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

**REQUEST FOR PROPSAL**

**AMENDMENT NO. 2**

This RFP amendment No. 2 is raised to;

1- Extend the RFP closing date by one week to September 24, 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:** 17 September 2014

**INSERT:** 24 September 2014

**2. At Part 3 of the RFP 'Bid Preparation Instructions', article 3.4 'Section III: Certifications' REVISE as follows:**

**DELETE:** this article in its entirety.

**3. At Part 4 of the RFP, 'Evaluation Procedures and Basis of Selection', article 4.1 'Evaluation Procedures' REVISE as follows:**

**DELETE:** sub-article 'd)' in its entirety.

**4. At Part 6 of the RFP 'Resulting Contract Clauses', article 6.2 'Task Solicitation and Task Authorization Procedures' REVISE as follows:**

**DELETE:** sub-article 6.2.8 'Pre-Cleared Resources' in its entirety.

**5. At Attachment 1 to Part 4 of the RFP, article 3 'Mandatory Criteria' at 'M1' REVISE as follows:**

**DELETE:** the 'Mandatory Requirement' Column for M1 and;

**INSERT** the following in its place:

The Bidder must have demonstrated contract experience in supplying all of the following resource categories, for the required Mandatory Billable Days per category.

| **Category of Personnel** | **Mandatory Minimum Number of Billable Days** |
|---|---|
| IT Security Vulnerability Assessment (VA) Specialist | **1600** |
| IT Security Engineer | **1000** |
| Computer Forensics Specialist | **1800** |

| | |
|---|---|
| IT Security Incident Management Specialist | **2000** |
| IT Security Methodology, Policy and Procedures Analyst | **600** |
| IT Security Installation Specialist | **600** |

Bidders must complete Appendix A and B to Part 4.

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 $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.

**6. At Appendix A to Attachment 1 to Part 4 of the RFP 'Evaluation Criteria', REVISE as follows:**

**DELETE:** the previous version in its entirety and;

**INSERT:** the new version which is attached hereto this RFP amendment.

**7. At Attachment 2 to Part 4 of the RFP 'Financial Evaluation of Proposal', REVISE as follows:**

**DELETE:** the previous version in its entirety and;

**INSERT:** the new version which is attached hereto this RFP amendment.

**8. At Annex A 'Statement of Work', REVISE as follows:**

**DELETE:** the previous version in its entirety and;

**INSERT:** the new version which is attached hereto this RFP amendment.

**9. 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. | Canada is presently reviewing and will make changes to the mandatory certifications required. These changes should be available early next week. |
| **#8**- Question re: 2.1.2 M2: The requested mandatory certifications (CISSP, CISM, or CISA) | See answer to Q #7. |

| | |
|---|---|
| are general IT security certifications that do not demonstrate detailed knowledge of incident management procedures or practices. The SANS Institute GIAC Certified Incident Handler (GCIH) and GIAC Certified Intrusion Analyst (GCIA) certifications are longstanding and recognized technical certifications for incident management specialists. Please confirm that SANS GCIH and GCIA will be accepted to comply with this mandatory requirement. | |
| **#9**- Question re: 2.1.3 M2: ACP is a technical certification for a specific product. IT Security Engineers have broad experience in the design and implementation of IT security solutions that are currently or may be deployed in the FIPC. If ArcSight-specific experience is required for a specific TA it is reasonable to expect ACP as a mandatory requirement, but it is unnecessarily restrictive for the complete range of IT security engineer activities that could be performed under this contract. Please consider removing ACP as a mandatory requirement this solicitation and instead include ACP as needed in individual task requests. | See answer to Q #7. |
| **#10**- Question re: 2.1.5 M2 and R5: The requested mandatory certifications (CISSP, CISM, or CISA) as well as the rated certifications are general IT security certifications that do not demonstrate detailed knowledge of computer forensics procedures or practices. The SANS Institute GIAC certifications: 1) Forensic Examiner (GCFE); 2) Forensic Analyst (GCFA); and 3) Reverse Engineering Malware (GREM) certifications are longstanding and recognized technical certifications for forensics specialists. Please confirm that SANS GCFE or GCFA or GREM certifications will be accepted to comply with both the mandatory and rated requirements. | See answer to Q #7. |
| **#11**- Question re: 2.1.6 M2 and R5: CISA is not a technical vulnerability assessment certification and does not demonstrate detailed knowledge of vulnerability assessment and penetration testing activities. The SANS Institute GIAC certifications: 1) Penetration Tester (GPEN); 2) Web Application Penetration Tester (GWAPT); 3) GIAC Certified Incident Handler (GCIH); and 4) Systems and Network Auditor (GSNA) are longstanding and recognized technical certifications for vulnerability assessment specialists. Please confirm that SANS GPEN or GWAPT or GCIH or GSNA certifications will be accepted to comply with both the mandatory and rated requirements. | See answer to Q #7. |
| **#12**- Appendix A to Annex A, Item 2.0 Mandatory Requirements: In order for the Crown to obtain the best qualified candidate for each Task Solicitation, we request that Certification (ie CISSP, CISA, | See answer to Q #7. |

