Various Senior Cyber Protection Services Class Resources to Provide Level 2 support to the Federal Information Protection Centre

REQUEST FOR PROPSAL

AMENDMENT NO. 3

This RFP amendment No. 3 is raised to;

1- Extend the RFP closing date by one week to October 01, 2014;
2- Make administrative changes; and
3- Publish Canada's responses to Industry questions received during the question period.

1. At the RFP cover page, 'Solicitation Closes' REVISE as follows.

DELETE: 24 September 2014

INSERT: 01 October 2014

2. At Part 3 of the RFP 'Bid Preparation Instructions', article 3.1 'Bid Preparation Instructions' REVISE as follows:

DELETE: (iii) Section III: Certifications (1 hard copy)

3. At Attachment 1 to Part 4 of the RFP, REVISE as follows:

DELETE: the previous version in its entirety.

INSERT: the following new version attached hereto this amendment.

4. At Appendix A to Annex A, REVISE as follows:

DELETE: the previous version in its entirety.

INSERT: the following new version attached hereto this amendment.

5. Publish Canada's responses to Industry questions received during the question period.

Question	Answer
#7 Question re: 2.1.4 M2: CISSP is a non-technical certification that does not demonstrate competency for many installation specialist activities. Vendor or product-specific certifications are more appropriate for individual TA requirements. Please consider making CISSP a rated requirement on this solicitation and adding vendor product certifications in several categories (firewall, IDS, routing/switching, and/or OS) as acceptable certifications.	Please see the updates to Appendix A to Annex A related to Certifications.

#31- Please confirm that Shared Services Canada (SSC) cannot be used as a reference for this Solicitation as it would be a conflict of interest having the same entity act as both the RFP issuer and a reference.	Bidders are permitted to use applicable SSC contracts as references for this solicitation.
#32- SSC's response to question 27 & 28 in amendment 2 of Solicitation 13-18653/A does not answer the questions. As the original organization that asked the question – we recognized that it is common for SSC to measure bidders billable days in relevant personnel categories, however the intent of our inquiry was to question the amount of days and the restrictions SSC puts against measuring bidders. Requesting greater than 34 years of experience for a one year contract (+ two one year options) in not in line with any RFP from Canada we have seen. It is unrealistic for an organization to demonstrate the experience being asked in M1 and R1 under the following strict criteria: • Five contracts • Within the last 5 years • Contracts with a minimum value of $1M The original question also did not suggest that references were limited to Government of Canada, rather we were suggesting that the Government of Canada (GoC) is the largest consumer of IT Security services in the country and this type of experience would be limited to GoC. SSC's response to question 15 showing Bell Canada's SCNet contract with SSC valued at $2,980,000.00 last year validates this concern. In an effort to open the bidding process to extremely experienced organizations with a proven track record of providing IT Security services in the categories requested we request that SSC substitute within M1 & R1 the following: Remove the following: The services provided must have been provided under a maximum of five contracts. It is not necessary for each contract to demonstrate all categories of personnel. Referenced contracts must have an excess ("Billed") value in excess of	SSC will accept a maximum of 10 reference contracts to demonstrate the experience required in M1 and R1.

$1M. Insert the Following: The services provided must have been provided under a maximum of ten contracts. It is not necessary for each contract to demonstrate all categories of personnel. Referenced contracts must have an excess ("Billed") value in excess of $1M. If SSC chooses not to make the change, please provide reasoning and highlight how making this change would compromise the goal of the mandatory and Rated criteria M1 & R2. Additionally please comment on how not making the change will address the national Procurement strategy initiative relating to fair procurement	
#33- SSC's response to question 29 within Amendment two (2) highlights the need for bidders to demonstrate a record of providing high volume delivery to a single client within the NCR. Although the reference client is not limited to Government of Canada, SSC will likely be the only organization within the NCR that 30 or more resources would have been placed in the 12-24 months; this ask may limit 70% - 100% scores to incumbent organization as identified in Question /Answer 15 , significantly limiting the number of qualified security organizations that will be able to bid. Given the desire is to demonstrate the ability to provide high volume of resources – we request that R2 be changed to include multiple clients, for individual consultants (resources can only be counted once). By limiting to individual consultants, a resource will not be able to be counted more than once, ensuring that the bidding organization has the necessary bench strength to fulfill forecasted requirements. If SSC chooses not to make the change, please provide reasoning and highlight how making this change would compromise the goal of the mandatory and Rated criteria M1 & R2. Additionally please comment on how not making	SSC has considered this request and maintains its position regarding R2. For better clarity with R2, please see the new Attachment 1 to Part 4 attached hereto this amendment.

