate that the proposed resource has experience in the last seven (7) years working in an in-service support/helpdesk environment.	1 point: 1 to 6 months of experience. 2 points: >6 months of experience.	2		
R7	The Contractor should demonstrate that the proposed resource completed ArcSight specific training and/or holds a current certification for ArcSight Technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
	Total:	**Minimum Passing Score: 13 points**	**Maximum Score: 18 points**		

C.12 – Incident Management Specialist - Level 3
Specific Task Title: Security Information and Event Management (SIEM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.12 – Incident Management Specialist - Level 3 Specific Task Title: Security Information and Event Management (SIEM)					
R1	The Contractor should demonstrate that the proposed resource has experience in the last seven (7) years performing network security monitoring and log analysis to detect malicious activity.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and maintaining production SIEM solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years providing technical support to at least three (3) of the following network security technologies: 1) Host-based security 2) IDS/IPS (Intrusion Prevention System) 3) Firewalls/UTMs 4) Proxies 5) Load Balancers 6) Matrix Switches/Taps	1 point: 2 to 5 months of experience. 2 points: >5 months of experience.	2		
R4	The Contractor should demonstrate that the proposed resource has experience deploying and operating all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience tuning and configuring SIEM components to improve efficiency, accuracy, and performance.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience in the last seven (7) years working in an in-service support/helpdesk environment.	1 point: 1 to 6 months of experience. 2 points: >6 months of experience.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource completed ArcSight specific training and/or holds a current certification for ArcSight Technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
	Total:	**Minimum Passing Score: 13 points**	**Maximum Score: 18 points**		

ATTACHMENT 4.1

BID EVALUATION CRITERIA

WORKSTREAM 2 – TOP SECRET

1. The evaluation criteria contained in this attachment will be used to evaluate bids during the solicitation and to facilitate resource assessment after contract award.

2. The Bidder must provide a qualifying résumé for each of the Resource Categories requested for evaluation (the Bidder must not propose the same resource more than once in response to this solicitation).

3. The Bidder must complete an evaluation grid for each of the résumés being provided as described in Table 1 below. For each criterion the Bidder must indicate the section in the résumé where compliance with the criteria is described. Failure to provide a qualifying résumé for each Resource Category results in a non-responsive bid.

Table 1: Bidders must submit the following number of résumés per resource category in response to this evaluation. The actual numbers of resources required are listed in Part 1, 1.2 Summary, of the bid solicitation;

Resource Category with Specific Task Title	Level	Number of Résumés
C.6 IT Security Engineer Specific Task Title: Configuration Management	3	1
C.6 IT Security Engineer Specific Task Title: Information Exchange Gateway (IEG)	2	1
C.6 IT Security Engineer Specific Task Title: Cyber Security Reference Architecture	3	1
C.6 IT Security Engineer Specific Task Title: Cross Domain Solution - Access	3	1
C.6 IT Security Engineer Specific Task Title: Cross Domain Solution - Transfer	2	1
C.6 IT Security Engineer Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning	2	1
C.6 IT Security Engineer Specific Task Title: Network Security Monitoring (NSM)	3	1
C.7 IT Security Design Specialist	2	1

Specific Task Title: Full Packet Capture		
C.7 IT Security Design Specialist Specific Task Title: Host Security	2	1
C.7 IT Security Design Specialist Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)	3	1
C.7 IT Security Design Specialist Specific Task Title: Information Exchange Gateway (IEG)	3	1
C.7 IT Security Design Specialist Specific Task Title: Cross Domain Solution - Access	3	1
C.7 IT Security Design Specialist Specific Task Title: Host Security	3	1
C.7 IT Security Design Specialist Specific Task Title: Network Security – Content Inspection	3	1
C.7 IT Security Design Specialist Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)	3	1
C.8 Network Security Analyst Specific Task Title: Network Security Monitoring (NSM)	3	1
C.8 Network Security Analyst Specific Task Title: Security Information and Event Management (SIEM)	3	1
C.12 Incident Management Specialist Specific Task Title: Security Information and Event Management (SIEM)	3	1