| | |
|---|---|
| CISM, etc.) be removed from Mandatory Requirements and added to Rated Requirements. We also request that the Crown consider equivalent experience in lieu of formal certification to ensure that excellent candidates who have vast experience in these specific areas can be considered for the positions. | |
| **#13**- Question regarding the role of small businesses in SSC professional services contracts.<br><br>13-18653/A is a large, multi-year, multi-resource RFP that has 6 IT security roles and 72 resources within the TBIPS contracting vehicle (non-ASA). The corporate mandatory requirements for this contract are clearly tailored to very large organizations and intended to exclude small and medium-size firms from bidding. Furthermore, the requirements are specifically written to prevent small and medium-size suppliers from partnering in a Joint Venture (JV) with two or more firms. This intent is revealed through the use of a single mandatory corporate requirement that bundles together:<br>○ $5 million in contract experience<br>○ 6 resource categories<br>○ 7600 billable days (over 33 billable years) of experience<br><br>This clever combination prevents small and medium-size organizations interested in forming a JV from pooling contracts, resources, or billable days and effectively eliminates such suppliers from bidding.<br><br>The RFP clearly states (corporate rated requirement R2) that: "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."<br><br>The decision to combine corporate requirements as described above will funnel all opportunities through one (and up to four - but we believe that there will not be four compliant bids) large firms. These large firms do not currently enjoy a monopoly on the pool of experienced IT security consultants in the NCR and therefore SSC's approach actually limits its access to qualified personnel.<br><br>We are very concerned that this RFP is limited only to very large organizations. Notwithstanding that | a) SSC continues to tender and award Tier 1 and 2 contract vehicles for the purposes of achieving its mandate.<br><br>b) Only current, formalized TBIPS Tier 2 joint venture entities are permitted to bid, SSC will not recognize corporate mandatory and rated requirement experience claimed through other types of partnerships. |

| | |
|---|---|
| SSC's mandate is efficiency and cost savings and that its approach to date has been to consolidate business to very large companies, the active exclusion of small and mid-size businesses from SSC contracts will do irreparable damage to these organizations and their staff. The extreme result of this disadvantage could put specialized firms in this space out of business by denying them access to GOC contract mechanisms for which they have previously been able to compete through a variety of vehicles.<br><br>The RFP states "SSC may choose to use this Contract for some or all of its clients and may use alternative means to provide the same or similar services" but there is no indication or commitment of those alternative means.<br><br>In consideration of these points, please:<br><br>a) describe SSC's plans and timeframes regarding the establishment of contract vehicles that will be accessible to small and mid-size businesses; and<br>b) indicate whether the corporate mandatory and rated requirements can be split in a manner that will permit small and mid-size businesses to partner in Joint Venture for this specific contract | |
| **#14**- Question regarding the role of Aboriginal businesses in SSC professional services contracts.<br><br>In response to the historical disadvantages faced by Aboriginal Canadians, Public Works and Government Services (PWGSC) on behalf of the Government of Canada has established programs to support Aboriginal businesses and Aboriginal peoples in their dealings with the government. These programs include Aboriginal set-aside (ASA) procurement strategies which enable Aboriginal businesses to develop and grow within a competitive environment.<br><br>Most, if not all large professional services standing offers and supply arrangements managed by PWGSC over the past 10 years have included or currently include an ASA component. Relevant examples include ITISPS, CPSA, SBIPS, and TBIPS. Large hardware and software supply arrangements such as NESS and SLSA also | a) SSC continues to adhere to Treasury Board contracting policy regarding Aboriginal Business and endeavors to establish ASA contracts whenever it is feasible.<br><br>b) There will be no ASA component for this specific requirement. |