the change will address the national Procurement strategy initiative relating to fair procurement	
#34- Section 1.2 (Summary) says "It is intended to result in the award of a maximum of four contract(s) for one year…" Can you please confirm that Canada will award contracts to all vendors that qualify (up to four) to take part in the TA process as outlined in the solicitation? In other words, if 4 qualify, Canada does not reserve the right to limit the number of contracts awarded to less than four?	Confirmed.
#35- We respectfully respect an extension to October 8th, 2014 due to the fact that the existing extension provided in amendment 2 to September 24th was issued on September 11th and does not allow enough time for follow up questions and answers.	An extension to the closing date has been provided in this RFP amendment.

ALL OTHER TERMS AND CONDITIONS OF THIS INVITATION TO QUALIFY REMAIN UNCHANGED.

==========

Following is a summary of Amendments issued to date to this Request for Proposal (RFP)

Document Tracking	Date	Description
Amendment No. 001	August 26, 2014	Administrative changes and published responses to questions
Amendment No. 002	September 04, 2014	Extend the bid closing date, administrative changes and publish responses to questions
Amendment No. 003	September 18, 2014	Extend the bid closing date, administrative changes and publish responses to questions

ATTACHMENT 1 TO PART 4
Evaluation Criteria

1. Evaluation Disclaimer

The mandatory criteria will be evaluated on a "Met/Not Met" (i.e. compliant/non-compliant) basis. Proposals **must** demonstrate compliance with all of the following Mandatory requirements and must provide the necessary documentation to support a determination of compliance. Proposals that fail to meet any mandatory requirements will be deemed non-compliant and will be given no further consideration.

The Contracting Authority reserves the right to request reference(s)* from any of the SA Holder's listed projects to verify and validate the information stated in the proposal. If the reference is unable to verify or validate the information stated in the proposal, the bid will be deemed non-compliant.

2. Customer Reference Contact Information

The Bidder must provide customer references for point rated requirements R2 and R3 who must each confirm, the facts identified in the Bidder's bid. For each customer reference, the Bidder must, at a minimum, provide the name and either the telephone number or e-mail address for a contact person. Bidders are also requested to include the title of the contact person. If the named individual is unavailable when required during the evaluation period, the Bidder may provide the name and contact information of an alternate contact from the same customer.

Canada is not obliged to, but may in its discretion contact the Primary reference and, where applicable, the Backup reference, in order to validate the information submitted for point rated requirements R2 and R3. Canada may conduct any Project Reference validation check in writing by e-mail. Canada will email (cc) the Respondent's contact when an e-mail is sent out for Project Reference validation checks.

If Canada chooses to contact one or more references to validate information provided by a Bidder, Canada must receive the reference's response within 5 Federal Government Working Days (FGWDs) from the date of the request. If Canada does not receive confirmation (within 5 FGWDs) from either the Primary or Backup reference that the information in their bid is accurate (or that any inaccuracies are not material to whether or not the project meets the mandatory requirements), that Bidders Project Reference will not be considered in the evaluation. Canada may also contact a Primary or Backup reference for clarification purposes, either by email or by telephone.

If during a bid validation by Canada it becomes apparent that the address, telephone number, or email address for any of the references is incorrect or missing, the Bidder will be permitted to provide the correct address, telephone number, or email address within 1 FGWD of a request. If the named individual for the Primary reference is unavailable because they are on leave, or no longer working for that organization, Canada will contact the Backup reference from the same customer organization.

The Bidder will not be permitted to submit an alternate customer organization or project as a reference for the RFP after the bid closing date.

