Various Level 3 Resources For Cyber and IT Security

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**
Business Analyst	**1600**
IT Strategic Security Planning and Protection Specialist	**1000**
IT TRA & C&A Specialist	**1800**
IT Security Design Specialist	**2000**

IT Security VA Specialist	**600**
IT Privacy 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
#8- With respect to Appendix B to Part 4, which requires specific Customer Reference Contact Information. Due to the nature of security related work, our contracts and terms of engagement require confidentiality, and we are not allowed to divulge Client names. As has been done on other SSC solicitations, will SSC agree to let Bidders insert "Confidential" in cases where the Customer organization and contact information must be kept Confidential, with the agreement that the Bidder MUST provide the Organizations Name and other Contact information directly to SSC within 24 hours of request?	SSC agrees to let Bidders insert "Confidential" in cases where the Customer organization and contact information must be kept Confidential, with the agreement that the Bidder MUST provide the Organizations Name and other Contact information directly to SSC within 24 hours of request.

#9- Question regarding the role of small businesses in SSC professional services contracts. 13-18801-0/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: ○ $5 million in contract experience ○ 6 resource categories ○ 7600 billable days (over 33 billable years) of experience 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. 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." 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. We are very concerned that this RFP is limited only to very large organizations. 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, 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	a) SSC continues to tender and award Tier 1 and 2 contract vehicles for the purposes of achieving its mandate. 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.

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. 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. In consideration of these points, please: a) describe SSC's plans and timeframes regarding the establishment of contract vehicles that will be accessible to small and mid-size businesses; and 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	
#10- Question regarding the role of Aboriginal businesses in SSC professional services contracts. 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. 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 include ASA components. 13-18801-0/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	a) SSC continues to adhere to Treasury Board contracting policy regarding Aboriginal Business and endeavors to establish ASA contracts whenever it is feasible. b) There will be no ASA component for this specific requirement.

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. 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. 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. In consideration of these points, please: a) describe SSC's plans and timeframes regarding the establishment of ASA contracts; and b) indicate whether there will be an ASA component for this specific contract	
#11- Is there now, or has there ever been, a consultant or consultants delivering to services similar or identical to those solicited herein? If so, who is the contracting firm and what was or is the value of the contract?	Over the past 12 months CITS has utilized a number of TBIPS vehicles in order to secure similar resources under individual task authorizations, namely vehicles CTO-EA, ETS (Engineering and Technical Services) and BATS(Business and Technology Professional Services) For CTO-EA vehicle incumbent companies include

	Ibiska Telecom Inc., CGI and Maplesoft. Each vendor has at times provided various resources for initial contracts durations of 6 months with possible optional extensions. The incumbent companies include CGI for the ETS vehicle ending October 31 2014. For BATS vehicle incumbent companies include Eagle, TEK Systems and Maplesoft. Each vendor has at times provided various resources for initial contracts durations of 6 months with possible optional extensions.
#12- 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. a) Could the Crown kindly consider removing corporate requirements? 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. b) SSC will not withdraw this TBIPS RFP solicitation.
#13- With respect to Mandatory Requirement to show that the work delivered by the Category of Personnel must include at least 70% of the associated tasks listed in the Statement of Work,	In order to substantiate each Category of Personnel, bidders must demonstrate that reference projects have addressed at least 70% of the task related bullets. Where a bullet has a list of

can SSC please confirm that 70% refers to the bulleted tasks, and does not include the lettered qualifiers (e.g. the items listed as a), b), etc. that follow some bulleted tasks?	sub-tasks ie. a - g, a reference project must have addressed at least 70% of the sub-tasks in order to receive credit for the bullet.
#14- 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).
#15- Page 4 of 83 clause 1.2 Summary. Please confirm that the signed non-disclosure agreement is only required after contract award.	Confirmed.
#16- 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.
17- 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.
#18- 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.
#19- 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.
#20- Rated R2, Page 75 of 83 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.
#21- 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.
#23- As a result of the many procurements in 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.	The closing date has been extended to September 24, 2014 at 2:00pm Eastern Standard Time (EST).
#24- The noted solicitation 13-18801/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- Can the Crown advise how many contracts have been awarded for PIA services that would represent a level of effort greater than 120 days (600 / 5).	The values derived for M1, R1, and Total Estimated # of Resources Required (per year) are based on current business models and forecast based on SSC/CITS mandate and priorities.
#28- Will the Crown allow for the rated level of effort to go back as far as 8 years?	No.
#29- Finally, as the answers to these questions will allow us to provide a proposal response or not, will the Crown please allow an extension of three (3) weeks from the date these answers are published.	The closing date has been extended to September 24, 2014 at 2:00pm Eastern Standard Time (EST).
#30- Due to the fact that the Cover page containing critical information for preparing and submitting a bid was provided 15 days after the release of the RFP and the fact that Appendix C to part 4 is not contained within the RFP package; again a mandatory document necessary to evaluate, prepare and submit a bid we request the crown	The closing date has been extended to September 24, 2014 at 2:00pm Eastern Standard Time (EST).

