RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0A1 / Noyau 0A1
Gatineau, Québec K1A 0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

THIS REQUIREMENT CONTAINS A SECURITY REQUIREMENT - SEE PART 6.

Issuing Office - Bureau de distribution

Business Management and Consulting Services Division / Division des services de gestion des affaires et de consultation
11 Laurier St. / 11, rue Laurier
10C1, Place du Portage
Gatineau, Québec K1A 0S5

Title - Sujet
PCI CONSULTANT

Solicitation No. - N° de l'invitation	Date
EN891-121307/B	2012-04-04

Client Reference No. - N° de référence du client
20121307

GETS Reference No. - N° de référence de SEAG
PW-$$ZG-406-24295

File No. - N° de dossier	CCC No./N° CCC - FMS No./N° VME
406zg.EN891-121307	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2012-05-15

Time Zone
Fuseau horaire
Eastern Standard Time
EST

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Harrington, Ingrid	406zg

Telephone No. - N° de téléphone	FAX No. - N° de FAX
(819) 956-3201 ( )	(819) 956-2675

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Specified Herein
Précisé dans les présentes

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée	Delivery Offered - Livraison proposée
See Herein	

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

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Destination Code - Code destinataire	Destination Address - Adresse de la destination	Invoice Code - Code bur.-comptable	Invoice Address - Adresse de facturation
D - 1	DEPARTMENT OF PUBLIC WORKS AND GOVERNMENT SERVICES CANADA TPSGC/PWGSC NATIONAL CAPITAL AREA (GATINEAU) PHASE III, PLACE DU PORTAGE 11 LAURIER ST. GATINEAU, QC K1A0S5	EN891	DEPARTMENT OF PUBLIC WORKS AND GOVERNMENT SERV PORTAGE III 15A2 11 LAURIER ST Gatineau Quebec K1A0S5 Canada

Item Article	Description	Dest. Code Dest.	Inv. Code Fact.	Qty Qté	U. of I. U. de D.	Unit Price/Prix unitaire FOB/FAM Destination	Plant/Usine	Delivery Req. Livraison Req.	Del. Offered Liv. offerte
1	PCI CONSULTANT	D - 1	EN891	1	LOT	$	XXXXXXXXXX	See Herein	
2	LOI	D - 1	EN891	1	LOT	$	XXXXXXXXXX	See Herein	

TABLE OF CONTENTS

PART 7 - RESULTING CONTRACT CLAUSES

1. Statement of Work
2. Standard Clauses and Conditions
3. Security Requirement
4. Term of Contract
5. Authorities
6. Payment
7. Invoicing Instructions
8. Certifications
9. Applicable Laws
10. Priority of Documents
11. SACC Manual Clauses
12. Foreign Nationals (Canadian Contractor)
    Foreign Nationals (Foreign Contractor)
13. Insurance
14. Government Site Regulations

List of Annexes:

Annex A, Statement of Work
Annex B, Basis of Payment
Annex C, Security Requirements Check List
Annex D, Task Authorization Form

PART 1 - GENERAL INFORMATION

1. Introduction

The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

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

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation ;

Part 3 Bid Preparation Instructions: provides bidders with instructions on how to prepare their bid;

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

Part 5 Certifications: includes the certifications to be provided;

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The Attachments include Pricing Schedule, Technical and Financial Criteria, Certifications Precedent to Contract Award, Certifications Required with the Bid.

And

The Annexes include the Statement of Work, Basis of Payment, Security Requirements Check List and Task Authorization Form.

2. Summary

2.1 The Receiver General (RG) requires the advice and knowledge transfer of a Contractor that has an in-depth understanding of the Payment Card Industry Data Security Standards (PCI DSS) best practices. While individual requirements will be specified in each Task Authorization (TA) the RG requires qualified resources to provide the following services on an as and when requested basis.

The qualified resources will be required to:

- Provide an in-depth review of departmental business flows and security controls to provide PCI compliance audit readiness and ultimately, ensure each federal department is either fully PCI DSS compliant or has a clear timeline for compliancy;
- Ensure knowledge to oversee the PCI project is transferred to the RG PCI project office and governance body; and
- Provide guidance in the effective establishment and management of competitive contractual arrangements to obtain the services of a Qualified Security Assessor (QSA), an Approved Scanning Vendor (ASV) and / or the acquisition of PCI DSS tools.

The Contractor's work will take place primarily at the Contractor's premises. Certain meetings will be conducted in person at the Receiver General's headquarters in the National Capital Region (NCR) or at department's locations.

The period of the Contract will be two (2) years commencing from date of contract with an irrevocable option, on the part of Canada, to extend the Contract by up to two (2) additional one (1) year periods, under the same terms and conditions of the Contract.

There is a security requirement associated with this requirement. Bidder's are reminded to obtain the required security clearance promptly. Please refer to Part 6, Security Requirements, Part 7, Resulting Contract Clauses Security Requirement and Annex C Security Requirements Checklist and its associated attachment. Bidders who currently do not meet the facility security clearance requirements and (or) personnel security clearance are advised to initiate the security clearance process immediately by requesting sponsorship from the Contracting Authority.

For any inquiries concerning any security requirements, bidders should contact CISD at 1-866-368-4646, or (613) 948-4176 in the National Capital Region (NCR), CISD Website: *http://ssi-iss.tpsgc-pwgsc.gc.ca/*.

3. Debriefings

After contract award, bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days of receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

4. Prohibition to Bid on Future Related Requirement

The Contractor, during and after the period of performance of the Contract agrees that it and its parent, subsidiaries or other affiliates, and its subcontractors must not bid on the future solicitation to contract the services of a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV), and must not participate as an agent, subcontractor or consultant in the preparation of any other Bidder's tender or proposal for such requirement.