1. CORPORATE REQUIREMENTS

1.1. Corporate Mandatory Requirements

MANDATORY REQUIREMENTS – CORPORATE CRITERIA			
Item	**Mandatory Corporate Criteria**	**MET (Yes/No)**	**Page number(s) in bid**
M1	The Bidder must have been awarded at least 2 Government* informatics professional service† contracts. For each contract identified: 1. The value must be at least $5,000,000.00 ($5M) excluding applicable taxes; 2. The duration must be at least two (2) years within the last eight (8) years from the closing date of this solicitation and cannot include option periods that have not been exercised; 3. The Bidder must have provided at least five (5) resources simultaneously for a period of at least twelve (12) consecutive months; and Each contract used must also demonstrate that the Bidder has provided services to an organization with the following environment: • At least 100 workstations on a classified network or secret network; • Microsoft Windows workstation operating system (Windows XP, Windows Vista, Windows 7 and/or Windows 10); and • Centralized software distribution and patch management. The Bidder must provide one reference for each contract. The references must include the name of the organization, the unique contract identification number, a short description of the services provided, the name, title, email address and telephone number of the organization's responsible manager, the number of resources provided, as well as the award date, expiry date and dollar value of each contract. It is the Bidder's responsibility to ensure that any information divulged has the permission of the references provided. The Bidder must have been the prime contractor, rather than a subcontractor. This means that the Bidder contracted directly with the customer of the work. If the Bidder's contract was to perform work which another entity had itself first contracted to perform, the Bidder will not be considered the prime contractor. For example, Z (customer) contracted with Y for services. Y, in turn, entered into a contract with X to provide all or part of these services		

	to Z. In this example, Y is a prime contractor and X is a subcontractor. Bidders are reminded that a Supply Arrangement or Standing Offer is not a contract and therefore any reference to this type of document will not be accepted for the purpose of evaluating contract experience. For example if the Bidder references it's TBIPS SA number such as EN578-055605/XXX/EL for the purpose of demonstrating experience under the evaluation criteria, Canada will disregard this experience because it does not relate to a specific contract. * Government client may include a Federal, Provincial or Municipal Department/Agency or Crown Corporation. † Informatics Professional Services are professional services provided by the Bidder in support of an information technology or information management project or contract.		

RESOURCE CRITERIA

MANDATORY CRITERIA

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Configuration Management

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Configuration Management				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience planning and implementing IT security solutions.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years performing security architecture design or engineering support in the area of IT security.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the last ten (10) years, planning, developing, implementing and integrating vulnerability assessment solutions.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last eight (8) years, developing and implementing a vulnerability management program for an organization of at least 5,000 users.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience applying Government IT Security policies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience engineering, designing, configuring and integrating Border Protection Service solutions.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Cyber Security Reference Architecture

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Cyber Security Reference Architecture				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the design, planning, and/or implementation of information technology services, such as web services, database services, directory services, user access services, virtualized environments, and/or virtual desktops.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the review, design, planning, and/or implementation of security services, or security architectures for IT systems supporting more than 100 users.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience authoring technical configuration or implementation documentation.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Cross Domain Solution – Access

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Cross Domain Solution – Access				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience developing, configuring and testing of network security controls and policies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of experience designing and delivering virtual desktop services.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of experience designing, configuring and implementing role and rule-based access control models.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M6	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in designing, configuring and implementing IPSec tunneling schemes.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: Cross Domain Solution – Transfer

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: Cross Domain Solution – Transfer				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating High Assurance Guard technologies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of experience configuring and integrating Firewall technologies.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of combined experience engineering, designing, configuring and integrating e-mail content filter (such as malware prevention) and data loss prevention (such as label checking and word checking) technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience engineering, designing, configuring and integrating Border Protection Service solutions.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an IT Security Engineer.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of combined experience composing and maintaining Security Information and Event Management (SIEM) and/or Full Packet Capture (FPC) technical and engineering documentation.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in designing and implementing network security monitoring use cases in an enterprise deployment.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the last ten (10) years designing, deploying and integrating SIEM tools and/or Full Packet Capture (FPC) tools in a production environment.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Full Packet Capture

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Full Packet Capture				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years, working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years, designing, deploying, administering and troubleshooting local and wide-area network communications infrastructure components.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years performing system administration with Linux or a Linux variant.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Host Security				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years, working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of combined experience, within the last seven (7) years, designing, engineering, installing, configuring, and testing endpoint protection security software in an enterprise IT environment. Endpoint protection security software experience must include two (2) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME)			
M3	The Bidder must demonstrate that the proposed resource has a minimum of one (1) year of experience applying IT Security end-point protection policies in an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last seven (7) years developing security architecture design for a Government classified solution (SECRET and above).			
M3	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience using at least one (1) of the following architectural methods/frameworks within the past seven (7) years: • TOGAF; • US government FEAP; • Canadian government BTEP; • Zachman; • SABSA Security Architecture Framework; and/or • Department of National Defence Architecture Framework (DNDAF)			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last seven (7) years conducting detailed ICAM solution requirements analysis, design and implementation.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of one (1) year of experience briefing senior managers (Director level and above) on IT security implications and recommended courses of action.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following security networking technologies: • Guards and Gateways; • Firewalls; • Border Protection Services; • Data Diodes; • Web proxies; and • Mail Transfer Agent. A minimum of two years of experience is required for each of the above technologies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following IT products and infrastructure: • Microsoft Network Operating System; • IP Networks; • Applications Integration; and • Virtualization. A minimum of three years of experience is required for each of the above technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last six (6) years working with common classified networks at the Secret and/or Top Secret level.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Cross Domain Solution – Access