| | |
|---|---|
| include ASA components.<br><br>13-18653/A is a large, multi-year, multi-resource RFP that has 6 IT security roles and 72 resources within the TBIPS contracting vehicle (non-ASA). The RFP documents state this contract is to be used "by SSC to provide shared services to its clients, which include SSC itself, those government institutions for whom SSC's services are mandatory at any point during the Contract period, and those other organizations for whom SSC's services are optional at any point in the Contract period and that choose to use those services from time to time." It is evident that SSC's intent is to leverage this contract in the manner of a supply arrangement by using it to satisfy a significant number of requirements. In effect, Aboriginal businesses unable to qualify for the non-ASA contract will be denied the ability to provide IT security services directly to the largest consumer of such services in the government.<br><br>We are very concerned that there is no ASA component within this RFP. Notwithstanding that SSC's mandate is efficiency and cost savings and that its approach to date has been to consolidate business to very large companies, failure to create/include an Aboriginal procurement strategy within SSC not only goes against GoC position on ASA but will also do irreparable damage to Aboriginal IT security businesses and resources in our nation's capital. The extreme result of this disadvantage could put Aboriginal firms in this space out of business by denying them access to GOC contract mechanisms for which they have previously been able to compete through an ASA.<br><br>The RFP states "SSC may choose to use this Contract for some or all of its clients and may use alternative means to provide the same or similar services" but there is no indication or commitment of those alternative means.<br><br>In consideration of these points, please:<br><br>a) describe SSC's plans and timeframes regarding the establishment of ASA contracts; and<br>b) indicate whether there will be an ASA component for this specific contract | |
| **#15-** Is there now, or has there ever been, a consultant or consultants delivering to services | Bell SCNet PS contract expires Dec 31, 2014. $2,980,000.00 approx. for one year. |

| | |
|---|---|
| similar or identical to those solicited herein? If so, who is the contracting firm and what was or is the value of the contract? | |
| **#16-** We have reviewed this RFP and determined that since this TBIPS has extensive corporate requirements, we (and many others) are unable to bid. We continue to be perplexed as to why Industry members that went to great lengths to qualify for this TBIPS vehicle at Tier 2 are precluded from bidding wherein additional corporate mandatory requirements are imposed by the Crown. Additionally, we have made efforts to team (prime/sub) with other Industry members only to find that several other firms are equally unable to meet these unnecessary additional mandatory corporate requirements. These requirements serve only to limit competition, protect the incumbent contractors, and dramatically increase the overall cost of the contract to the Crown.<br><br>a) Could the Crown kindly consider removing corporate requirements?<br><br>b) Optionally, in the best interests of a fiscally responsible procurement process, could the Crown consider cancelling this TBIPS and simply solicit this RFP as its own contract thereby allowing firms to create a joint venture. Joint Venture bids are not permitted under the TBIPS vehicle unless they were the means to qualify for the Tier initially. We, and many others, did not require a JV to qualify for Tier 2, yet, as indicated, cannot meet the requirements. | a) The Crown reserves its right to include additional corporate requirements in order to satisfy the best interest of the Crown.<br><br>b) SSC will not withdraw this TBIPS RFP solicitation. |
| **#17**- Given that SSC has released at least three Bid Solicitations that are all due at the same time, this has placed an excessive burden on firms that are qualified and wish to submit bids for more than one of the solicitations. Given that most Firms must often submit many bids with the hopes of winning one. Given this, we respectfully request a 10 calendar day extension to the current closing date. | The closing date has been extended to September 24, 2014 at 2:00pm Eastern Standard Time (EST). |
| **#18-** Page 4 of 83 clause 1.2 Summary. Please confirm that the signed non-disclosure agreement is only required after contract award. | Confirmed. |