extend the due date of the RFP the same 15 days to October 2nd, 2014 @ 2pm.	
#31- 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: • The exact categories • For the exact number of Billable days (7,600 in total or 34.55 years of experience) • In a maximum of five contracts • In contracts only within the past five years • In contracts with a minimum billed value of $1M 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) 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. 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. 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: ***The Bidder should demonstrate that it has***	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. Assuming 5 years' service of 220 billable days per year, SSC will award full points to bidders that demonstrate the equivalent of 3 Business Analysts (3200 days), 2 IT Strategic Security Planning and Protection Specialists (2000 days), 3.5 IT TRA and C&A Specialists (3600 days), 4 IT Security Design Specialists (4000 days), 1.1 IT Security VA Specialists (1200 days), and 1.1 IT Privacy Specialists (1200 days). Client project references are not limited to the Government of Canada. As per Amendment 1, the CPSA may be used as one contract to substantiate M1 and R1. No other changes will be considered.

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. ***The following information must be provided to substantiate the business volume claimed:*** ***- Contract number(s)*** ***- Client name and contact information for verification purposes*** ***- Start and end date of contract(s), including option periods*** ***- Contract value*** ***- Amount billed for each contract referenced*** ***- 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.*** ***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.***	
#32- 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. 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: ***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***	Please see answer to Q#31

service of up to $10Million above and beyond M1 for full points. Only work invoiced for since September 17, 2009 will be accepted. ***The following information must be provided to substantiate the business volume claimed:*** ***- Contract number(s)*** ***- Client name and contact information for verification purposes*** ***- Start and end date of contract(s), including option periods*** ***- Contract value*** ***- Amount billed for each contract referenced*** ***- 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.*** ***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.*** • **$5M to $6M = 20 points** • **>$6M to $7M = 40 points** • **>$7M to $8M = 60 points** • **>$8M to $9M = 80 points** • **>$9M to $10M = 100 points**	
#33- 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.	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.

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: 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 client project(s) within the region of delivery. 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 in the NCR in support of client projects. To be considered, a single resource may only be used/counted once. 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 individual PS resources provided the last 12-24 months** • **10 points**- 10 individual resources provided to client(s) in the NCR within the last 12-24 months; • **25 points**- 15 individual resources provided to client(s) in the NCR within the last 12-24 months; • **35 points**- 25 individual resources provided to client(s) in the NCR within the last 12-24 months; • **50 points**- 30 individual resources provided to client(s) in the NCR within the last 12-24 months	
#34- 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	Appendix C is not required to bid on this RFP and has been removed. This is not grounds for an extension.

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	
#35- Mandatory Requirement M1 requires that Bidders must complete Appendix A … to Part 4, in order to substantiate experience, and requires that experience used to demonstrate billable days "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". Appendix A to Attachment 1 to Part 4, however, it is suggested that the billing period is restricted to a scope of "24 consecutive months between dd/mm/yy to dd/mm/yy".This change also carries implications for interpreting Rated Requirement R1 as well as it is an extension of the M1 Requirement. Can the Crown please confirm that the Appendix A to Part 4 is in error as it contradicts the specifics of the mandatory and remove the 24 month scope from Appendix A as it relates to both M1 and R1 requirements? We note the enquiries period is 14 calendar days which is not typical or sufficient for an RFP of this short duration. Would the Crown kindly adjust the enquiries period to the more standard 10 calendar days in order to provide Bidders sufficient time to pose questions concerning this RFP or alternatively provide a rationale as to the justification for such a short window for questions for this RFP?	24 months is incorrect. This period is 60 months. This has been corrected in this RFP amendment. With the extension to the bid closing date, Bidder will have additional time to ask questions regarding the RFP.
The maximum of five contracts to respond to M1, and indeed to double that to maximize the R1 requirement, seems excessively narrow and would restrict the pool of Bidders for this requirement unduly. Would the Crown agree that for such a large volume of specific experience the maximum number of contracts should be ten instead of five, as has been standard in other RFPs calling for specific expertise, in order to invite an adequate number of Bidders to compete?	No changes with respect to the number of contract in order to attain experience will be considered.

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. Objectives

To acquire six (6) categories of Informatics professional services from the private sector by using the Task-Based Informatics Professional Services (TBIPS) supply arrangement on an as required basis.

2. Shared Services Canada (SSC) - Background

Shared Services Canada was created on August 4, 2011 to fundamentally transform how the Government manages its information technology (IT) infrastructure. SSC mandate is to consolidate and operate data center, network and email services with central agencies and SSC's Partners. The mandate for the provision of enterprise-wide IT-infrastructure services represents better value for money and a more reliable IT infrastructure to support modern government operations.

3. Cyber and IT Security Transformation Program (CITS)-Background

CITS Mandate: "Cyber and Information Technology Security Transformation is responsible for the development of plans and designs for GC IT infrastructure Cyber and IT security services and for GC Secret Infrastructure, within SSC mandate. This directorate will develop business cases for design-ready IT security and secret infrastructure services, and will develop and continuously improve strategic sourcing solutions, security controls and business architecture for the implementation and delivery of transformed services. This directorate fosters strategic relationships with central agencies and SSC's partners to develop policies, standards, technology guidance and on-going oversight for Cyber and IT security service management and delivery."