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Cross Domain Solution - Access				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience planning and implementing IT Security integration architectures.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of experience in the design, implementation and change management of network security controls and policies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of virtual desktop services.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of role- and rule-based access control models.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of IPSec tunneling schemes.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M6	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Host Security				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience designing and implementing IT security solutions.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of combined experience, within the last eight (8) years, designing, engineering, installing, configuring, and testing endpoint protection security software in an enterprise IT environment. Endpoint protection security software experience must include three (3) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME)			
M3	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience in the last eight (8) years applying IT Security end-point protection policies to an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Bidder must demonstrate that the resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Network Security – Content Inspection

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Network Security – Content Inspection				
M1	The Bidder must demonstrate that the proposed resource has a minimum ten (10) years of experience within the last fifteen (15) years working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years configuring and integrating networking equipment.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last ten (10) years designing secure architectures while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience in the last eight (8) years configuring, integrating and troubleshooting Firewalls.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience integrating IT security solution Proof of Concepts (POCs).			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience, within the last fifteen (15) years, working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has at least two (2) years of experience, within the last five (5) years developing and implementing an Enterprise Governance, Risk, and Compliance (eGRC) solution for an organization of at least 5,000 users.			
M3	The Bidder must demonstrate that the proposed resource has at least two (2) years of experience within the last five (5) years in the assessment of applied Security Controls, the evaluation of Threats and Risks to an IT system, or the interpretation and application of Information Technology Security Guidance (ITSG) 33 Annex A.			
M4	The Bidder must demonstrate that the proposed resource has at least two (2) years of experience within the last ten (10) years defining requirements, translating business process into workflow, and engineering solutions in the definition and implementation stages of an IT Security project.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as a Network Security Analyst.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience monitoring and analysing security log files from an enterprise network of at least 500 users.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience with the collection and analysis of malicious code from hosts and network traffic.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the last eight (8) years monitoring, configuring and tuning Security Information and Event Management (SIEM) tools and/or Full Packet Capture tools in a production environment.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Security Information and Event Management (SIEM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Security Information and Event Management (SIEM)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as a Network Security Analyst			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last five (5) years configuring and providing technical support for the Security Information and Event Management (SIEM) tool ArcSight in a production environment.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience monitoring and analyzing security log files from an enterprise network of at least 500 users.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design and implementation of SIEM use cases for both servers and workstations in an enterprise deployment.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience building, configuring, and troubleshooting Linux servers.			
	Compliant (Yes/No)?			

C.12 Incident Management Specialist – Level 3
Specific Task Title: Security Information and Event Management (SIEM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.12 Incident Management Specialist – Level 3 Specific Task Title: Security Information and Event Management (SIEM)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an Incident Management Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years implementing and providing technical support for the Security Information and Event Management (SIEM) tool ArcSight in a production environment.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design and implementation of SIEM use cases for both servers and workstations in an enterprise deployment.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience building, configuring, and troubleshooting Linux servers.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience composing and maintaining SIEM documents or SIEM engineering deliverables.			
	Compliant (Yes/No)?			

RATED CRITERIA

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Configuration Management

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Configuration Management					
R1	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Bidder should demonstrate that the proposed resource has experience performing options analysis of IT security tools and techniques.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R3	The Bidder should demonstrate that the proposed resource has experience planning, developing, implementing and integrating IT asset discovery or configuration management database (CMDB) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R4	The Bidder should demonstrate that the proposed resource has experience in planning, developing, implementing and integrating automated configuration compliance auditing solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience writing technical reports such as requirements analysis, options analysis, and technical architecture documents.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R6	The Bidder should demonstrate that the proposed resource has experience developing hardening guides for IT systems.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The proposed resource should hold one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 19 points**	**Maximum Score: 27 points**		