PART 2 - BIDDER INSTRUCTIONS

1. Standard Instructions, Clauses and Conditions

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

Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

The 2003 (2011-05-16), Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation, with the following modification: subsection 1. (a) and (b) of Section 12, Rejection of Bid, must be replaced with the following:

1. Canada may reject a bid where any of the following circumstances is present:

(a) the Bidder is subject to a Vendor Performance Corrective Measure, under the Vendor Performance Corrective Measure Policy, which renders the Bidder ineligible to bid on the requirement;

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

Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: sixty (60) days
Insert: One hundred and twenty (120) calendar days

2. Submission of Bids

Bids must be submitted only to Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and place indicated on page 1 of the bid solicitation. Bids transmitted to PWGSC by electronic mail will not be accepted.

Due to the nature of the bid solicitation, bids transmitted by facsimile to PWGSC will not be accepted.

3. Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than fifteen (15) calendar days before the bid closing date. Enquiries received after that time may not be answered.

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as “proprietary” will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the questions or may request that the Bidder do so, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all bidders. Enquiries not submitted in a form that can be distributed to all bidders may not be answered by Canada.

4. Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in the province of Ontario.

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the bidders.

5. Basis for Canada's Ownership of Intellectual Property

Canada has determined that any intellectual property rights arising from the performance of the Work under the resulting contract will belong to Canada, on the following grounds:

- where the material developed or produced consists of material subject to copyright, with the exception of computer software and all documentation pertaining to that software

6. Improvement of Requirement During Solicitation Period

Should bidders consider that any or all of the security requirements in the Information Technology Security Requirements Technical Document in the attachment to Annex C SRCL, contained in the bid solicitation, could preclude them from meeting the security requirements and therefore affect their ability to bid, bidders are invited to provide comments, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly explain what would preclude them from bidding. Comments will be given consideration provided they are submitted to the Contracting Authority at least fifteen (15) days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

PART 3 - BID PREPARATION INSTRUCTIONS

1. Bid Preparation Instructions

Canada requests that bidders provide their bid in separately bound sections as follows:

Section I: Technical Bid (4 hard copies);
Section II: Financial Bid (1 hard copy); and
Section III: Certifications (1 hard copy).

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

Canada requests that bidders follow the format instructions described below in the preparation of their bid:

(a) use 8.5 x 11 inch (216 mm x 279 mm) paper; and
(b) use a numbering system that corresponds to the bid solicitation.

In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process Policy on Green Procurement (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html).

To assist Canada in reaching its objectives, bidders are encouraged to:

1) use paper containing fibre certified as originating from a sustainably-managed forest and/or containing minimum 30% recycled content; and

2) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

Section I: Technical Bid

In their technical bid, bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

Part 4, Evaluation Procedures, contains additional instructions that bidders should consider when preparing their technical bid.

Section II: Financial Bid

1.1 Bidders must submit their financial bid in Canadian funds and in accordance with the pricing schedule detailed in Attachment 1 to Part 3. The total amount of Goods and Services Tax (GST) or Harmonized Sales Tax (HST) must be shown separately, as applicable.

1.2 Bidders must submit their rates FOB destination; Canadian customs duties and excise taxes included, as applicable; and GST or HST excluded.

1.3 When preparing their financial bid, bidders should review the basis of payment in Annex B and clause 1.2, Financial Evaluation, of Part 4**.**

1.4 The rates included in the pricing schedule detailed in Attachment 1 to Part 3 exclude the total estimated cost of all travel and living expenses that may need to be incurred for Work described in Part 7, Resulting Contract Clauses, of the bid solicitation required to be performed outside the National Capital Region (NCR). The NCR is defined in the *National Capital Act*, R.S.C. 1985, c. N-4, S.2. *The National Capital Act* is available on the Justice Website: http://laws.justice.gc.ca/eng/acts/N-4 /"

1.5 Bidders should include the following information in their financial bid:

1. Their legal name;
2. Their Procurement Business Number (PBN); and
3. The name of the contact person (including this person's mailing address, phone and facsimile numbers and email address) authorized by the Bidder to enter into communications with Canada with regards to:
   a. their bid; and
   b. any contract that may result from their bid.

1.6 SACC Manual Clauses

C3011T (2010-01-11) Exchange rate Fluctuation

Section III: Certifications

In Section III, Bidders should include the certifications required under Part 5.

ATTACHMENT 1 to PART 3
PRICING SCHEDULE

The Bidder should complete this pricing schedule and include it in its financial bid once completed. As a minimum, the Bidder must respond to this pricing schedule by including in its financial bid for each of the periods specified below its quoted all inclusive fixed hourly rate (in Cdn $) for each of the resource categories identified.

The inclusion of volumetric data in this document does not represent a commitment by Canada that Canada's future usage of the services described in the bid solicitation will be consistent with this data.

The rates specified below, when quoted by the Bidder, include the total estimated cost of all travel and living expenses that may need to be incurred for:

a. work described in Part 7, Resulting Contract Clauses, of the bid solicitation required to be performed within the National Capital Region (NCR). The NCR is defined in the *National Capital Act*, R.S.C. 1985, c. N-4, S.2. *The National Capital Act* is available on the Justice Website: http://laws.justice.gc.ca/eng/acts/N-4/ ;

b. travel between the successful bidder's place of business and the NCR; and

c. the relocation of resources

to satisfy the terms of any resulting contract. These expenses cannot be charged directly and separately from the professional fees to any contract that may result from the bid solicitation.