| | |
|---|---|
| **#19**- Page 12 of 83 clause 4.1 Evaluation Procedures item d): "for the resource proposed, the Bidder must include an up to date resume" – Please confirm this will only be required at time of Task Authorization | Regarding Part4, Paragraph 4.1, Item d), this item refers to the Task Solicitation process after contract award, as so therefore is to be removed. |
| Page 13 of 74, Clause 4.3 (b) Method 1, item (i) states the calculation formula for the lower median rate to a value of minus 10% and on Page 15 of 74 Step 1 (Median 1) states "numbers are based on a -15%". Can the Crown please confirm which percentage will be used for evaluation. | The percentages described on page 13 are correct. Page 15 is merely a sample of the financial evaluation model. |
| **#20-** Page 20 of 83, clause 5.1 Mandatory at Contract Award – Security Requirements: Please confirm Personnel Security Clearance is only required at time of Task Authorization | Personnel Security Clearance is required from Contractors at the time of Task Solicitation. |
| **#21-** Page 28 of 83, 6.2.8 Pre-Cleared resources Item i. states: ensure that the specific individuals named in Annex E of this contract..... Please confirm that Annex E is either missing or not required and that names of resources will only be required at time of Task Authorization. | Annex E is not required for this RFP and will be deleted via RFP amendment. |
| **#22-** In Mandatory 1, Page 72 of 83, it states "Bidders must complete Appendix A,B and C to Part 4" Would SSC please clarify what constitutes Appendix C or delete this reference. | Appendix C does not exist and this reference has been deleted. |
| **#23-** Page 41, 4.0, Tasks, Would SSC please number the bullets for ease of reference for all bidders. | This has been provided in this RFP amendment. |
| **#24-** 4.0 Tasks, please confirm that a task is represented by the sub-bullets listed (as indicated with the outlined bullets, not the black solid bullets). | Confirmed. |
| **#25-** Page 78 of 83 Attachment 2 to Part 4, Financial Evaluation, second paragraph; Please confirm that the sentence "bidders must propose the same per diem rate for both resources" is an error and should be removed. | Confirmed. |
| **#22-** Appendix A to Attachment 1 Part 4: Please confirm "billing period (24 months)" should be replaced by 60 months. | Confirmed. |
| Rated R2, Page 66 of 74 Please confirm that paragraph 2 "vendors should demonstrate their ability to supply a single client contract reference...." implies that any Professional Services engagement (ie: non Cyber & IT Security) meet the reference criteria | Confirmed. |
| **#23-** As a result of the many procurements in | The closing date has been extended to September |

| | |
|---|---|
| progress for Professional Services and other IT programs which require many man hours for bid response from the same pool of subject matter experts we kindly request a one month extension to October 17, 2014. We also request that the question period be extended to October 3rd, 2014. | 24, 2014 at 2:00pm Eastern Standard Time (EST). |
| On the following pages, the resources categories are listed as "Senior" (Level 3) when the overall RFP requires Level 2 (Intermediate) resources: Annex A SOW pp 40-43, Appendix A to Annex A pp 46-56, Annex B Basis of payment p 57, Attachment 2 to Part 4 p 69. Please clarify the level of the resource categories. | This RFP is for Level 2 resources only. |
| **#24-** The noted solicitation 13-18653/A indicates that up to four (4) contracts may be awarded for this solicitation. Based on this, are bidders allowed to submit a bid for less than the number of requested 'Category of Personnel' stipulated within the solicitation? | No. |
| **#25-** Can the Crown please confirm that only one (1) qualifying resource is required to be submitted for each 'Category of Personnel' being bid for proposal evaluation purposes. | Through references projects, Bidders are required to demonstrate a minimum number of billable days, and address at least 70% of the tasks listed for each Category of Personnel. Bidders may use the experience of any number of project resources, provided that their project tasks meet the criteria. However, only after contract award, during a Task Solicitation, will specific resources be evaluated against a prepared resource grid. |
| **#26-** Will the Crown consider allowing firms to still demonstrate all the relevant services that they delivered via 5 contracts within the five years however allow the totals to be rated rather than a mandatory minimum? | The mandatory billable days and rated billable days remained unchanged. |
| **#27-** It is clear that the Crown is using corporate Mandatory (M1) as method to qualify security organizations that have undoubtedly demonstrated experience and expertise in recently providing long term security resources to Canadian organizations. The constriction of:<br>• The exact categories<br>• For the exact number of Billable days (7,600 in total or 34.55 years of experience)<br>• In a maximum of five contracts<br>• In contracts only within the past five years<br>• In contracts with a minimum billed | The professional services requirements that this vehicle intends to satisfy are task-based in nature. It is common for SSC, with Tier 2 procurements, to measure bidders' billable days experience in relevant personnel categories with their associated descriptions. Client project references are not limited to the Government of Canada. |

| | |
|---|---|
| value of $1M<br><br>Requesting 34.55 years of experience in exact categories in a 5 year window for a one year plus two option year(s) contract is impractical and will restrict the number of quality bids SSC will receive, and may be viewed as favoring the incumbent organization(s)<br><br>The SSC managed network for the Government of Canada is the largest consumer of Security consultants and services in the country. Therefore requiring over 34 years of experience as a minimum to qualify seriously restricts the number of highly qualified and mature security practices that will be able to bid.<br><br>It is not typical of security contracts in Canada to be as long term or as large of a dollar value that Canada is asking for in this requirement; It is typical for large Security organization to have a thriving practice spread over numerous smaller contracts in an effort to harden the network(s) they protect.<br><br>Due to the structure of the contract the Crown appears to striving toward; multiple qualified organizations (max 4) to compete on an as and when required basis. Therefore in an effort to protect the integrity of the procurement process and provide SSC with the maximum number of qualified Security bidders who have demonstrated a mature security practice more than capable of providing the SSC with qualified resources we request that the Crown revise Mandatory 1 to:<br><br>*The Bidder should demonstrate that it has sufficient recent experience providing IT Security consulting services. To demonstrate this experience, the Bidder is required to have invoiced for at least $5,000,000 of IT Security consulting services. Only work invoiced for since September 17, 2009 will be accepted.*<br><br>*The following information must be provided to substantiate the business volume claimed:*<br><br>*- Contract number(s)*<br><br>*- Client name and contact information for verification purposes*<br><br>*- Start and end date of contract(s), including option periods*<br><br>*- Contract value*<br><br>*- Amount billed for each contract referenced*<br><br>*- Description of the services performed* | |