C.6 – Information Technology Security Engineer - Level 2
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 – Information Technology Security Engineer - Level 2 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing proxy solutions, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Cyber Security Reference Architecture

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Cyber Security Reference Architecture					
R1	The Bidder should demonstrate that the proposed resource has at least 6 months experience designing, or co-designing one major scale IT (Information Technology) environment for a minimum of 100 users.	IT supporting users: 3 points: 100 to 300 users. 4 points: >300 to 1000 users. 5 points: >1000 or more users.	5		
R2	The Bidder should demonstrate that the proposed resource has experience working in the application of IT Security Risk Management processes or System Security Engineering processes.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience designing or implementing and configuring IT Intrusion Detection and Protection methodologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience working with the design or implementing and configuring System Monitoring for accesses, changes or operational status.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience designing or implementing and configuring IT Enterprise Services, including directory, single sign-on, email, backup, or distributed database for an IT system supporting at least 500 users.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience designing or implementing and configuring IT Defence in Depth principles. The Bidder should also demonstrate and provide a description of how the resource applied the principles.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience working with a recognized enterprise architecture framework.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R8	The Bidder should demonstrate that the proposed resource has experience writing technical documents using desktop office-class tools, for audience at the corporate level.	1 point: 1 to 2 years of experience. 2 points: >2 to 4 years of experience. 3 points: >4 to 6 years of experience 4 points: >6 years of experience.	4		
	Total:	**Minimum Passing Score: 19 points**	**Maximum Score: 27 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Cross Domain Solution – Access

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Cross Domain Solution – Access					
R1	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.6 - Information Technology Security Engineer - Level 2
Specific Task Title: Cross Domain Solution – Transfer

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 2 Specific Task Title: Cross Domain Solution – Transfer					
R1	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.6 - Information Technology Security Engineer - Level 2
Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 2 Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning					
R1	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing proxy solutions, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Red Hat Enterprise Linux (RHEL).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R8	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 17 points**	**Maximum Score: 24 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Bidder should demonstrate that the proposed resource has experience in the last ten (10) years engineering network security monitoring solutions using at least three (3) of the following security technologies: 1) Host-based security; 2) IDS/IPS (Intrusion Prevention System); 3) Firewalls/UTMs; 4) Full Packet Capture; 5) Proxies; 6) Load Balancers; and 7) Matrix Switches/Taps.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Bidder should demonstrate that the proposed resource has experience within the last ten (10) years designing network security monitoring solutions for the Government based on IT Security Directive (ITSD) 02 or IT Security Guidance (ITSG) 22 at the Protected B level or higher.	1 point per project up to a maximum 3 projects*† *If a Bidder provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		
R4	The Bidder should demonstrate that the proposed resource has experience providing IT security engineering services to Government departments and agencies in the form of security architecture development, advice and guidance.	1 point: 3 to 5 years of experience. 2 points: >5 to 7 years of experience. 3 points: >7 to 9 years of experience. 4 points: >9 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate the proposed resource holds one or more of the following IT security certifications: 1) International Information Systems Security Certification Consortium $(ISC)^2$ CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA) A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 16 points**		

C.7 - Information Technology Security Design Specialist - Level 2
Specific Task Title: Full Packet Capture

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 2 Specific Task Title: Full Packet Capture					
R1	The Bidder should demonstrate the proposed resource has experience within the last seven (7) years designing, planning and implementing network infrastructure of complex and highly available* environments. *Complex and highly available environments are defined as environments spanning multiple cities or countries with zero-downtime.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R2	The Bidder should demonstrate that the proposed resource has combined experience within the last ten (10) years performing one or more of the following IT-related tasks: 1. Writing technical reports such as requirement analysis, options analysis, engineering process artefacts and/or technical architecture documents; 2. Automating the administration of Linux systems through scripting and APIs such as (but not limited to) Ruby, PHP, Bash, Perl or Python; 3. Analysis of raw network traffic capture to support troubleshooting or network forensics; 4. Deployment and administration of network forensics or traffic monitoring devices such as (but not limited to) FireEye, Solera, Sourcefire/Cisco IDS/IPS, SNORT or Netwitness (RSA Security Analytics); 5. Review alerts and packet-level data from IDS sensors/ packet capture devices;	1 point: 6 to 9 months of experience. 2 points: >9 to 12 months of experience. 3 points: >12 to 15 months of experience. 4 points: >15 months of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R2	6. Malware analysis and sandboxing with applications like (but not limited to) Netwitness Spectrum/RSA Malware, WireShark, CaptureBAT or Cuckoo Sandbox and the ability to reverse engineer and debug malware samples using tools such as (but not limited to) IDA Pro, Responder Pro or OllyDbg, including defeating anti debugging, packing and obfuscation techniques; and/or 7. Management of SAN and NAS technologies – Fibre Channel, FCOE, iSCSI, NFS, CIFS, including but not limited to the provisioning of LUNs, cabling, troubleshooting and patching. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.				