	PERIOD / CATEGORY	**QUOTED ALL-INCLUSIVE FIXED HOURLY RATE (in Cdn $)**	**Volumetric Data (estimated hours)**	**Total (in Cdn $)**
		A	**B**	**C= A x B**
1	**Contract Period: Year 1 and Year 2**			
1a	Senior PCI Advisor		1500	
1b	PCI Advisor		1500	
			Total Contract Period:	
2	**Optional Period - Year 3 and Year 4**			
2a	Senior PCI Advisor		1500	
2b	PCI Advisor		1500	
			Total Optional Period:	
3	**Evaluated Price (GST/HST excluded):** **$**_____ (i.e., sum of: Total Contract Period + Total Optional Period)			
4	**GST or HST** Insert GST or HST amount, as applicable:			GST: HST:

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

1. Evaluation Procedures

(a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria.

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

1.1 Technical Evaluation

1.1.1 Mandatory Technical Criteria

Refer to Attachment 1 to Part 4.

1.1.2 Point Rated Technical Criteria

Refer to Attachment 1 to Part 4. Point-rated technical criteria not addressed will be given a score of zero.

1.2 Financial Evaluation

1.2.1 The volumetric data included in the pricing schedule detailed in Attachment 1 to Part 3 are provided for bid evaluated price determination purposes only. They are not to be considered as a contract guarantee.

1.2.2 For bid evaluation and contractor(s) selection purposes only, the evaluated price of a bid will be determined in accordance with the Pricing Schedule detailed in Attachment 1 to Part 3.

2. Basis of Selection

2.1 Basis of Selection - Lowest Evaluated Price Per Point

1. To be declared responsive, a bid must:

(a) comply with all the requirements of the bid solicitation;

(b) meet all the mandatory evaluation criteria; and

(c) obtain the required minimum number of points specified in Attachment 1 to Part 4 for the point rated technical criteria.

2. Bids not meeting (a) or (b) or (c) will be declared non-responsive. Neither the responsive bid obtaining the highest number of points nor the one with the lowest evaluated price will necessarily be accepted.

3. The evaluated price per point of a responsive bid will be determined by dividing its evaluated price by the overall score it obtained for all the point rated technical criteria detailed in Attachment 1 to Part 4.

4. The responsive bid with the lowest evaluated price per point will be recommended for award of a contract. In the event two or more responsive bids have the same lowest evaluated price per point, the responsive bid that obtained the highest overall score for all point rated technical criteria, detailed in Attachment 1 to Part 4, will be recommended for award of a contract.

ATTACHMENT 1 to PART 4
TECHNICAL CRITERIA

1.1.1 Mandatory Technical Criteria

The bid must meet the mandatory technical criteria specified below. The Bidder must provide the necessary documentation to support compliance with this requirement.

Bids which fail to meet the mandatory technical criteria will be declared non-responsive. Each mandatory technical criterion should be addressed separately.

Mandatory Technical Criteria (MT)

For the purpose of the mandatory technical criteria the experience of the Bidder will be considered.

Number	Mandatory Technical Criterion	Bid Preparation Instructions
MT1	At bid closing, the Bidder must have possessed the following certifications for at least four (4) years: •Qualified Security Assessor (QSA) certification, qualified by the PCI Security Standards Council to ensure employees assess compliance to the PCI DSS Standard; **AND** •Approved Scanning Vendor (ASV) certification, qualified by the PCI Security Standards Council to ensure employees perform vulnerability scans of Internet facing environments of merchants and service providers.	The Bidder should include copies of these certifications with their bid.
MT2	At bid closing, the Bidder must have acquired, within the last 5 years, experience in providing resources, to clients exterior to the Bidder's own organization, that have experience in conducting: •PCI advisory related activities, as defined in the Statement of Work, in the area of policy/procedure, risks, information security, PCI audits, compensating controls and strategies for fraud prevention.	The Bidder must include their company's history and demonstrate relevant experience by submitting the following for each project of similar quality/quantity: •The name and a brief description of the project and for whom; and •The duration of the project including start and end dates. (must be chronologically indicated in years/months, e.g. May 2009 to March 2010)

MT3	The Bidder must propose a Senior PCI Advisor who meets the following: At bid closing, the proposed Senior PCI Advisor must have completed a bachelor's degree in the field of Finance, Accounting, Administration, Information Technology, Security or equivalent and must have acquired five (5) years of full-time professional work experience, within the last 10 years, conducting PCI Analysis related activities, as defined in the Statement of Work, in at least four (4) of the following areas: •Policy/procedure, •Risk, •Information Security, •PCI audits, •Compensating Controls, or •Strategies for fraud prevention. **OR** The proposed Senior PCI Advisor must have acquired seven (7) years of full-time professional work experience, within the last 10 years, conducting PCI Analysis related activities, as defined in the Statement of Work, in at least four (4) of the following areas: •Policy/procedure, •Risk, •Information Security, •PCI Audits •Compensating Controls, or •Strategies for fraud prevention. **Experience:** For the purpose of resource qualifications, experience gained during formal education will not be considered work experience. All requirements for work experience must be obtained in a work environment as opposed to an educational setting. Co-op terms are considered work experience provided that they are related to the required services. Listing	The Bidder must provide the name of the proposed resource, including: •Relevant work/project experience; •Language capabilities; and •Relevant academic attainments of the proposed resource in relation to the requirements. The Bidder must demonstrate the experience of the Senior PCI Advisor by submitting information including the following for each relevant acquired experience. •The name and a brief description of the project and for whom; •The duration of the project including start and end dates. (must be chronologically indicated in years/months, e.g. May 2005 to March 2006) •How the Senior PCI Advisor meets the educational requirement listed; and •Where and when the proposed candidate acquired education.