3. Mandatory Criteria

<table>
<tr><th colspan="4">Corporate Mandatory Requirement</th></tr>
<tr><th>Criteria</th><th>Mandatory Requirement</th><th colspan="2">Bidders Response</th></tr>
<tr><td></td><td></td><td>Met</td><td>Not Met</td><td>Reference to Additional Documentation within the Bid</td></tr>
<tr><td>M1</td><td>The Bidder must have demonstrated contract experience in supplying all of the following resource categories, for the required Mandatory Billable Days per category.
<table>
<tr><th>Category of Personnel</th><th>Mandatory Minimum Number of Billable Days</th></tr>
<tr><td>IT Security Vulnerability Assessment (VA) Specialist</td><td>1600</td></tr>
<tr><td>IT Security Engineer</td><td>1000</td></tr>
<tr><td>Computer Forensics Specialist</td><td>1800</td></tr>
<tr><td>IT Security Incident Management Specialist</td><td>2000</td></tr>
<tr><td>IT Security Methodology, Policy and Procedures Analyst</td><td>600</td></tr>
<tr><td>IT Security Installation Specialist</td><td>600</td></tr>
</table>
Bidders must complete Appendix A and B to Part 4.

The services provided must have been provided under a maximum of ten (10) contracts. It is not necessary for each contract to demonstrate all categories of</td><td></td><td></td><td></td></tr>
</table>

Corporate Mandatory Requirement				
	personnel. Referenced contracts must have an excess (“Billed”) value in excess of $1M. The experience must occur within the past five years prior to the RFP closing date. The experience may occur at any time during the five year period, so long as the-total number of Billable Days when added together meets the Minimum Billable Days requirement. The work delivered by the Category of Personnel must include at least 70% of the associated tasks listed in the Statement of Work of this bid solicitation for that Category of Personnel.			

This page has been left intentionally blank.

4. Point-Rated Technical Criteria

Corporate Rated Requirements

#	Rated Evaluation Criteria	Points Max	Bidder's Response: Demonstrated Experience	Bidder's Response: Reference to Extra Documentation Within The Bid
R1	The Bidder should demonstrate its billable days experience in excess to the minimum billable days under M1. The Bidder's demonstrated "Total Billable Days" provided in response to M1 will be used to evaluate this criterion. **Example Evaluation Scenario:**	**100**		

	Billable DAYS			
	(A)	(B)	(C)	(D)
CATEGORY OF PERSONNEL	TOTAL BILL DAY PROVIDED BY BIDDER	MINIMUM DAYS REQUIRED UNDER M1	BIDDER EXCESS	BIDDERS % INCREASE TO A MAXIMUM 100 PTS
IT Security Vulnerability Assessment (VA) Specialist	2175	1600	575	35.94
IT Security Engineer	1225	1000	225	22.5

Corporate Rated Requirements

#	Rated Evaluation Criteria	Points Max	Bidder's Response: Demonstrated Experience	Bidder's Response: Reference to Extra Documentation Within The Bid

Computer Forensics Specialist	4000	1800	2200	100.00
IT Security Incident Management Specialist	3000	2200	800	36.36
IT Security Methodology, Policy and Procedures Analyst	850	600	250	41.67
IT Security Installation Specialist	800	600	200	33.33
BIDDER SCORE = SUM (D) / # of CATEGORIES				
Sum (D) / 6 = 44.97				

The Bidder will be awarded points for billable days in excess of the minimums identified under M1 as demonstrated in the example evaluation scenario provided below. In this example the Bidder would score 44.97 points out of a possible 100 points.

Bidders must complete Appendix A and B to Part 4

Corporate Rated Requirements				
			Bidder's Response	
#	Rated Evaluation Criteria	Points Max	Demonstrated Experience	Reference to Extra Documentation Within The Bid
R2	SSC believes that the most significant risk associated with this contract is that the Contractor will be unable to provide the required number of qualified resources, in the required categories/level, within the timeframe specified in the Task Solicitation process. Vendors should demonstrate their ability to supply, manage and retain large groups of resources in support of a single client/project within the region of delivery. Bidders should supply a single client contract with a contact reference within the past 24 months encompassing a minimum of 10 resources in the NCR in support of a single client project for a minimum six consecutive months To be considered, reference project information must include: • Client Organization Name • Client Contact name and Title • Client Contact Phone # • Client Contact Email Address • Project start and end dates (yy/mo) • Total number of PS resources provided for a 6 month period within the last 24 months	**50**	• **10 points**- A team of 10 resources were provided to a single client in the NCR; • **25 points**- A team of 15 resources were provided to a single client in the NCR; • **35 points**- A team of 25 resources were provided to a single client in the NCR; • **50 points**- A team of 30, or more, resources were provided to a single client in the NCR.	