4. Scope of Work

Shared Services Canada (SSC), Cyber and IT Security Transformation division has a requirement for professional services on a "as and when required basis" for the services provided by IT Professionals in the IT Security domain, and to assist with the establishment of the Cyber and IT Security transformation program. CITS requires experienced, dynamic IT Security professional services with a secret clearance and expertise in various IM/IT technologies. Responsibilities will be initiated using a Task Authorization process.

The work performed under this contract will provide IT Security support and services in Unclassified, Classified and all Designated Domains for all Shared Services Canada Transformation Programs and Projects related to CITS sub-programs including:

4.1 Cyber Security sub-Program

- ***Scope:*** *... develops and continuously improves SSC's capacity to defend against emerging cyber threats through improved situational awareness, evaluation of risk likelihood and impact and the development of effective mitigation strategies. This includes developing cyber strategies, standards, guidelines, threat and impact assessments for SSC.*

- ***Functions:***
    - *Cyber Assessments and Situation Awareness*
    - *Supply Chain Integrity*
    - *Strategic Planning and policy development in the cyber security domain*

4.2 IT Security Services sub-Program

- ***Scope:*** *... consolidation and standardization of the IT Security services identified below for unclassified, designated*, and secret infrastructures. This sub-program provides ongoing planning, monitoring, advice, and guidance regarding the design, implementation and operation of these services.*
- ***Functions:***
    - *Provide IT Security Advice and Guidance and develop security controls to the three SSC-mandated Transformation Programs (DCE, DCC, TTP, WTD), TBS Back-Office Application Consolidation initiatives, security tripartite partners (CSEC, TBS), partner projects and SSC Operations;*
    - *Develop strategic approaches and provide input to strategic plans in support of IT security strategies, sourcing strategies, and IT policies*
    - *Implement Identity, Credential and Access Management (ICAM) services*
    - *Transform Network Security services at the network level*
    - *Transform Device Security services for end user devices and for backend infrastructure devices*

4.3 Government of Canada Secure Infrastructure (GCSI) sub-Program

- ***Scope:*** *... design, development and implementation of GC secret level infrastructure for common and core services to support secret level processing requirements.*
- ***Functions:***
    - *Develop the GCSI Program*
    - *Define, plan, and coordinate GCSI program projects*

4.4 Enterprise Security Requirements Definition and Integration Services

- ***Scope:*** *... define security requirements in support of steady state SSC security services to transformation programs, partner projects, and other identified government initiatives.*
- ***Functions:***
    - *This service will provide the following core activities:*
    - *Definition of Security Profiles;*
    - *Definition of Security Controls;*
    - *Provision of Security Requirements Advice and Guidance; and,*
    - *Act as security requirements liaison with CSEC and TBS.*
    - *This service will provide the following program activity in support of transformation programs and partner projects:*
    - *Defining security requirements in support of procurement documents (e.g. RFP, contracts, SOWs, etc).*

5. Personnel Requirements

The Contractor must provide Informatics Professional Services in Six (6) different resource categories on an “as and when required” basis:

RESOURCE CATEGORY	LEVEL	TBIPS ID
IT Business Analyst	Level III	B1

IT Security Planning and Protection Specialist	Level III	C1
IT TRA & C&A Specialist	Level III	C3
IT Security Design Specialist	Level III	C7
IT Security VA Specialist	Level III	C11
IT Privacy Specialist	Level III	C16

These professional services are required in a large number of projects all related to the EA mandate identified above, or in general activities for related projects including: as Enterprise Architecture; Security Architecture, Evaluations or Certifications; and/or Project Management.

The level of effort and duration of projects may vary (e.g. from two weeks to two+ years). The Contractor personnel involved in both shorter and longer-term projects must be prepared to perform the same tasks repetitively. The Contractor personnel involved in longer duration projects may be required to participate in either all of the project, or only the part of the project pertaining to their area of expertise (possibly while working in a preformed project team).

The required services will be related to one or more of the activities listed below (Note: these activities are not inclusive of the entire spectrum of activities which may require the involvement of Contractor personnel):

5.1 Role Descriptions

The following provides a description of the proposed tasks and duties to be performed by each resource category.

5.1.1 <u>B1 Business Analyst Level 3</u>

The following responsibilities are associated with this “Statement of Work” (but are not limited to):

1) Develop, review and manage business requirements
2) Plan, coordinate, capture and follow up on meetings with SSC partner Departments and agencies for business requirements gathering along with their prioritization, associated business impact, costs/cost models and business dependencies
3) Perform analysis of the business requirements to identify and document SSC and partner roles and responsibilities
4) Perform analysis of the business requirements to identify and document information, procedures and decision flows, and associated policies
5) Capture the current use cases associated with the business requirements
6) Obtain and manage formal written SSC partner approvals of the business requirements specification document
7) Establish acceptance test criteria with client
8) Support and use the selected departmental methodologies
9) Document, review with stakeholders and track actions and meetings decisions
10) Identify and document current state business processes (business or operations)
11) Provide guidance to technical architects and developers to meet the requirements