	experience without providing any supporting information describing where, when and how such experience was obtained will result in the experience not being included for evaluation purposes. **For evaluation purposes:** •Where means the name of the employer as well as the position/title held by the individual; •When means the start date and end date (e.g. from January 2008 to March 2009) of the period during which the individual acquired the qualification/experience; and •How means a clear description of the activities performed and the responsibilities assigned to the individual under this position and during this period. Furthermore, Bidders are advised that the month(s) of experience listed for a project in which the time frame overlaps that of another referenced project for the same named Resource must only be counted once. For example: Project #1 time frame is July 2008 to December 2008; Project #2 time frame is October 2008 to January 2009; the total months of experience for these two project references is seven (7) months.	
MT4	The Bidder must propose two (2) PCI Advisors who meet the following: At bid closing, the proposed PCI Advisors must have completed a bachelor's degree in the field of Accounting, Commerce, Business Administration, Information Technology, Security or equivalent and must have acquired five (5) years of full-time professional work experience, within the last 10 years, conducting PCI related activities, as defined in the Statement of Work, in the at least two (2) of the following: •Risks; •PCI audits; •Compensating controls; or	The Bidder must provide the name of the proposed resources including: •Relevant work/project experience; •Language capabilities; and •Relevant academic attainments of the proposed resource in relation to the requirements. The Bidder must demonstrate the experience of the PCI Advisors by submitting information including the following for each relevant acquired project experience: •The name and a brief description of the project and for whom; and

	•Financial analysis,. **OR** The proposed PCI Advisors must have acquired seven (7) years of full-time professional work experience, within the last 10 years, conducting PCI related activities, as defined in the Statement of Work, in the at least two (2) of the following: •Risks; •PCI Audits; •Compensating controls; or •Financial analysis. **Experience:** For the purpose of resource qualifications, experience gained during formal education will not be considered work experience. All requirements for work experience must be obtained in a work environment as opposed to an educational setting. Co-op terms are considered work experience provided that they are related to the required services. Listing experience without providing any supporting information describing where, when and how such experience was obtained will result in the experience not being included for evaluation purposes. **For evaluation purposes:** •Where means the name of the employer as well as the position/title held by the individual; •When means the start date and end date (e.g. from January 2008 to March 2009) of the period during which the individual acquired the qualification/experience; and •How means a clear description of the activities performed and the responsibilities assigned to the individual under this position and during this period. Furthermore, Bidders are advised that the month(s) of experience listed for a project in which the time frame overlaps that of another	•The duration of the project including start and end dates. (must be chronologically indicated in years/months, e.g. May 2008 to March 2009). The Bidder must include the following: •How the PCI Advisors meet the educational requirements listed; and •Where and when the proposed candidate acquired education.

	referenced project for the same named Resource must only be counted once. For example: Project #1 time frame is July 2008 to December 2008; Project #2 time frame is October 2008 to January 2009; the total months of experience for these two project references is seven (7) months.	

1.1.2 Point Rated Technical Criteria

Bids which meet all the mandatory technical criteria will be evaluated and scored as specified in the tables inserted below

Bids which fail to obtain the required minimum number of points specified will be declared non-responsive. Each point rated technical criterion should be addressed separately.

Point Rated Technical Criteria (RT) and Scores		**Required Minimum Number of Points (70%)**	**Maximum Number of Points**
RT1	Experience and Qualification	210	300
RT2	Understanding of Government Business and Technical Environment	252	360
Overall Score		462	660

Point Rated Technical Criteria (RT) Rating Scheme	
The rating scheme 0 to 10 will be assigned to the Bidder's response as detailed below.	
Rating	**Description**
0 = 0%	Unsatisfactory response, rated area not addressed, bid response does not meet the rated area.
3 = 30%	Unsatisfactory response, rated area is partially addressed but bidder's response does not meet the rated area.
5 = 50%	Rated area is partially addressed and response meet the rated area.
7 = 70%	Rated area is satisfactorily addressed, bidder's response meets the rated area
10 = 100%	Superior response, rated area is dealt with in-depth, bidder's response more than satisfies the rated area.

Point Rated Technical Criteria (RT)

For the purpose of the point rated technical criteria specified below the experience of the Bidder will be considered.

Number	Point Rated Technical Criterion	Bid Preparation Instructions	Weighting (Points)
RT1	Experience and Qualification: PCI Services and Solutions		Total 300 Points See rating scheme table above.
RT1.1	The Bidder should demonstrate that the Senior PCI Advisor has obtained its experience from past projects in the areas identified under RT1.1. •Providing analyses and strategic advice on PCI DSS requirements; •Developing and implementing a strategy of Fraud Prevention; •Training, support and knowledge transfer; and •Developing and implementing PCI policy/procedures.		Total 200 Points 50 points 50 points 50 points 50 points
RT1.2	The Bidder should provide: a) the description; and b) size of one (1) industry with which the Bidder has performed PCI remediation and assurance services within the last three (3) years. Only one (1) project will be evaluated. a**) Description:** •Public Sector organization; •Multi jurisdictional; •Complexity of IT and integrated sites; •Multiple lines of business b) **Size measured by number of workstations:** •Over 1,000 workstations **Between:** •500 and 999 workstations •401 and 500 workstations	The Bidder should provide a reference name, address, current telephone and facsimile number and/or an e-mail identification for the one (1) project cited.	Total 100 Points Maximum 50 Points 11 Points 13 Points 13 Points 13 Points Maximum 50 Points 50 Points 35 Points 25 Points