Corporate Rated Requirements				
			Bidder's Response	
#	Rated Evaluation Criteria	Points Max	Demonstrated Experience	Reference to Extra Documentation Within The Bid
R3	The Bidder should describe its proposed Risk Mitigation strategy, including the approach and or measures it proposes to undertake, to ensure its ability to propose fully qualified resources to Shared Services Canada (SSC) within 5 days of receipt of a TA Request. The Bidder's mitigation strategy should include current corporate processes, as well as specific measures it proposes to implement to manage the resulting contract. In addition, the Bidder must provide a single Reference Project where it has successfully used a similar/same approach to ensure the timely provision of qualified resources to the client. To be considered, the reference project information must include: • Client Organization Name • Client Contact Name and Title • Client Contact Phone Number • Client Contact Email Address • Project start and end dates (yy/mo) • A description of the approach and/or measures implemented to ensure the timely provision of qualified resources to the client	**150**	*The extent to which the proposed risk mitigation strategy is fully and clearly described:* • **30 points:** The risk mitigation strategy is described; • **75 points:** The risk mitigation strategy is reasonably described with a good level of detail of existing corporate processes, • **100 points:** The risk mitigation strategy is thoroughly described, including complete details of existing supporting corporate processes and specific measures to be implemented. *Relevance of the proposed risk mitigation strategy to ensure the timely provision of qualified*	

Corporate Rated Requirements				
			Bidder's Response	
#	Rated Evaluation Criteria	Points Max	Demonstrated Experience	Reference to Extra Documentation Within The Bid
			resources: • **15 points**: Response proposes a risk mitigation strategy (i.e. methods and/or activities) that demonstrates a minimal understanding of the stated risk; • **25 points:** Response proposes a risk mitigation strategy (i.e. methods and/or activities) which demonstrates some understanding of the stated risk; • **35 points:** Response proposes a risk mitigation strategy (i.e. methods and/or activities) which demonstrates a good understanding of the stated risk; • **50 points:** Response proposes a risk mitigation strategy (i.e. methods	

Corporate Rated Requirements				
			Bidder's Response	
#	Rated Evaluation Criteria	Points Max	Demonstrated Experience	Reference to Extra Documentation Within The Bid
			and/or activities) which demonstrates a clear and profound understanding of the stated risk.	
	Maximum Points Available:	300		
	Minimum Score Required:	210		
	Bidder's Score:			

Appendix A to Annex A

Mandatory and Rated Requirements for the Task Solicitation Process

1.0 General Information

1.1 All work to be completed pursuant to this Contract will be authorized under the process detailed in Contract article 6.2.

1.2 In accordance with Task Solicitation of the Contract, the Contractor will be asked to submit resumes for each of the resources they propose to work on a Task Authorization (TA) requested by Canada.

1.3 The resource will be evaluated by the Technical Authority against the mandatory and rated requirements contained in the task authorization.

1.4 To be awarded an approved Task Authorization, the proposed Contractor resource must meet all of the mandatory requirements, and receive the highest score on the rated requirements.

2.0 Mandatory Requirements

2.1 The following are the mandatory requirements which will be used to evaluate each proposed resource in the relevant resource category of the TA:

2.1.1 Senior IT Security Methodology, Policy and Procedures Analyst Level II

Criteria	Mandatory Requirement	Demonstrated Experience	Project #
M1	The proposed resource must possess five (5) years of recent experience in interpreting and applying Government of Canada (GoC) IT Security Policy.		
M2	Demonstrate a minimum of five (5)years of experience working with IT security.		
M3	Demonstrate a minimum of three (3) years of experience providing IT security advice and guidance.		
M4	The proposed resource must hold a valid security clearance at the Secret level at a minimum.		