| | |
|---|---|
| *IT Security consulting services are defined as equivalent to any of the common activities for the resource categories offered under TBIPS categories as listed within the Supply Arrangement.*<br><br>*The Bidder must have provided the services to Outside Clients. "Outside Clients" are defined as any legal entities that are not a parent, subsidiary or affiliate of the Bidder. This is applicable to all members of any Joint Venture submitting a bid.* | |
| **#28-** R1 as a continuation of M1 would require an additional 34.55 years (or 7600 days) of experience to obtain the maximum 100 points; a total of 15,200 days or 69.1 years when combining M1 with R1.<br>Given the landscape of security in Canada, this ask does not seem realistic or line up with SSC's desire to award up to four contracts for as & when required security services. As outlined in our question above (for M1) R1 as it is written today would restrict the number of qualified bids SSC will receive and we request that R2 be modified to the following:<br><br>*The Bidder should demonstrate that it has sufficient recent experience providing IT Security consulting services. To demonstrate this experience, the Bidder is required to list billed revenue of IT Security consulting service of up to $10Million above and beyond M1 for full points. Only work invoiced for since September 17, 2009 will be accepted.*<br><br>*The following information must be provided to substantiate the business volume claimed:*<br><br>*- Contract number(s)*<br><br>*- Client name and contact information for verification purposes*<br><br>*- Start and end date of contract(s), including option periods*<br><br>*- Contract value*<br><br>*- Amount billed for each contract referenced*<br><br>*- Description of the services performed*<br><br>*IT Security consulting services are defined as equivalent to any of the common activities for the resource categories offered under TBIPS* | Please see answer to Q#27 |

| | |
|---|---|
| *categories as listed within the Supply Arrangement.*<br><br>*The Bidder must have provided the services to Outside Clients. "Outside Clients" are defined as any legal entities that are not a parent, subsidiary or affiliate of the Bidder. This is applicable to all members of any Joint Venture submitting a bid.*<br><br>• $5M to $6M = 20 points<br>• >$6M to $7M = 40 points<br>• >$7M to $8M = 60 points<br>• >$8M to $9M = 80 points<br>• >$9M to $10M = 100 points | |
| **#29-** As stated in R2; SSC's belief that the most significant risk associated with this contract is a contractor's ability to provide the number of qualified resources is a valid one. However validating a potential contractors ability to provide a high volume of resources solely on a single contract within the NCR in the last 12-24 months is not realistic. SSC's existing contracts are likely the only agreements that would amount to full points and therefore restricts the number of bid SSC will receive.<br><br>It is clear that SSC is looking for organizations to demonstrate the bench strength of the resources and as such we request that R2 be modified to the following:<br><br>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.<br><br>Vendors should demonstrate their ability to supply, manage and retain large groups of resources in support of client project(s) within the region of delivery.<br><br>Bidders should supply a list of client contract(s) with a contact reference within the past 12 to 24 months encompassing a minimum of 10 resources | Given the task distribution process, and potential volume of Task Authorizations through any one contract awarded through this solicitation, it is critical that successful bidders have a record of high volume delivery to a client within the NCR. The reference client is not limited to the Government of Canada. No change to R2 will be considered. |

| | |
|---|---|
| in the NCR in support of client projects.<br>To be considered, a single resource may only be used/counted once.<br>Reference project information must include:<br>• **Client Organization Name**<br>• **Client Contact name and Title**<br>• **Client Contact Phone #**<br>• **Client Contact Email Address**<br>• **Project start and end dates (yy/mo)**<br>• **Total number of individual PS resources provided the last 12-24 months**<br>• **10 points**- 10 individual resources provided to client(s) in the NCR within the last 12-24 months;<br>• **25 points**- 15 individual resources provided to client(s) in the NCR within the last 12-24 months;<br>• **35 points**- 25 individual resources provided to client(s) in the NCR within the last 12-24 months;<br>• **50 points**- 30 individual resources provided to client(s) in the NCR within the last 12-24 months | |
| **#30-** Please provide Appendix C to part 4 of the RFP as it is missing from the RFP package and necessary to evaluate, prepare and submit a bid for this solicitation. As a result of the missing information and to protect the integrity of the bid process and ensuring the maximum number of bids for SSC to evaluate, we request that an extension to October 2nd, 2014 be granted | Appendix C is not required to bid on this RFP and has been removed. This is not grounds for an extension. |