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Bidder should demonstrate that the proposed resource has one or more of the following IT security certifications: 1) RSA Security Analytics Certified Administrator; 2) Any Cisco Associate level certification; 3) Any Cisco Professional level certification; 4) Any Cisco Expert level certification; 5) Any SANS GIAC certification in the Security Administration category; 6) Any Redhat Certified System Administrator, Engineer and/or architect certification; A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 or more certifications.	5		
	Total:	**Minimum Passing Score: 8 points**	**Maximum Score: 12 points**		

C.7 - Information Technology Security Design Specialist - Level 2
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 2 Specific Task Title: Host Security					
R1	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience implementing centrally managed host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience implementing McAfee, Symantec or Trend-Micro host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has a minimum one (1) year each of experience engineering and implementing the following host-based security technologies, in an enterprise IT environment: 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; or 3) Trend-Micro Control Manager.	1 point: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 2 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 3 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	3		
R5	The Bidder should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec, or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		
R6	The Bidder should demonstrate that the proposed resource has experience evaluating various IT security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Bidder provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Bidder should demonstrate that the proposed resource has experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and 9) Other Content Inspection systems. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Bidder should demonstrate that the proposed resource holds at least one of the following IT security certifications: 1) ISC2 Certified Information System Security Professional (CISSP); 2) ISC2 Certified Cloud Security Professional (CCSP); 3) ISC2 Systems Security Certified Professional (SSCP); and/or 4) Global Information Assurance Certification (GIAC) certification (any). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 or more certifications.	5		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 26 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)					
R1	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years developing Standard Operating Procedures (SOP) on projects.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years designing and deploying PKI technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years designing and deploying Identity, Credential and Access Management (ICAM) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months experience designing IT solutions requiring interoperability with: • one or more GoC departments; and/or • one or more of the following International partners: US, UK, AUS, NZ.	1 point: demonstrated at least six (6) months of experience designing IT solutions requiring interoperability with GoC department(s). 2 points: demonstrated at least six (6) months of experience designing IT solutions requiring interoperability with International partner(s) (US, UK, AUS, NZ)	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years designing process mapping for a security architecture design.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Firewall technologies, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing proxy technologies, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP technologies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware technology.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent versions), Active Directory and Domain Name System in large (at least 1,000 users) IT networks.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Cross Domain Solution – Access

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Cross Domain Solution – Access					
R1	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has combined experience performing at least three (3) the following IT Security tasks: 1) Analysis of IT Security tools and techniques; 2) Analysis of security data and provision of advisories and reports; 3) Writing technical reports including requirements analysis, options analysis, technical architecture documents and mathematical risk modeling; 4) Security architecture design and engineering support; and 5) Data security classification studies. A minimum of six (6) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent versions) Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience in design, implementation and change management of VMWare Technologies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource holds one or more of the following architecture certifications: 1) Certification in The Open Group Architecture Framework (TOGAF); 2) Certification in Information Technology Service Management (ITSM); 3) Certification in Enterprise Architecture Center of Excellence (EACOE); 4) Certification in Microsoft Certified Architect (MCA); and/or 5) Certification in VMWare Certified Design Expert (VCDX). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Host Security					
R1	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience implementing centrally managed host-based endpoint security policies in an enterprise IT environment.	1 point: 2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience implementing McAfee host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has a minimum one (1) year each of experience engineering and implementing the following host-based security technologies, on an enterprise IT environment: 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; or 3) Trend-Micro Control Manager.	1 point: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 2 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 3 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	3		
R5	The Bidder should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec, or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		
R6	The Bidder should demonstrate that the proposed resource has experience evaluating various security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Bidder provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Bidder should demonstrate that the proposed resource has experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and 9) Other Content Inspection systems. A minimum of six (6) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Network Security – Content Inspection