2.1.2 Senior IT Security Incident Management Specialist Level II

Criteria	Mandatory Requirement	Demonstrated Experience	Project #
M1	The proposed resources must hold a valid University degree at the Bachelor level in Sciences, Engineering, Mathematics and a minimum of one (1) year of work experience related to vulnerability analyst duties. Or A college diploma in Computer Engineering Technology, Computer Technology (computer science) and a minimum of two (2) years of work experience related to the incident management duties listed in Annex A Section 4.2. Or A minimum of four (4) years of work experience related to the incident management duties listed in Annex A Section 4.2.		
M2	The proposed resource must hold a Certified Information Systems Security Professionals (CISSP) or a Certified Information Security Manager (CISM) or a Certified Information Systems Auditor (CISA) designation. *Or* *A SANS GIAC Certified Incident Handler (GCIH) certification.* *Or* *A SANS GIAC Certified Intrusion Analyst (GCIA) certification..* *Or* *A minimum 5 years demonstrated experience in security incident handling in the last 8 years with a minimum of 3 years in the last 5 years. The bidder will also need to provide 2 references (with full valid contact information) for each proposed resource related to the experience being demonstrated which must be available for consultation to the crown during the evaluation period. At least one reference must be in relation to the work performed in the last 3 years.* The Bidder will be requested proof of certification for the proposed resource before Contract Award.		
M3	Proposed resources must hold a valid security clearance at a minimum level of Secret – and in certain cases some of the proposed resources must hold a valid security clearance at Top Secret.		

2.1.3 Senior IT Security Engineer Level II

Criteria	Mandatory Requirement	Demonstrated Experience	Project #
M1	University degree at the Bachelor level in Sciences, Engineering, Mathematics and; a minimum of one (1) year working in the designing and deployment of Security *Solutions for which the resource is being proposed (for example, a resource proposed for Security Information and Event Management (SIEM), would need to have a minimum of one (1) year working in the design and deployment of Security Information and Event Management (SIEM))* Or A college diploma in Computer Engineering Technology, Computer Technology (computer science) or other computer technology and; a minimum of two (2) years working in the designing and deployment of Security *Solutions*. Or A minimum of five (5) years of experience working in the designing and deployment of Security *Solutions*		
M2	*Where the proposed resources is being put forth under Security Information and Event management (SIEM), t*he proposed resource must be an ArcSight Certified Professional (ACP). The contractor will be requested proof of certification for the proposed resource.		
M3	Must hold a minimum of a valid Secret Security Clearance issued by PWGSC-CISD and provide both file number and expiry date.		

2.1.4 Senior IT Security Installation Specialist Level II

Criteria	***Mandatory Requirement***	***Demonstrated Experience***	***Project #***
M1	University degree at the Bachelor level in Sciences, Engineering, Mathematics and; a minimum of one (1) year related to a Senior IT Security Installation Specialist duties		

	Or A three (3) year college diploma in Computer Engineering Technology, Computer Technology (computer science) or other computer technology related field and; a minimum of two (2) years related to a Senior IT Security Installation Specialist duties Or A minimum of five (5) years of experience related to a Senior IT Security Installation Specialist duties		
M2	The proposed resource must hold a Certified Information Systems Security Professional designation. *Or* *A SANS GIAC Security Expert certification (GSE).* *Or* *A minimum 5 years demonstrated experience in security systems installations in the last 8 years with a minimum of 3 years in the last 5 years. The bidder will also need to provide 2 references (with full valid contact information) for each proposed resource related to the experience being demonstrated which must be available for consultation to the crown during the evaluation period. At least one reference must be in relation to the work performed in the last 3 years* The Contractor will be requested proof of certification for the proposed resource.		
M3	The proposed resource must hold a minimum of a valid Secret Security Clearance issued by PWGSC-CISD and provide both file number and expiry date.		

2.1.5 Senior Computer Forensic Specialist Level II

Criteria	**Mandatory Requirement**	**Demonstrated Experience**	**Project #**
M1	University degree at the Bachelor level in Sciences, Engineering, Mathematics or other and; a minimum of one (1) year related to the IT Security Forensic Specialist duties listed in Annex A Section 4.4. Or		