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 |

# ANNEX A

# STATEMENT OF WORK

## 1.0 Objective

The objective of this contract is to assist in the daily IT security operations and functions of the Shared Services Canada (SSC) Federal Information Protection Centre (FIPC).

## 2.0 Background

Shared Services Canada (SSC) was formed in 2011 with the mandate to consolidate and streamline the delivery of IT infrastructure services specifically email, data centre and telecommunications services to 43 federal departments and most of the Government of Canada IT assets.

In order to assist with the SSC mandate, the IT Security Services Section provides advice and guidance related to IT security and risk management with an emphasis on IT security methodologies, policies and security.

## 3.0 Requirement

This professional services contract is for the provision of six different labour categories:

1. Senior IT Security Methodology, Policy and Procedures Analyst
    - 1 resource (Secret security clearance) for a total of 270 days per year
2. Senior IT Security Incident Management Specialist
    - 7 resources;
        - 2 resources (Top Secret security clearance) for 230 days per year
        - 2 resources (Secret security clearance) for 230 days per year
        - 1 resource (Top Secret security clearance) for 100 days per year
        - 2 resources (Secret security clearance) for 100 days per year
3. Senior IT Security Engineer
    - 2 resources (Secret security clearance) for 230 days per year
4. Senior Computer Forensics Specialist
    - 3 resources;
        - 1 resource (Top Secret security clearance) for 230 days per year
        - 2 resources (Top Secret security clearance) for 100 days per year
5. Senior IT Security Installation Specialist
    - 2 resources (Secret security clearance) for 230 days per year
6. IT Security Vulnerability Assessment (VA) Specialist
    - 3 resources;
        - 1 resource (Secret security clearance) for 230 days per year
        - 2 resources (Secret security clearance) for 100 days per year

## 4.0 Tasks

### 4.1 Senior IT Security Methodology, Policy and Procedures Analyst

The tasks of the IT Security Methodology, Policy and Procedures Analyst will include but will not limited to:

1) Prepare work plans and schedules of work;
2) Review/analyze and ensure conformity with:
    a. Federal, Provincial and Territorial Government IT Security methodologies, programs, policies, and/or procedures;
    b. Federal, Provincial or Territorial Government IT Security standards and/or guidelines; and
    c. IT Security Risk Management methodologies.
3) Develop IT Security standards, procedures and guidelines pursuant to the requirements of:
    a. The National Service Provider (NSP), Policy on Government Security (PGS) and supporting operational standards (i.e. management of Information Technology Security (MITS));`
    b. Departmental/Agency Security policy; and
    c. Other relevant standards, procedures and guidelines.
4) Develop IT Security processes/procedures in in support of Security Operations:
    a. IT Security and assurance;
    b. Security Assessment and Authorization (SA&A);
    c. Information Infrastructure Protection;
    d. Product evaluation;
    e. Privacy;
    f. Business Continuity Plan (BCP);
    g. Continuity Planning and Disaster Recovery Planning (DRP);
5) Develop and provide awareness training material relevant to IT Security Operations (when required); and
6) Review policy guidelines in the context of Security Operations.

### 4.2 Senior IT Security Incident Management Specialist

The tasks of the Senior IT Security Incident Management Specialist will include but are not limited to:

1) Prepare work plans and schedules of work;
2) Respond to security/cyber related incidents/attacks;
3) Write/modify SIM correlation rules;
4) Tune IDS/IPS systems;
5) Create/modify IDS/IPS signatures;
6) Analyze of events in depth and provide recommendations;
7) Assess vulnerabilities and provide recommendations;
8) Produce reports, analysis and recommendations related to threats;
9) Collect, collate, analyze and disseminate public information related to networked computer threats and vulnerabilities, security incidents and incident response;
10) Configure intrusion detection systems, firewalls and content checkers;
11) Extract and analyze reports and logs;
12) Configure/update virus scanners;
13) Provide support to multiple partners, clients;

14) Create tickets and monitor the ticketing systems and respond to Incident Requests (IR's);
15) Scrip to automate tasks;
16) Prepare and/or deliver IT Security threat, vulnerability and/or risk briefings;
17) Work with other GC resources in the performance of their work as required;
18) Perform tasks directly supporting the departmental IT Security and Cyber Protection Program;
19) Maintain and recommending enhancements to the security posture; and
20) Make technical and procedural recommendations and enhancements in coordination with the other members of the FIPC.