	• 301 and 400 workstations • 201 and 300 workstations • 101 and 200 workstations • 1 and 100 workstations		20 Points 15 Points 10 Points 5 Points
RT2	Understanding of Government Business, Technical Environment and Approach.		Total 360 Points See rating scheme table above.
RT2.1	The Bidder should explain the rationale of their approach in providing the PCI service. This should include the following: • Understanding of the Government diverse line of business; • Understanding of the Government technical and financial architecture; • Identifying relevant information security measures and internal control over financial reporting; and • Tailoring PCI DSS assessments to the Government business process, including appropriate application of compensating controls.	The Bidder should provide their understanding of government business, the diverse technical environment, the potential problem areas and their ability to address each situation identified under RT2.1.	Maximum 200 Points 50 Points 50 Points 50 Points 50 Points
RT2.2	The Bidder should demonstrate their understanding of the requirements by providing a Risk Management Plan that addresses the following: • Identifying relevant constraints; • Identifying foreseeable relevant risks; • Providing relevant consequences and probabilities of the risks identified above; and • Proposing relevant risk mitigation strategies for the risks identified above.	The Bidder should provide a Risk Management Plan that addresses each item identified under RT2.2.	Maximum 160 Points • 5 constraints: 8 points per each constraint, maximum 40 points • 5 risks: 8 points per each risk, maximum 40 points • 5 consequences: 6 points each, and 5 probabilities: 2 points each (maximum 40 points) • 5 strategies: 8 points per each strategy (maximum 40 points)

PART 5 - CERTIFICATIONS

Bidders must provide the required certifications to be awarded a contract. Canada will declare a bid non-responsive if the required certifications are not completed and submitted as requested. Bidders should provide the required certifications in Section III of their bid.

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

1. Certifications Precedent to Contract Award

The certifications included in Attachment 1 to Part 5, Certifications Precedent to Contract Award, should be completed and submitted with the bid, but may be submitted afterwards. If any of these required certifications is not completed and submitted as requested, the Contracting Authority will so inform the Bidder and provide the Bidder with a time frame within which to meet the requirement. Failure to comply with the request of the Contracting Authority and meet the requirement within that time period will render the bid non-responsive.

ATTACHMENT 1 to PART 5
CERTIFICATIONS PRECEDENT TO CONTRACT AWARD

1.1 Federal Contractors Program

1.1.1 Federal Contractors Program - $200,000 or more

1. The Federal Contractors Program (FCP) requires that some suppliers, including a supplier who is a member of a joint venture, bidding for federal government contracts, valued at $200,000 or more (including all applicable taxes), make a formal commitment to implement employment equity. This is a condition precedent to contract award. If the Bidder is subject to the FCP or, if the Bidder is a joint venture and if any of the members of the joint venture is subject to the FCP, evidence of the commitment made by the Bidder or by each member of the joint venture who is subject to the FCP must be provided by the Bidder before the award of any contract resulting from the bid solicitation.

   Suppliers who have been declared ineligible contractors by Human Resources and Skills Development Canada (HRSDC) are no longer eligible to receive government contracts over the threshold for solicitation of bids as set out in the *Government Contracts Regulations*. Suppliers may be declared ineligible contractors either, as a result of a finding of non-compliance by HRSDC, or, following their voluntary withdrawal from the FCP for a reason other than the reduction of their workforce to less than 100 employees. Any bids from ineligible contractors, including a bid from a joint venture that has a member who is an ineligible contractor, will be declared non-responsive.

2. The Bidder or, if the Bidder is a joint venture, any of the members of the joint venture who does not fall within the exceptions enumerated in 3.a or b below or does not have a valid certificate number confirming its adherence to the FCP must fax (819-953- 8768) a copy of the signed form LAB 1168, Certificate of Commitment to Implement Employment Equity, to the Labour Branch of HRSDC.

3. The Bidder or, if the Bidder is a joint venture, the member of the joint venture certifies its status with the FCP, as follows:

   The Bidder or the member of the joint venture

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

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

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

d. ( ) is subject to the FCP, has not been declared an ineligible contractor by HRSDC, and has a valid certificate number as follows: _____ .

Further information on the FCP is available on the HRSDC Web site.

1.2 Former Public Servants Certification

Contracts with former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny and reflect fairness in spending public funds. In order to comply with Treasury Board policies and directives on contracts with FPS, bidders must provide the information required below.

Definitions

For the purposes of this clause,

"former public servant" is any former member of a department as defined in the *Financial Administration Act, R.S. , 1985, c. F-11*, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

a) an individual;
b) an individual who has incorporated;
c) a partnership made of former public servants; or
d) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means, in the context of the fee abatement formula, a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act,* R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act*, 1970, c. D-3, the *Royal Canadian Mounted Police Pension Continuation Act* , 1970, c. R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c. R-11, the *Members of Parliament Retiring Allowances Act* , R.S., 1985, c. M-5, and that portion of pension payable to the *Canada Pension Plan Act*, R.S., 1985, c. C-8.

Former Public Servant in Receipt of a Pension

Is the Bidder a FPS in receipt of a pension as defined above ? **YES ( ) NO ( )**

If so, the Bidder must provide the following information:

a) name of former public servant; and
b) date of termination of employment or retirement from the Public Service.

Work Force Reduction Program

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of a work force reduction program? **YES ( ) NO ( )**

If so, the Bidder must provide the following information:

a) name of former public servant;
b) conditions of the lump sum payment incentive;
c) date of termination of employment;
d) amount of lump sum payment;
e) rate of pay on which lump sum payment is based;
f) period of lump sum payment including start date, end date and number of weeks; and
g) number and amount (professional fees) of other contracts subject to the restrictions of a work force reduction program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Goods and Services Tax or Harmonized Sales Tax.

Certification

By submitting a bid, the Bidder certifies that the information submitted by the Bidder in response to the above requirements is accurate and complete.

1.3 Status and Availability of Resources

The Bidder certifies that, should it be awarded a contract as a result of the bid solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the bid solicitation or agreed to with Canada's representatives. If for reasons beyond its control, the Bidder is unable to provide the services of an individual named in its bid, the Bidder may propose a substitute with similar qualifications and experience. The Bidder must advise the Contracting Authority of the reason for the substitution and provide the name, qualifications and experience of the proposed replacement. For the purposes of this clause, only the following reasons will be considered as beyond the control of the Bidder: death, sickness, maternity and parental leave, retirement, resignation, dismissal for cause or termination of an agreement for default.