	A college diploma in Computer Engineering Technology, Computer Technology (computer science) or other computer technology and; a minimum of two (2) years related to the IT Security Forensic Specialist duties listed in Annex A Section 4.4 Or A minimum of five (5) years of experience related to the IT Security Forensic Specialist duties listed in Annex A Section 4.4		
M2	The proposed resource must hold a Certified Information Systems Security Professionals (CISSP) or Certified Information Security Manager (CISM) or Certified Information Systems Auditor (CISA) designation. *Or* *A SANS GIAC Certified Forensics Analyst certification (GCFA)* *Or* *A SANS GIAC Computer Forensics Examiners certification (GCFE)* *Or* *A minimum 5 years demonstrated experience in IT forensics in the last 8 years with a minimum of 3 years in the last 5 years. The bidder will also need to provide 2 references (with full valid contact information) for each proposed resource related to the experience being demonstrated which must be available for consultation to the crown during the evaluation period. At least one reference must be in relation to the work performed in the last 3 years* The Bidder will be requested proof of certification for the proposed resource before Contract Award.		
M3	The proposed resource must be fluent in both official languages of Canada (English and French).		
M4	Must hold a minimum of a valid Top Secret Security Clearance issued by PWGSC-CISD and provide both file number and expiry date.		

2.1.6 Senior IT Security Vulnerability Assessment (VA) Specialist Level II

Criteria	Mandatory Requirement	Demonstrated Experience	Project #
M1	University degree at the Bachelor level in Sciences, Engineering, Mathematics And; a minimum of one (1) year related to the vulnerability analyst duties listed in Annex A Section 4.6. Or A college diploma in Computer Engineering Technology, Computer Technology (computer science) or other computer technology and; a minimum of two (2) years related to the vulnerability analyst duties listed in Annex A Section 4.6. Or A minimum of three (3) years of experience related to the vulnerability assessment duties listed in Annex A Section 4.6.		
M2	The proposed resource must hold a Certified Information Systems Auditor (CISA) designation. *Or* *A SANS GIAC Penetration Testing certification (GPEN)* *Or* *A SANS GIAC Auditing Wireless Network certification (GAWN)* *Or* *A SANS GIAC Exploit Researcher and Advanced Penetration Tester certification (GXPN)* *Or* *A minimum 5 years demonstrated experience in performing IT Vulnerability Assesments or IT Penetration Testing in the last 8 years with a minimum of 3 years in the last 5 years. The bidder will also need to provide 2 references (with full valid contact information) for each proposed resource related to the experience being demonstrated which must be available for consultation to the crown during the evaluation period. At least one reference must be in relation to the work performed in the last 3 years* The Bidder will be requested proof of certification for the proposed resource before Contract Award.		

M3	Must hold a minimum of a valid Secret Security Clearance issued by PWGSC-CISD and provide both file number and expiry date.		

3.0 Point-Rated Requirements

3.1 The following examples are some, but not an exclusive list, of, the point-rated requirements which will be used to create evaluation grids for each proposed resource in the relevant resource category of the Task Solicitation process:

3.1.1 Senior IT Security Methodology, Policy and Procedures Analyst Level II

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R.1	The proposed resource should have RECENT experience performing IT security tasks in any the following areas: a) PKI b) Certification and Accreditation (C&A) c) Business Continuity and Contingency Planning (BCP) The experience claimed can be obtained either as a Methodology, Policy and Procedures Analyst or in the direct performance of the tasks related to the activity listed in Annex A Section 4.1	**15**	RATED POINT SCORE: • One year of experience demonstrated in PKI = **5 points** • One year of experience demonstrated in C&A = **5 points** • One year of experience demonstrated in BCP = **5 points**
R.2	The proposed resource should have RECENT experience interpreting and applying Management of Information Technology Security (MITS) standards or its predecessor the Information Technology Security Standard, Chapter 2-3 of the Treasury Board Information and Administrative Management Security Manual.	**25**	RATED POINT SCORE: • 12 to 18 months: **5 points** • >18 to 24 months: **10 points** • >24 to 30 months: **15 points** • >30 to 36 months: **20 points** • >36 months: **25 points**
R.3	Using project reference where applicable, the proposed resource should have experience working in the Government of Canada.	**15**	RATED POINT SCORE: • 0– 1 years: **5 points** • 1– 3 years: **10 points**

			• More than 3 years: **15 points**
R.4	The proposed resource should have experience with the virtual technologies vmware.	**15**	RATED POINT SCORE: • Less than 3 years: **5 points** • 3 – 5 years**: 10 points** • More than 5 years**: 15 points**