4.3 Senior IT Security Engineer

The tasks of the Senior IT Security Engineer will include but are not limited to:

1) the review/analysis and evaluation of:
    - Directory standards such as X.400, X.500, and SMTP;
    - Operating systems such as MS, Unix, Linux, and Novell;
    - Networking protocols such as HTTP, FTP, and Telnet;
    - IT security architecture fundamentals, standards, communications and security protocols such as IPSec, IPv6, SSL, and SSH;
    - IT security protocols at all layers of the Open Systems Interconnection (OSI) and TCP/IP stacks;
    - Domain Name Services (DNS) and Network Time Protocols (NTP);
    - Network routers, multiplexers and switches;
    - Application, host and/or network hardening and security best practices such as shell scripting, service identification, and access control;
    - Wireless technology;
    - Cryptographic Algorithms;
    - Technical threats to, and vulnerabilities of, networks;
    - IT security configuration management;
    - IT security tools and methodologies;
    - Security data and provision of advisories and reports;
    - IT Security statistical analysis;

4.4 Senior Computer Forensics Specialist

The tasks of the Senior Computer Forensics Specialist will include but are not limited to:

1) Prepare work plans and schedules of work;
2) Respond to security related incidents;
3) Write/modify SIM correlation rules;
4) Perform investigations as directed by appropriate authorities;
5) Produce reports, analysis and recommendations related to investigations;
6) Extract and analyze reports and logs;
7) Provide support to multiple partners, clients;
8) Create tickets and respond to Incident Requests (IR's);
9) Prepare and/or deliver computer forensic related briefings;
10) Work with other GC resources in the performance of their work as required;
11) Perform tasks directly supporting the departmental IT Security and Cyber Protection Program;
12) Maintain and recommend enhancements to the security posture; and

13) Make technical and procedural recommendations and enhancements in coordination with the other members of the FIPC.

4.5 Senior IT Security Installation Specialist

The tasks of the Senior Computer Forensics Specialist will include but are not limited to:

1) The identification and analysis of threats to, and vulnerabilities of, IT systems and IT security safeguards;
2) System installation, configuration, integration, policy fine-tuning, operation, performance monitoring and fault detection for:
    a. Host and network intrusion detection and prevention systems;
    b. Network and computer forensics systems;
    c. Firewalls, VPNs and network devices;
    d. Enterprise network vulnerability tools;
    e. Malicious code, anti-spam and content management tools;
    f. File integrity tools;
    g. Remote management utilities;
    h. Enterprise Security Management (ESM)/Security Information Management (SIM) systems;
    i. Data preservation and archiving utilities;
    j. Threat agents analysis tools and other emerging technologies including privacy enhancement, predictive analysis, VoIP, data visualization and fusion, wireless security devices, PBX, and telephony firewall;
3) Installation of operating systems such as MS, Unix, Linux, and Novell;
4) Installation of intrusion detection systems, firewalls, and content checkers;
5) Installation and integration of supporting access control technology, such as CCTV, card access readers, electronic access control systems;
6) Tasks directly supporting the departmental IT Security and Cyber Protection Program; and;
7) Development and delivery of training material relevant to the resource category.
8) Working with other GC resources in the performance of their work as required;
9) Maintaining and recommending enhancements to the security posture; and
10) Making technical and procedural recommendations and enhancements in coordination with the other members of the FIPC.
11) Making technical and procedural recommendations and enhancements in coordination with the other members of the FIPC.

4.6 IT Security Vulnerability Assessment (VA) Specialist

The tasks of the IT Security Vulnerability Assessment (VA) Specialist will include but are not limited to:

1) The preparation of work plans and schedules of work;
2) Perform vulnerability assessments of SSC infrastructure;
3) Produce reports, analysis and recommendations related to VA's;
4) Perform onsite reviews and analysis of system security logs;
5) Collect, collate, analyze and disseminate public information related to networked computer threats and vulnerabilities, security incidents and incident response;
6) Prepare and/or deliver IT Security threat, vulnerability and/or risk briefings;
7) Perform tasks directly supporting the departmental IT Security and Cyber Protection Program;

8) Develop and/or refine existing processes/procedures for the execution of VA's; and

9) Participate in the evolution of VA's within SSC.