If the Bidder has proposed any individual who is not an employee of the Bidder, the Bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Bidder and of his/her availability.

1.4 Education and Experience

The Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.

PART 6 - SECURITY REQUIREMENTS

1. Security Requirement

Before award of a contract, the following conditions must be met:

(a) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

(b) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirement as indicated in Part 7 - Resulting Contract Clauses; and

(c) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites.

2. Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

3. For additional information on security requirements, bidders should consult the “Security Requirements for PWGSC Bid Solicitations - Instructions for Bidders” (http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-eng.html#a31) document on the Departmental Standard Procurement Documents Website.

PART 7 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

1. Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work in Annex A.

1.1 Destination of Services

Public Works and Government Services Canada
Accounting, Banking and Compensation Branch
Banking Arrangements Directorate
Place du Portage, Phase III, 15A2
11 Laurier Street, Gatineau, Quebec - K1A 0S5

1.2 Task Authorization

1.2.1 Work described at Annex A, Statement of Work, will be performed under the Contract on an "as and when requested basis".

1.2.2 With respect to the Work mentioned under paragraph 1.2.1 of this clause,

1.2.2a) an obligation will come into force only when the Contractor receives a Task Authorization (TA), inclusive of any revisions, authorized and issued in accordance with this clause, and only to the extent designated in the authorized TA;

1.2.2b) the TA Authority and limit will be determined in accordance with paragraph 1.2.3 of this clause;

1.2.2c) the Contractor must not commence work until a TA, inclusive of any revisions, has been authorized and issued in accordance with the Contract. The Contractor acknowledges that work performed before a TA, inclusive of any revisions, has been authorized and issued in accordance with the Contract will be done at the Contractor's own risk and expense;

1.2.2d) the task description, inclusive of any revisions, included in an authorized TA must fall within the scope of the Statement of Work, in Annex A; and

1.2.2e) the TA, inclusive of any revisions, will be authorized under the Contract through the use of Annex D, Task Authorization Form. An authorized TA is a completed Annex D signed by the TA Authority.

1.2.3 TA Authority and Limit

1.2.3.1 The Project Authority may authorize individual TAs, inclusive of any revisions, the sole applicable Contract basis of payment of which is Limitation of Expenditure up to a limit of $75,000.00, GST or HST extra. Any TA the total value of which would exceed that limit or any revision to a previously authorized TA that would increase the TA total value above that limit, or any revision to a previously authorized TA the applicable Contract basis of payment of which is firm lot price must be authorized by the Contracting Authority before issuance to the Contractor.

1.2.3.2 The authority specified under paragraph 1.2.3.1 of this clause is granted subject to the sum specified in the Contract under clause 6.2 Limitation of Expenditure - Cumulative Total of all authorized TAs, not being exceeded.

1.2.4. TA Process

1.2.4.1 For each task or revision of a previously authorized task, the Project Authority will provide the Contractor with a request to perform a task prepared using Annex D Task Authorization Form, containing as a minimum:

1. the task or revised task description of the Work required, including:

   i. the details of the activities or revised activities to be performed;
   ii. a description of the deliverables or revised deliverables to be submitted; and
   iii. a schedule or revised schedule indicating completion dates for the major activities or submission dates for the deliverables, or both, as applicable;

2. the Contract security requirements applicable to the task or revised task;

3. the Contract basis (bases) of payment applicable to the task or revised task*;* and

4. the Contract method(s) of payment applicable to the task or revised task and, as applicable, the associated schedule of milestones.

1.2.4.2 Within five (5) calendar days of its receipt of the request, the Contractor must provide the Project Authority with a signed and dated response prepared and submitted using the TA form received from the Project Authority, containing as a minimum:

1. the total estimated cost proposed for performing the task or, as applicable, revised task;
2. a breakdown of that cost in accordance with Annex B, to be provided, as applicable, per milestone contained in the Schedule of Milestones ; and
3. for each resource proposed by the Contractor for the performance of the Work required:
   i. the name of the proposed resource; and
   ii. a demonstration that the proposed resource meets:
      a. the Contract security requirements (1.2.4.1.2 above); and
      b. Contractor Resource Requirements, SOW 4.0.

1.2.4.3 TA Authorization

1.2.4.3.1 The TA Authority will authorize the TA based on:

1. the request submitted to the Contractor pursuant to paragraph 1.2.4.1 above;
2. the Contractor's response received, submitted pursuant to paragraph 1.2.4.2 above; and
3. the agreed total estimated cost for performing the task or, as applicable, revised task and the breakdown of that cost per milestone contained in the Schedule of Milestones.

1.2.4.3.2 The TA Authority will authorize the TA provided each resource proposed by the Contractor for the performance of the Work required meets all the requirements specified under paragraph 1.2.4.2.3 above.

1.2.4.4 The authorized TA will be issued to the Contractor by email (as an email attachment in PDF format).

1.2.5 Minimum Work Guarantee - All the Work - Authorized TAs

1.2.5.1

- "Maximum Contract Value" means the sum specified in Contract clause 6.2 Limitation of Expenditure - Cumulative Total of All Authorized TAs; and
- "Minimum Contract Value" means 1% of the Maximum Contract Value.

1.2.5.2 Canada's obligation under the Contract is to request Work in the amount of the Minimum Contract Value or, at Canada's option, to pay the Contractor at the end of the Contract in accordance with paragraph 1.2.5.3 of this clause. In consideration of such obligation, the Contractor agrees to stand in readiness throughout the Contract period to perform the Work. Canada's maximum liability for Work requested in authorized TAs, performed by the Contractor and accepted by Canada must not exceed the Maximum Contract Value, unless an increase is authorized in writing by the Contracting Authority.