3.1.2 Senior IT Security Incident Management Specialist Level II

Criteria	**Point-Rated Criteria**	**Max Points**	**Evaluation Criteria**
R. 1	The proposed resource should possess a minimum of (4 years cumulative experience in the last ten years performing incident Specialist related tasks). The tasks related to Senior IT Security Incident Management Specialist are listed in Annex A Section 4.2.	**15**	• 12 to 24 months**: 5 points** • >24 to 48 months: **10 points** • >48 months: **15 points**
R.2	The proposed resource should provide a minimum of 2 projects demonstrating in-depth experience with TCP/IP communications protocol and web service protocols (ex: HTTP, HTTPS, FTP, XML, SOAP)	**10**	• 2 projects: **5 points** • 3 or more projects: **10 points**
R.3	The proposed resource should provide a minimum of 2 projects which demonstrate experience with prevention measures against attack methods/techniques and malware (ex: Cross-site scripting, denial of service, spam, BotNets, worms).	**10**	• 2 projects: **5 points** • >3 or more projects: **10 points**
R.4	The proposed resource should have RECENT experience in the following areas.	**10**	**One point** per list item up to a **maximum of 10 points**

	• X.500 Directory Standards; • LDAP; • MS operating systems; • Unix operating systems; • Linux operating systems; • z/OS operating systems; • Networking Protocols (HTTP, FTP, Telnet); • Internet security protocols (SSL, S-HTTP, S-MIME, IPSec, SSH); • Wireless Security; • TCP/IP, UDP, DNS, SMTP; • Intrusion detection systems and firewalls; and • Approved GoC Cryptographic Algorithms. Evaluation will consider RECENT experience for each of the above in terms of work performed and months of experience gained since January 1, 2003.		

3.1.3 Senior IT Security Engineer Level II

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R.1	Demonstrate that the proposed resource has experience developing network security architectures based on IT Security Directive (ITSD) and/or IT Security Guidance (ITSG) at the Protected B level or higher. The tasks related to Senior IT Security Engineer are listed in Annex A Section 4.3.	**25**	• 12 to 18 months**: 5 points** • >18 to 24 months: **10 points** • >24 to 30 months: **15 points** • >30 to 36 months: **20 points** • >36 months: **25 points**
R.2	Demonstrate that the proposed resource has experience developing and documenting system requirement specifications for any one of the following IT Security Solutions: • Host-based Intrusion	**25**	• 12 to 24 months**: 5 points** • >24 to 36 months: **10 points** • >36 to 48 months: **15 points** • >48 to 60 months: **20 points** • >60 months: **25 points**

	Prevention System (HIPS) • Wireless Networking Security Technologies • Intrusion Detection Systems (IDS) • Network Intrusion Prevention System (IPS) • Security Information and Event Management (SIEM) • Full Packet Capture (FPC) • Network Access Control (NAC) • Identity Credentials and Access Management (ICAM) • Endpoint Protection.		

3.1.4 Senior IT Security Installation Specialist Level II

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R.1	The proposed resource should have experience detecting and analyzing malicious activity from hosts and network traffic and/or experience completing tasks related to the role of Senior IT Security Installation Specialist. The tasks related to Senior IT Security Installation Specialist are listed in Annex A Section 4.5.	**15**	• 12 to 18 months: 5 points • >18 to 24 months: 10 points • >24 months: 15 points

R.2	The proposed resource should have experience providing technical support for the following security technologies including: • Host-based security • IDS/IPS (Intrusion Prevention System) • Firewalls/UTMs • Proxies • Load Balancers Experience claimed must include at least three of the items listed above in order to be considered for evaluation purposes.	**15**	• 12 to 24 months**: 5 points** • >24 to 48 months: **10 points** • > 48 months: **15 points**
R.3	The proposed resource should have experience performing log analysis. Bidders must provide the following information: a. Duration of the proposed resource's experience; b. Description of the experience.	**25**	• 24 to 30 months: **5 points** • >30 to 36 months: **10 points** • >36 to 42 months: **15 points** • >32 to 48 months: **20 points** • >48 months: **25 points**
R.4	The proposed resource should have experience (since January 1, 2003) in the following areas. X.500 Directory Standards; • LDAP; • MS operating systems; • Unix operating systems; • Linux operating systems; • z/OS operating systems; • Networking Protocols (HTTP, FTP, Telnet); • Internet security protocols (SSL, S-HTTP, S-MIME, IPSec, SSH); • Wireless Security; • TCP/IP, UDP, DNS, SMTP; • Intrusion detection systems and firewalls; and • Approved GoC Cryptographic Algorithms.	**10**	One point per list item up to a maximum of 10 points