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Network Security – Content Inspection					
R1	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco technologies including Routers, and/or Nexus and Catalyst Series Switches.	1 point: 5 to 6 years of experience. 2 points: >6 to 7 years of experience. 3 points: >7 to 8 years of experience. 4 points: >8 years of experience.	4		
R2	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and troubleshooting Palo Alto firewalls.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience working with application aware traffic generators.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience working with Intrusion Detection Systems (IDS).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience working with VMWare.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning F5 load balancers.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience working with inline network encryption technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Bidder should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 25 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Enterprise Governance, Risk, and Compliance (eGRC)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Enterprise Governance, Risk, and Compliance (eGRC)					
R1	The Bidder should demonstrate that the proposed resource holds one or more of the following administrating IT GRC or eGRC application certifications: 1) RSA Archer Certified Administrator 2) IBM OpenPages Administrator 3) MetricStream GRC Certified Administrator A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
R2	The Bidder should demonstrate that the proposed resource has combined experience within the last five (5) years authoring XML data transformation and/or translation scripts.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience with IT Security Design projects within an eGRC implementation environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years writing technical reports such as options analysis, and/or implementation plans.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has combined experience within the last five (5) years accrediting an IT system using the Security Assessment and Authorization (SA&A) process and/or the Certification and Accreditation (C&A) program.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years developing network security architectures (Level II or higher) based on IT Security Directives (ITSD) and /or IT Security Guidance (ITSG).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Bidder should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications	3		
	Total:	**Minimum Passing Score: 16 points**	**Maximum Score: 23 points**		

C.8 – Network Security Analyst - Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 – Network Security Analyst - Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Bidder should demonstrate that the proposed resource has experience in the last ten (10) years performing network security monitoring and log analysis to detect malicious activity.	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and optimizing production Security Information and Event Management System (SIEM) and/or Full Packet Capture solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		
R3	The Bidder should demonstrate that the proposed resource has experience providing IT security incident detection, analysis and handling services using automated Security Information and Event Management System (SIEM) tool(s).	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience operating and configuring all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
R6	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of experience reviewing, developing and implementing incident handling and escalation process flows in an IM/IT project.	1 point = 1 project. 2 points = 2 projects. 3 points = 3 or more projects. A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Bidder should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) International Information System Security Certification Consortium (ISC)2 CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE); A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 14 points**	**Maximum Score: 20 points**		

C.8 – Network Security Analyst - Level 3
Specific Task Title: Security Information and Event Management (SIEM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 – Network Security Analyst - Level 3 Specific Task Title: Security Information and Event Management (SIEM)					
R1	The Bidder should demonstrate that the proposed resource has experience in the last seven (7) years performing network security monitoring and log analysis to detect malicious activity.	1 point: 2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and maintaining production SIEM solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		
R3	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years providing technical support to at least three (3) of the following network security technologies: 1) Host-based security 2) IDS/IPS (Intrusion Prevention System) 3) Firewalls/UTMs 4) Proxies 5) Load Balancers 6) Matrix Switches/Taps	1 point: 2 to 5 months of experience. 2 points: >5 months of experience.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience deploying and operating all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience tuning and configuring SIEM components to improve efficiency, accuracy, and performance.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience in the last seven (7) years working in an in-service support/helpdesk environment.	1 point: 1 to 6 months of experience. 2 points: >6 months of experience.	2		
R7	The Bidder should demonstrate that the proposed resource completed ArcSight specific training and/or holds a current certification for ArcSight Technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
	Total:	**Minimum Passing Score: 13 points**	**Maximum Score: 18 points**		

C.12 – Incident Management Specialist - Level 3
Specific Task Title: Security Information and Event Management (SIEM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.12 – Incident Management Specialist - Level 3 Specific Task Title: Security Information and Event Management (SIEM)					
R1	The Bidder should demonstrate that the proposed resource has experience in the last seven (7) years performing network security monitoring and log analysis to detect malicious activity.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and maintaining production SIEM solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		
R3	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years providing technical support to at least three (3) of the following network security technologies: 1) Host-based security 2) IDS/IPS (Intrusion Prevention System) 3) Firewalls/UTMs 4) Proxies 5) Load Balancers 6) Matrix Switches/Taps	1 point: 2 to 5 months of experience. 2 points: >5 months of experience.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience deploying and operating all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience tuning and configuring SIEM components to improve efficiency, accuracy, and performance.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience in the last seven (7) years working in an in-service support/helpdesk environment.	1 point: 1 to 6 months of experience. 2 points: >6 months of experience.	2		
R7	The Bidder should demonstrate that the proposed resource completed ArcSight specific training and/or holds a current certification for ArcSight Technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
	Total:	**Minimum Passing Score: 13 points**	**Maximum Score: 18 points**		