1.2.5.3 In the event that Canada does not request Work in the amount of the Minimum Contract Value during the period of the Contract, Canada must pay the Contractor the difference between the Minimum Contract Value and the cost of the Work requested in authorized TAs, performed by the Contractor and accepted by Canada.

1.2.5.4 Canada will have no obligation to the Contractor under this clause if Canada terminates the Contract in whole or in part for default.

1.2.6 Periodic Usage Reports - Contracts with TAs

1.2.6.1 The Contractor must compile and maintain detailed and current data on its performance of Work required and requested under TAs (inclusive of any revisions) authorized and issued under the Contract.

1.2.6.2 No later than 15 calendar days after the end of each of the reporting periods below, the Contractor must submit to the Contracting Authority and Project Authority a periodic usage report containing, in an electronic spreadsheet (such as MSOffice Excel), the data elements specified in paragraphs 1.2.6.3 and 1.2.6.4 below in the order they are presented. Where at the end of a reporting period, no changes are required to be made to the data contained in the periodic usage report submitted for the previous period, the Contractor must submit a "NIL" report to the Contracting Authority and Project Authority.

The reporting periods are defined as follows:

1st quarter: April 1 to June 30;
2nd quarter: July 1 to September 30;
3rd quarter: October 1 to December 31; and
4th quarter: January 1 to March 31.

1.2.6.3 For each TA authorized and issued under the Contract, the data must contain the following data elements in the order presented:

- the TA number appearing on the TA form;
- the date the task was authorized appearing on the TA form;
- the total estimated cost of the task (GST/HSTextra) before any revisions appearing on the TA form;
- the following information appearing on the TA form must be included for each authorized revision, starting with revision 1, than 2, etc.:
  - the TA revision number;
  - the date the revision to the task was authorized;
  - the authorized increase or decrease (GST/HSTextra);
  - the total estimated cost of the task (GST/HST extra) after authorization of the revision;
- the total cost incurred for the task (as last revised, as applicable), GST/HST extra;
- the total cost incurred and invoiced for the task (as last revised, as applicable), GST/HST extra;
- the GST/HST total amount invoiced;
- the total amount paid, GST/HST included;
- the start and completion date of the task (as last revised, as applicable); and
- the active status (i.e., the percentage of the work completed) of the task (as last revised, as applicable) with an explanation (as applicable).

1.2.6.4 For all TAs authorized and issued under the Contract, the data must contain the following data elements in the order presented:

- the sum (GST/HSTextra) specified in clause 6.2 Limitation of Expenditure - Cumulative Total of all Authorized TAs of the Contract (as last amended, if applicable.);
- the total cost incurred for all authorized tasks inclusive of any revisions, GST/HST extra;
- the total cost incurred and invoiced for all authorized tasks inclusive of any revisions, GST/HST extra;
- the GST/HST total amount invoiced for all authorized tasks inclusive of any revisions; and
- the total amount paid for all authorized tasks inclusive of any revisions, GST/HST extra.

2. Standard Clauses and Conditions

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

2.1 General Conditions

2035 (2011-05-16), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

2.2 Supplemental General Conditions

4008 (2008-12-12), apply to and form part of the Contract.

3. Security Requirement

1. The Contractor must, at all times during the performance of the Contract, hold a valid Facility Security Clearance at the level of SECRET, with approved Document Safeguarding at the level of Protected B, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).

2. The Contractor personnel requiring access to CLASSIFIED information, assets or sensitive work site(s) must EACH hold a valid personnel security screening at the level of SECRET, granted or approved by the CISD, PWGSC.

3. The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store any sensitive CLASSIFIED information until CISD/PWGSC has issued written approval. After approval has been granted, these tasks may be performed at the level of Protected B.

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

5. The Contractor must comply with the provisions of the:

(a) Security Requirements Check List and security guide (if applicable), attached at Annex C;
(b) Industrial Security Manual (Latest Edition).

4. Term of Contract

4.1 Period of the Contract

The period of the Contract will be two (2) years commencing from date of contract.

4.2 Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to two (2) additional one (1) year period(s) under the same conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least thirty (30) calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

5. Authorities

5.1 Contracting Authority

The Contracting Authority for the Contract is:

Ingrid Harrington, Supply Specialist
Public Works and Government Services Canada
Acquisitions Branch
Business Management and Consulting Services Division

Place du Portage, Phase III, 10C1
11 Laurier Street, Gatineau, Quebec - K1A 0S5
Telephone: 819-956-3201
Facsimile: 819-956-2675
E-mail address: ingrid.harrington@tpsgc-pwgsc.gc.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

5.2 Project Authority

The Project Authority for the Contract is:

To be determined at Contract Award.

The Project Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Project Authority; however, the Project Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

5.3 Contractor's Representative

To be determined at Contract Award.

6. Payment

6.1 Basis of Payment

a) Firm Lot Price TA

When the applicable basis of payment specified in a TA authorized and issued under the Contract is firm lot price, in consideration of the Contractor satisfactorily completing all of its obligations under the authorized TA, the Contractor will be paid the firm lot price stipulated in the authorized TA, as determined in accordance with the basis of payment cost elements in Annex B. Customs duties are included and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work specified in the authorized TA, unless they have been authorized, in writing, by the Contracting Authority before their incorporation into the Work specified in the authorized TA.

b) TA subject to a Limitation of Expenditure

When the basis of payment specified in a TA authorized and issued under the Contract is limitation of expenditure, the Contractor will be reimbursed for the costs reasonably and properly incurred in the performance of the Work specified in the authorized TA, as determined in accordance with the basis of payment cost elements, in Annex B, to the limitation of expenditure specified in the authorized TA.