## 5.0 Deliverables

The Contractor must ensure that all resources maintain and provide the following deliverables as required:

- Weekly status reports;
- When requested, provide input into the development of business requirements;
- IT Security related briefing material;
- Requirements and option analysis documentation;
- Ad-hoc briefings to management including any reports;
- Reports on advice requested/provided; and
- Provide necessary documentation ensuring full audit ability.

## 6.0 Constraints

The Contractor must:

- follow all relevant policies and standards of the Government of Canada including:
  - Policy on Government Security (PGS) http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16578
  - Management of Information Technology Security Standard (MITS) http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text
  - CSE IT Security Guidance (ITSG33) http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng.html
- follow departmental guidance on the handling and classification of information use the provided secure IT equipment and media; and
- not use non-Government-approved IT equipment and/o r media, including mobile devices such as cell-phones
- obtain from its employee(s) or subcontractor(s) the completed and signed non-disclosure agreement, and provide it to the Technical Authority before they begin work under the Contract.

## 7.0 Departmental Support

The Contactors will be provided by the SSC FIPC Manager:

- Access to a safe workplace;
- Access and contact information to the SSC FIPC Manager and alternate contacts;
- All necessary IT tools and equipment to conduct of the work;
- Full access to relevant required resources and documentation;
- The SSC FIPC Incident Handling procedures; and
- The Departmental guidance on the handling and classification of information.

## 8.0 Location of Work

The resource will work in the National Capital Region (presently Place du Portage Phase III, Gatineau, Quebec).

## 9.0 Language

Most of the work will be conducted in English. French may be required for some duties.

## APPENDIX A TO ATTACHMENT 1 TO PART 4

## RFP BILLABLE DAYS RESPONSE TABLE

Bidder's Name:_____

Billing Period (60 consecutive months) between ___/___/___ to ___/___/___
(dd/mm/yy) (dd/mm/yy)

By providing a response, the bidder certifies that billable days provided occurred during the billing period indicated above for all of the resource categories listed.

| RESOURCE CATEGORY | NUMBER OF BILLABLE DAYS | | | | | |
|---|---|---|---|---|---|---|
| | Cross Reference to Contract Reference # _____ | Cross Reference to Contract Reference # _____ | Cross Reference to Contract Reference # _____ | Cross Reference to Contract Reference # _____ | Cross Reference to Contract Reference # _____ | Total |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**ATTACHMENT 2 TO PART 4**

**FINANCIAL EVALUATION OF PROPOSAL**

**(PRICING TABLE)**

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

As a minimum, the Bidder must respond to this pricing schedule by inserting in its financial bid for each of the periods specified below its quoted firm all inclusive per diem rate (in CAD $) for each of the resource categories identified.

| **FOR THE INITIAL CONTRACT PERIOD (1 YEAR)** | |
|---|---|
| **Category of Personnel** | **Bidders Proposed Per Diem Rate** |
| IT Security Vulnerability Assessment (VA) Specialist – Level 2 | |
| IT Security Engineer– Level 2 | |
| Computer Forensics Specialist– Level 2 | |
| IT Security Incident Management Specialist– Level 2 | |
| IT Security Methodology, Policy and Procedures Analyst– Level 2 | |
| IT Security Installation Specialist– Level 2 | |

| **FOR THE OPTION YEAR 1 (1 YEAR)** | |
|---|---|
| **Category of Personnel** | **Bidders Proposed Per Diem Rate** |
| IT Security Vulnerability Assessment (VA) Specialist – Level 2 | |
| IT Security Engineer– Level 2 | |
| Computer Forensics Specialist– Level 2 | |
| IT Security Incident Management Specialist– Level 2 | |
| IT Security Methodology, Policy and Procedures Analyst– Level 2 | |
| IT Security Installation Specialist– Level 2 | |

| FOR THE OPTION YEAR 2 (1 YEAR) | |
|---|---|
| **Category of Personnel** | **Bidders Proposed Per Diem Rate** |
| IT Security Vulnerability Assessment (VA) Specialist – Level 2 | |
| IT Security Engineer– Level 2 | |
| Computer Forensics Specialist– Level 2 | |
| IT Security Incident Management Specialist– Level 2 | |
| IT Security Methodology, Policy and Procedures Analyst– Level 2 | |
| IT Security Installation Specialist– Level 2 | |

**Taxes**

(a) All prices and amounts of money in the contract are exclusive of Harmonized Sales Tax (HST), unless otherwise indicated. The HST is extra to the price herein and will be paid by Canada.