12) Develop presentations for stakeholders or senior executives
13) Perform business analysis of functional requirements to identify information, procedures and decision flows
14) Identify and evaluate existing procedures, methods, and items such as database content and structure
15) Define and document interfaces of manual to automated operations within application subsystems, to external systems and between new and existing systems
16) Working with various stakeholders and other sources to understand and identify all requirements information that is relevant to the project. Facilitates cross-functional meetings and exercises to verify current state, to capture requirements and to ensure Cyber project(s) alignment to existing transformation initiatives/ programs;
    a) Planning and implementing all requirements-related activities, including elicitation, validation, reporting status, resolving conflicts, and gaining approval.
17) Develops and manages detailed business and functional requirements for Cyber project(s), by preparing use cases, data models, and capturing existing business rules from various forms of documentation such as process maps and interviews with subject matter experts. Organizing, structuring and understanding the elicited requirements; putting them into an appropriate form, and performing necessary verification and validation on them;
    a) Managing the requirements themselves, including requirements change control and scope control.
18) Assists in detailed design and development by maintaining “To-Be” process models, undertaking issues analysis and ensuring architecture and technical teams understand the underlying business objectives and functional capabilities required for project success.

The service required is to assist with the development and delivery of both an interim and longer-term Cyber Infrastructure Recall System by working among stakeholders and subject matter experts in gathering, analysing, modelling, communicating and validating requirements for architecture and design.

As time permits, the business analyst may be engaged in other work to support the Cyber Program.

In the course of this work, the Contractor may be required to provide Project Management assistance, with any or all of the tasks detailed below, to other professionals whose tasks fall within the Cyber Security program scope.

General Program Support:

a) Developing business documents such as business cases and strategic investment proposals and ensuring alignment with the Directorate’s business plan.

b) Analyzing and documenting new and existing business processes to support Cyber Program and project objective(s)

c) Assists the project managers in the preparation of project charters, statements of work, project plans and schedules; Assists project managers in performing processes that support the project management planning domains such as change control process, issue tracking, risk management and SSC gating processes

5.1.2 C1 IT Security Planning and Protection Specialist Level 3

The following responsibilities are associated with this “Statement of Work” (but are not limited to):

1) Review, analyze, and/or apply the IT Security Policies, Procedures and Guidelines of International government, Federal, Provincial or Territorial government.
2) Review, analyze, and apply the best practices, national or international computer law and ethics, IT Security architecture, and IT Security Risk Management Methodology
3) Develop vision papers delineating the way ahead to ensure that IT Security and cyber protection are business enablers
4) Conduct business function analysis and business impact assessments
5) Brief senior managers
6) Provide strategic assessments on technology trends and emerging technologies
7) Provide IT Security strategic planning and advice.
8) Conduct feasibility studies, technology assessments and cost-benefit analyses, and propose system implementation plans for IT Security
9) Develop advanced R&D policy/strategy
10) Collect, collate and prioritize client IT Security and Information Infrastructure Protection requirements
11) Evaluate and assist in the selection of enterprise-wide technology tools
12) Review and prioritize IT Security and Information Infrastructure Protection programs
13) Develop strategic IT Security architecture vision, strategies and designs using the Business Transformation Enablement Program (BTEP) methodology and the Government Strategic Reference Model(GSRM)
14) Develop IT Security programs and service designs using the following GSRM models: Program Logic Model, Program and Service Alignment Model, Service Integration and Accountability Model, State Transition Model, Information Model and Performance Model
15) Develop and deliver training material relevant to the resource category
16) Review and prioritize IT Security and Information Infrastructure Protection programs

5.1.3 C3 Security TRA and C&A Analyst Level 3

The following responsibilities are associated with this “Statement of Work” (but are not limited to):

1) Following the GC Harmonized Threat & Risk Assessment (HTRA) Methodology, formulate and document Statements of Sensitivity, identify threat agents, threats and threat scenarios, perform threat assessment, determine risks, identify potential vulnerabilities and recommend safeguards and other risk mitigation strategies on the IT enterprise-wide infrastructure, systems, and services identified by the Technical Authority
2) Formulate and document a draft and final Threat Assessment report
3) Formulate and document a draft and final Threat Risk Assessment report
4) Develop a report that synthesizes recommendations and risk mitigation strategies for senior management and other stakeholders, with supporting detailed technical documentation
5) Work in partnership with all stakeholders to identify technical architecture, challenges, risks, and recommendations for various SSC projects related to the SSC’s Transformation Programs/Initiatives