3.1.5 Senior Computer Forensic Specialist Level II

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R.1	The proposed resource should have experience with Forensics analysis of Windows, OS X, and Linux based Operating Systems.	**15**	• 12 to 18 months: 5 points • >18 to 24 months: 10 points • >24 months: 15 points
R.2	The proposed resource should have experience (since January 1, 2003) in drafting investigative reports.	**15**	• 12 to 24 months**: 5 points** • >24 to 48 months: **10 points** • > 48 months: **15 points**
R.3	The proposed resource should have experience (since January 1, 2003) in data extraction from devices commonly supported by Commercial Off-The-Shelf (COTS) recovery products.	**25**	• 24 to 30 months: **5 points** • >30 to 36 months: **10 points** • >36 to 42 months: **15 points** • >32 to 48 months: **20 points** • >48 months: **25 points**
R.4	The proposed resource should have experience (since January 1, 2003) in the following areas. X.500 Directory Standards; • LDAP; • MS operating systems; • Unix operating systems; • Linux operating systems; • z/OS operating systems; • Networking Protocols (HTTP, FTP, Telnet); • Internet security protocols (SSL, S-HTTP, S-MIME, IPSec, SSH); • Wireless Security; • TCP/IP, UDP, DNS, SMTP; • Intrusion detection systems and firewalls; and • Approved GoC Cryptographic Algorithms.	**10**	One point per list item up to a maximum of 10 points
R.5	Points will be awarded if the proposed	**15**	• 1 Certification : 5 points

	resource holds one or more additional professional certifications from the following list; • Certified Information Systems Security Professional (CISSP) • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) designation • SABSA Chartered Security Architect - Foundation Certificate (SCF) • SABSA Chartered Security Architect - Practitioner Certificates (SCP) • Information Technology Infrastructure Library (ITIL) certification. • Project Management Professional (PMP) from the Project Management Institute (PMI) A copy of the resource's valid Certification must be submitted with the Bidder's proposal.		• 2 Certifications : 10 points • 3 Certifications : 15 points

3.1.6 Senior IT Security Vulnerability Assessment (VA) Specialist Level II

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R.1	The proposed resource should have experience with Vulnerability analysis of Windows, OS X, and Linux based Operating Systems and completing tasks related to the role of Senior IT Security VA Specialist. The tasks related to Senior IT Security VA Specialist are listed in Annex A Section 4.6	**15**	• 12 to 18 months: 5 points • >18 to 24 months: 10 points • >24 months: 15 points
R.2	The proposed resource should have experience (since January 1, 2003) in drafting VA reports.	**15**	• 12 to 24 months**: 5 points** • >24 to 48 months: **10 points** • > 48 months: **15 points**

R.3	the proposed resource should have recent experience) in VA methods and software. Off-The-Shelf (COTS) recovery products.	**25**	• 24 to 30 months: **5 points** • >30 to 36 months: **10 points** • >36 to 42 months: **15 points** • >32 to 48 months: **20 points** • >48 months: **25 points**
R.4	The proposed resource should demonstrate experience (since January 1, 2003) in the following areas. X.500 Directory Standards; • LDAP; • MS operating systems; • Unix operating systems; • Linux operating systems; • z/OS operating systems; • Networking Protocols (HTTP, FTP, Telnet); • Internet security protocols (SSL, S-HTTP, S-MIME, IPSec, SSH); • Wireless Security; • TCP/IP, UDP, DNS, SMTP; • Intrusion detection systems and firewalls; and • Approved GoC Cryptographic Algorithms..	**10**	One point per list item up to a maximum of 10 points
R.5	Points will be awarded if the proposed resource holds one or more additional professional certifications from the following list; • Certified Information Systems Security Professional (CISSP) • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) designation • SABSA Chartered Security Architect - Foundation Certificate (SCF) • Information Technology Infrastructure Library (ITIL) certification • Certified in Risk and Information System Control (CRISC) with ISACA	**15**	• 1 Certification : 5 points • 2 Certifications : 10 points • 3 Certifications : 15 points

	A copy of the resource's valid Certification should be submitted with the Bidder's proposal to receive points		