6) Collaborate with all stakeholders on the evaluation of any relevant data from service providers, transformation teams, project management build teams and operational teams
7) Complete tasks as needed directly supporting the GC and SSC Cyber and IT Security Transformation Program as well as other CITS core transformation programs
8) Produce various security artifacts as needed
9) Participation in related IT Security meetings, discussions and presentations to stakeholders or senior management
10) Document, review and track actions and meetings decisions
11) Perform functional and options analysis in support of program delivery
12) Perform impact analysis with the perspective of an enterprise solution, evaluate and make recommendations
13) Create presentations and present to various stakeholders, and facilitate meetings and discussions
14) Review Statement of Sensitivity, Statement of Acceptable Risk documents
15) Identify threat agents, threats and threat scenarios, determine risks, identify potential vulnerabilities and recommend appropriate safeguards and other risk mitigation strategies on the IT infrastructure, systems, applications and services identified by the Technical Authority, while re-using existing relevant information as much as possible
16) Verify that security safeguards for applications, systems, and infrastructures meet the applicable policies and standards
17) Verify that security safeguards have been implemented correctly
18) Assess and verify that residual risk indicated in risk assessments meet an acceptable level
19) Review security assessment results to ensure that the system will operate at an acceptable level of risk and that it will comply with the departmental and system security policies and standards
20) Support the Certification Authority in evaluating the certification evidence package
21) Responsible for producing a number of SSC CITS ITSPD template documents, such as: SA&A Reports, Briefing Notes ITSG-33 based security controls profiles, TRAs, as well as other types of security assessments
22) Write Certification Report and Accreditation Letters based on status of the safeguards selected and implemented
23) Witness security tests where appropriate
24) Review and critique safeguard implementation plans
25) Audit results of security testing, security validation and security checklist compliance;
26) Collaborate on the investigation of security requirements, attributes, and safeguards that further enhance the security profile of the system
27) Assist business partners in the development of security requirements (Statement of Sensitivity, Asset Categorization, Threat modelling, Business Needs for Security, Statement of Acceptable Risk, etc...)
28) Assessment of Reference Architecture Documents, Technical Architecture Documents and Detailed Design Documents as they apply to security
29) Assessment of IT security controls (ITSG33 based) and safeguards
30) Assessment of mitigation strategies
31) Assessment of residual risk
32) As required, deliver IT Security training awareness sessions
33) Other ad hoc technical documents or reports as required by the Certification Authority.
34) The SA&A evidence review includes producing a Shared Services Canada (SSC) Certification Report as well as the related evidence package. Documents to review to produce both the report and package include (but are not limited to) Privacy Assessment questionnaire, Statement of Sensitivity, Architecture Diagrams, Statement of Acceptable Risk, Security Testing and Evaluation plan, Vulnerability Assessment report, Safeguard Implementation Plan, Concept of Operations, Security Requirements Traceability Matrix

35) Security Concept of Operations
36) A high level overview of what security (from privacy, organizational, administrative, personnel, and technical, procedural and contingency management viewpoints) must be met in the final system's design solution
37) A contextual security view of the project functionality (logical diagrams, specific business level circumstances, conditions and concerns) that the system's security design will be expected to satisfy
38) Architecture Design
39) Describes the conceptual design, logical design, network design and physical design from a security perspective
40) Threat and Risk Assessment comprised of:
    a) Statement of sensitivity
    b) Threat assessment
    c) Non-technical vulnerability assessment
    d) Risk assessment
    e) Recommendations for risk mitigation
    f) Privacy Assessment (Questionnaire)
    g) Security Requirements Traceability Matrix
    h) Security Testing and Evaluation Plan
    i) Vulnerability Assessment (VA) / Penetration Testing
    j) Develop Vulnerability Assessment Plan
41) In consultation with required parties, conduct (or observe in some cases) and document results of Vulnerability Assessment (VA) / Penetration Testing
42) Safeguard Implementation Plan
43) Identification of deficiencies found during formal security testing and evaluation activities and/or the final TRA with recommendations to address the deficiencies in the achievement of the required security
44) Provide evidence that services and /or applications and infrastructure meets the requirements that have been documented in the above mentioned deliverables, including:
    a) Verification that security safeguards meet the applicable policies and standards;
    b) Validation of security requirements by mapping system-specific security policy to functional security requirements, and mapping the security requirements through the various stages of design documents
    c) Verification that security safeguards have been implemented correctly and that assurance requirement have been met. This includes confirming that the system has been properly configured, and establishing that the safeguards meet applicable standards
    d) Security testing and evaluation (ST&E) to determine if the technical safeguards are functioning correctly
45) Review and provide written feedback on the following types of deliverables:
    a) Security Management Plan
    b) Privacy Management Plan
    c) Service Continuity Plan
    d) Security Risk Assessment Reports
46) Contractors' plans, documents and evidence of an ISO 27001 certified or equivalent Information Security Management System (ISMS)

5.1.4 <u>C7 IT Security Design Specialist Level 3</u>

The following responsibilities under this contract include the following, but not limited to:

1) Work in partnership with all stakeholders to identify technical architecture, challenges, risks, and recommendations for various SSC projects related to the SSC's Transformation Programs/Initiatives
2) Collaborate with all stakeholders on the evaluation of any relevant data from service providers, transformation teams, project management build teams and operational teams
3) Complete tasks as needed directly supporting the GC and SSC Cyber and IT Security Transformation Program as well as other CITS core transformation programs;
4) Conduct analysis of Current State Assessments in support of CITS core transformation programs
5) Produce various security artifacts as needed
6) Participation in related IT Security meetings, discussions and presentations to stakeholders or senior management
7) Document, review and track actions and meetings decisions
8) Perform functional and options analysis in support of program delivery
9) Perform impact analysis with the perspective of an enterprise solution, evaluate and make recommendations
10) Create presentations and present to various stakeholders, and facilitate meetings and discussions
11) Provide Security Training & Awareness

12) IT Security requirements support for core CITS Transformation Programs comprised of, but not limited to:

    a) Review business and IT Security requirements from various SSC programs and initiatives
    b) Work in partnership with all stakeholders to develop security control profiles based on CSEC ITSG-33 and other related security standards, in support of various SSC projects related to SSC's Transformation Programs/Initiatives
    c) Validate IT Security requirements by mapping business and/or security requirements through the various stages of the Information System Security Implementation Process (ISSIP)
    d) Analyze and evaluate client requirements and documentation
    e) Plan, conceptualize, coordinate and document recommendations for solutions based on client requirements
    f) Perform functional and options analysis in support of program delivery
    g) Perform impact analysis with the perspective of an enterprise solution, evaluate and make recommendations.

13) IT Security strategies, frameworks, models, methodologies, roadmaps, plans, heat maps, RACI matrices, policies and instruments in the areas of, but not limited to:
    a) Security Risk Management, including risk assessment methodologies
    b) Security Assessment & Authorization (SA&A)
    c) Security Program Management and Governance, including organizational and/or functional design or review, and IS and/or ITS program-level compliance reporting
    d) Review/analyze various SSC and/or TBS transformation initiative deliverables and ensure compliance, alignment, and conformity of deliverables with Government of Canada (e.g., TBS, CSEC, PS, SSC) IT Security strategies, principles, methodologies,

frameworks, programs, policies and instruments (directives, standards, guidelines), and procedures

e) Develop IT Security standards, procedures and guidelines pursuant to the requirements of Canada's National Security Policy, Treasury Board Secretariat's Policy on Government Security, and supporting operational standards (e.g., MITS), departmental/agency security policy, and other relevant standards, procedures and guidelines

f) Develop IT Security policy in the areas of IT security and assurance, standard Certification & Accreditation frameworks for IT systems, information infrastructure protection, product evaluation, privacy, Business Continuity Planning, contingency planning and Disaster Response Planning, Research & Development and IT Security Service Management.

14) IT Security risk management comprised of, but not limited to:

a) Review/analyze various SSC and/or TBS transformation initiative deliverables and ensure compliance, alignment, and conformity of deliverables with Government of Canada (e.g., TBS, CSEC, PS, SSC) IT Security strategies, principles, methodologies, frameworks, programs, policies and instruments (directives, standards, guidelines), and procedures;

b) Recommendations for IT Security risk mitigation and other related deliverables, as required.

Additional deliverables requirements for Cyber Security sub-Program (but are not limited to):

- Assist in completing all necessary documentation (such as Reports, Roadmaps, Presentation decks) on various current-state assessments (such as Communications Security (COMSEC), Local Information Protection Centre (LIPC);
- Document security related processes for transformation initiatives);
- Development of Request for proposals (RFP) documents to assist in the procurement process of security hardware/software to be used in the Shared Services Canada – Security Operations Centre (SSC-SOC).

Additional deliverables requirements for Security Services sub-Program (but are not limited to):

- Contribute to the development and/or create the following documentation in support of Device Security:
  a) Project Plan
  b) Project Charter
  c) Business Case
  d) Communications Plan
  e) Service Definition, Change Management Strategy/Plan and Implementation Strategy
  f) Procurement Strategy including: Request For Information (RFI), Request For Proposal (RFP), Statement of Work (SoW),
  g) Industry Day Information (i.e. Questions and Answers pertaining to Device Security, presentation)
  h) Security Assessment & Authorization Artifacts (Statement of Sensitivity, Concept of Operations, Threat Assessments).

- Develop and validate ITSG-33 security control profiles in support of various SSC back office projects related to the transformation of network perimeter security services;
- Create presentations and present to various stakeholders, and facilitate and record meetings and discussions as requested by the Technical Authority;
- Provide and document various security control profiles, reports, security analyses, work breakdown structures, schedules, and other related documents as requested by the Technical Authority.

Additional deliverables requirements for Enterprise Security Requirements Definition sub-Program (but are not limited to):

- Document requirements-gathering and security assurance input related to large scale Telecom and Converged Communications projects and possibly for other SSC Transformation Programs.
- Create and document service definitions for Telecom and Converged Communications-related projects, and possibly for other SSC Transformation Programs.
- Per ITSG-33 ISSIP security lifecycle process, determine and document related security controls based on GC, NIST and other guidance for input in to Enterprise architecture documents, RFP SOWs, and in order to fulfill the SA&A process. Input will be required commencing with the Concept phase and continuing through to the Installation phase.
- Perform and document Threat Assessments Reports.

5.1.5 C11 IT Security VA Specialist Level 3

The following responsibilities and scope of work under this contract include the following, but not limited to:

1) Review, analyze, and/or apply:
   a) 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
   b) War dialers, password crackers
   c) Public Domain IT vulnerability advisory services
   d) Network scanners and vulnerability analysis tools such as SATAN, ISS, Portscan & NMap
   e) Networking Protocols (HTTP, FTP, Telnet)
   f) Internet security protocols such as SSL, S-HTTP, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP, SNMP
   g) Wireless Security
   h) Intrusion detection systems, firewalls and content checkers
   i) Host and network intrusion detection and prevention systems - Anti-virus management
2) Identify threats to, and technical vulnerabilities of, networks
3) Conduct on-site reviews and analysis of system security logs
4) Collect, collate, analyze and disseminate public domain information related to networked computer threats and vulnerabilities, security incidents and incident responses
5) Prepare and/or deliver IT Security threat, vulnerability and/or risk briefings
6) Completed tasks directly supporting the departmental IT Security and Cyber Protection Program
7) Develop and deliver training material relevant to the resource category

5.1.6 C16 IT Security Specialist (Privacy) Level 3

The following responsibilities and scope of work under this contract include the following, but not limited to:

1) The Privacy Specialist will analyze privacy concerns related to SSC Services, create and deliver privacy checklist documents for review and approval, perform Privacy Impact Assessments (PIAs) against SSC services and work on various documents in response to the Office of Privacy commissioner
2) The work performed needs to be done according to the following standards, policies documents and best practices:
    a) Privacy Act and related provincial legislation
    b) Office of Privacy Commissioner Expectations on completing Privacy Impact Assessments (PIAs)
    c) Latest TBS Directive on Privacy Impact Assessments (PIA) (Treasury Board Core Privacy Impact Assessment (PIA) template)
    d) CSA's Model Code for the Protection of Personal Information (Q830)
    e) Records Management.
3) The resource is required to have extensive knowledge of the GC standards, policies and guidelines
4) The resource should be certified in the field of IT Privacy, preferably through an industry recognized certification body
5) Must analyses privacy concerns related to SSC services
6) Must create and deliver of privacy checklist document for review and approval
7) Must perform Privacy Impact Assessments (PIA) against SSC services while consulting with the Program area and Access to Information and Privacy (ATIP);
8) Must create and update (as required) presentations, briefing notes, responses to letters from the Office of Privacy Commissioner OPC, related to Privacy Impact Assessments (PIA) performed or in progress
9) Must assist with and review Privacy Impact Assessment (PIA) related activities pursuant to the new TBS Directive on Privacy Impact Assessments, and related policies and instruments (standards, processes, guidelines, and procedures)
10) Must assess privacy risks and propose mitigation mechanisms or strategies
11) Must review project documentation where available and/or applicable including demonstration(s), data flow diagrams and presentation materials
12) Must initiate and participate in discussions regarding privacy issues
13) Must meet with Office of Privacy Commissioner (OPC) to discuss elements of the Privacy Impact Assessment (PIA) and issue record of decision for each meeting. Follow-up on any action items identified
14) Must accept, review and respond to questions from departmental stakeholders prior to producing the final Privacy Impact Assessment (PIA) report(s)
15) Must follow-up on further information requirements; discuss privacy and policy risks that may be identified during analysis
16) Must review project documentation related to IT issues, technologies and architecture influencing privacy risks
17) Must report on compliance with policies and related instruments (e.g., directives, standards, processes, guidelines, and procedures)
18) Must produce final draft Privacy Impact Assessment (PIA) reports within a sufficient timeframe to allow ample opportunity to review findings with all stakeholders including ATIP
19) Must finalize Privacy Impact Assessments (PIAs)and briefing notes

6.0 Deliverables

- The actual requirements for resources will be identified on an "as-and-when-requested" basis through an approval Task Authorization (TA).
- In addition to the services described in each resource category, while performing the Work each resource must provide to or a representative of a GC entity technical advice and the transfer of functional knowledge through the provision of written documents and individual and group training.
- The Contractor must provide the deliverables (in draft, final or both forms) to the Technical Authority or their representative as specified in each Task Authorization (TA). The scope and specific content of each deliverable will be submitted to the Technical Authority for review and to determine acceptance.
- The final copies of the deliverables must incorporate the comments received and changes requested by the Technical Authority or their representative and will be delivered on or before the end date specified in each TA.
- Each resource must submit a weekly status report to the Technical Authority conforming to the report format specified in each TA.
- The schedule, format and content of each deliverable shall be mutually agreed to by the Task Authorization (TA) and the Contractor in writing and will be based on the Task Authorization TA's organizational standards (e.g. business requirement template to be used, standard architecture format for business views, etc.).
- Documentation deliverables shall be in hard copy format and electronic copy format using Microsoft (MS) Office suite of products, or agreed by the contractor and the Technical Authority in the event other format would be suitable.
- Progress (Status) Report. The Contractor shall prepare a written status and progress report on the work performed for the project, which is to be attached to the monthly timesheet claim. At a minimum, progress reports shall contain the following information:
  - All significant activities performed by the Contractor(s) during the period,
  - Status of all action/decision items, as well as a list of outstanding activities,
  - A description of any problems encountered which are likely to require the attention of the Technical Authority, and any recommendations relating to the conduct of the work.
  - Current milestones with planned dates, progress since last report, issues encountered, and next steps.
  - Hours expended by the contractor against the task during the reporting period.
  - Highlight the expectations/deliverables for the coming month, week, quarter.
- Progress report and timesheet must also be included when sending the invoice.

7. Format of Deliverables

Progress Reports must be submitted to the Technical Authority by email.

Unclassified and Protected-A documents can be submitted by email within the GC email system. Protected-B documents must be encrypted using a GC PKI Key then can be submitted within the GC email system. Secret documents (if applicable) must include one hard copy and one copy in electronic format (CD, DVD, or USB) and shall be hand delivered to the Technical Authority.

Deliverables must be editable in Microsoft Office Suite (e.g., Word, Excel, PowerPoint and Visio) version 2007 or newer.

8. Regular Meetings

The Contractor's Project Authority must meet with the Technical Authority or their representative on a priority basis or as requested to discuss any issues associated with the provision of the required Informatics Professional Services. These meetings will be at no additional cost.

9. Service Levels

9.1 Normal Working Hours

Normal working hours will be no earlier than 7:00 am to no later than 6:00 pm EST Monday through Friday (with the exception of statutory holidays as defined by the province of work). The Contractor will be expected to work 7.5 hours/day within normal working hours, unless arrangements are made ahead of time with the Technical Authority. The Technical Authority will authorize additional hours of work in advance at the same rate as normal office hours. The Contractor will normally work during regular business hours, on site, unless otherwise agreed upon by the Contractor and the Technical Authority. For the duration of the contract all personnel must be available to work outside normal office hours as required.

9.2 Work location

The contractor's work will be performed on-site at Shared Services Canada or off-site (at the discretion of the Technical Authority/Manager). Shared Services Canada is located within the National Capital Region and access to IT systems and infrastructure will be made available as required. Over the duration of the Contract, the main location of business of SSC's various locations or Branches may change but will remain in the National Capital Region (NCR), and no costs will be paid by SSC to the Contractor to compensate for any costs associated with such transition. The contractor is required to attend meetings at Shared Services Canada and at Key GC Stakeholders, but no significant travel will be required. All expenses for travel within the NCR are to be paid by the Contractor.

A TA could require that work be performed off-site on infrastructure provided by the Contractor.

9.3 Travel Requirement

There is no travel requirement expected to conduct the Statement of Work. However, if travel is deemed necessary, Travel and Living expenses will only apply when the Contractor is requested to work outside the National Capital Region. If required, the Project Authority must authorize travel in advance, in writing.

Invoices for Travel and Living costs are to be supported by documentation (receipts) and will be reimbursed in accordance with the Treasury Board Policy and Guidelines on Travel in effect at the time of travel at actual cost with no allowance for mark-up or profit. Charges for air travel shall not exceed that for economy travel.

9.4 Reporting Relationship

The resource will functionally report to the Technical Authority/Manager.

10. Security Requirement

The resource must be cleared to a minimum of Secret throughout the course of the contract. Bidder must specify security clearance file number and expiration date.

11. Non-Disclosure

All work carried out by the contractor with respect to this Statement of Work will remain the property of the Crown. All reports, documentation, and extensions thereto shall remain the property of the Crown and the contractor shall not divulge, disseminate or reproduce such reports and/or documentation to any other person without the prior written permission of the Crown.

12. Proprietary Information

All information and documents made available to the contractor during the course of this project are deemed proprietary, and shall be returned to the Crown upon completion of the tasks specified in this Statement of Work or upon termination of the contract.

13. Interpretation

In the case of disputes regarding interpretation of statement of this Statement of Work or any of the terminology contained herein, the ruling of the Technical Authority shall prevail.

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**
Business System Class	
Business Analyst - Level 3	
Cyber Protection Services Class	
IT Security Planning and Protection Specialist - Level 3	
IT TRA & C&A Specialist - Level 3	
IT Security Design Specialist - Level 3	
IT Security VA Specialist - Level 3	
IT Privacy Specialist - Level 3	

FOR THE OPTION YEAR 1 (1 YEAR)	
Category of Personnel	**Bidders Proposed Per Diem Rate**
Business System Class	
Business Analyst - Level 3	
Cyber Protection Services Class	
IT Security Planning and Protection Specialist - Level 3	

IT TRA & C&A Specialist - Level 3	
IT Security Design Specialist - Level 3	
IT Security VA Specialist - Level 3	
IT Privacy Specialist - Level 3	

FOR THE OPTION YEAR 2 (1 YEAR)	
Category of Personnel	**Bidders Proposed Per Diem Rate**
Business System Class	
Business Analyst - Level 3	
Cyber Protection Services Class	
IT Security Planning and Protection Specialist - Level 3	
IT TRA & C&A Specialist - Level 3	
IT Security Design Specialist - Level 3	
IT Security VA Specialist - Level 3	
IT Privacy Specialist - Level 3	

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.