Canada's total liability to the Contractor under the authorized TA must not exceed the limitation of expenditure specified in the authorized TA. Customs duties are included and Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

No increase in the liability of Canada or in the price of the Work specified in the authorized TA resulting from any design changes, modifications or interpretations of the Work specified in the authorized TA will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been authorized, in writing, by the TA Authority before their incorporation into the Work specified in the authorized TA. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written authorization of the TA Authority. The Contractor must notify the TA Authority in writing as to the adequacy of this sum:

(a) when it is 75 percent committed, or

(b) four (4) months before the final delivery date specified in the authorized TA, or

(c) as soon as the Contractor considers that the authorized TA funds are inadequate for the completion of the Work specified in the authorized TA,

whichever comes first.

If the notification is for inadequate authorized TA funds, the Contractor must provide to the TA Authority, a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

6.2 Canada's Total Liability - Limitation of Expenditure - Cumulative Total of all Authorized TAs

1. Canada's total liability to the Contractor under the Contract for all authorized TAs, inclusive of any revisions, must not exceed the sum of $ _____. *(insert amount at contract award)* Customs duties are included, and the Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.

2. No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.

3. The Contractor must notify the Contracting Authority, in writing, as to the adequacy of this sum:

(a) when it is 75 percent committed, or

(b) four (4) months before the Contract expiry date, or

(c) as soon as the Contractor considers that the sum is inadequate for the completion of the Work required and requested in all authorized TAs, inclusive of any revisions.

whichever comes first.

4. If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

6.3 Method of Payment

6.3.1 Methods of Payment - Authorized TA

One, several or all of the following methods of payment will form part of the authorized TA:

For the Work specified in an authorized firm lot price TA:

1) Single Payment

Canada will pay the Contractor upon completion and delivery of the Work in accordance with the payment provisions of the Contract if:

a) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

b) all such documents have been verified by Canada;

c) the Work delivered has been accepted by Canada.

OR

2) Milestone Payments

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Contract and the payment provisions of the Contract if:

a) an accurate and completed claim for payment using PWGSC-TPSGC 1111, Claim for Progress Payment, and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

b) all the certificates appearing on form PWGSC-TPSGC 1111 have been signed by the respective authorized representatives;

c) all work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada.

For the Work specified in an authorized TA subject to a Limitation of Expenditure:

1) Single Payment

Canada will pay the Contractor upon completion and delivery of the Work in accordance with the payment provisions of the Contract if:

a) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

b) all such documents have been verified by Canada;

c) the Work delivered has been accepted by Canada.

OR

2) Monthly Payment

Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

a) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

b) all such documents have been verified by Canada;

c) the Work performed has been accepted by Canada.

6.4 SACC Manual Clauses

A9117C (2007-11-30), T1204 - Direct Request by Customer Department
C2000C (2007-11-30), Taxes - Foreign-based Contractor
C0305C (2008-05-12), Cost Submission
C0705C (2010-01-11), Discretionary Audit

7. Invoicing Instructions

7.1 Invoicing Instructions

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

Each invoice must be supported by:
(a) a copy of time sheets to support the time claimed;
(b) a copy of the release document and any other documents as specified in the Contract;
(c) a copy of the invoices, receipts, vouchers for all direct expenses, and all travel and living expenses;
(d) a copy of the monthly progress report.

2. Invoices must be distributed as follows:

(a) The original and one (1) copy must be forwarded to the Project Authority identified under the section entitled "Authorities" of the Contract for appropriate certification after inspection and acceptance of the Work takes place

(b) One (1) copy must be forwarded to the Contracting Authority identified under the section entitled "Authorities" of the Contract.

(c) one (1) copy must be forwarded to the consignee.

7.2 Invoicing Instructions - Progress Payment Claim

1. In the case of a progress payment, the Contractor must submit a claim for payment using form PWGSC-TPSGC 1111, Claim for progress payment.

Each claim must show:

(a) all information required on form PWGSC-TPSGC 1111;
(b) all applicable information detailed under the section entitled "Invoice Submission" of the general conditions;
(c) a list of all expenses;

Each claim must be supported by:

(a) a copy of the invoices, receipts, vouchers for all direct expenses, travel and living expenses;
(b) a copy of the monthly progress report.

2. The Goods and Services Tax or Harmonized Sales Tax (GST/HST), as applicable, must be calculated on the total amount of the claim before the holdback is applied. At the time the holdback is claimed, there will be no GST/HST payable as it was claimed and payable under the previous claims for progress payments.

3. The Contractor must prepare and certify one original and two (2) copies of the claim on form PWGSC-TPSGC 1111, and forward it to the Project Authority identified under the section entitled "Authorities" of the Contract for appropriate certification after inspection and acceptance of the Work takes place.

The Project Authority will then forward the original and two (2) copies of the claim to the Contracting Authority for certification and onward submission to the Payment Office for the remaining certification and payment action.

4. The Contractor must not submit claims until all work identified in the claim is completed.

8. Certifications

8.1 Compliance with the certifications provided by the Contractor in its bid is a condition of the Contract and subject to verification by Canada during the term of the Contract. If the Contractor does not comply with any certification or it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

9. Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in _____.

10. Priority of Documents

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

(a) the Articles of Agreement;
(b) the supplemental general conditions;
(c) the general conditions 2035 (2011-05-16), General Conditions - Higher Complexity - Services;
(d) Annex A, Statement of Work;
(e) Annex B, Basis of Payment;
(f) Annex C, Security Requirements Check List;
(g) the signed Task Authorizations (including all of its annexes, if any); and
(i) the Contractor's bid dated _____ *(insert date of bid)*

11. SACC Manual Clause

A9122C (2008-05-12), Protection and Security of Data Stored in Databases

12. Foreign Nationals

12.1 SACC Manual clause A2001C (2006-06-16), Foreign Nationals (Foreign Contractor)

12.2 SACC Manual clause A2000C (2006-06-16), Foreign Nationals (Canadian Contractor)

13. Insurance

SACC Manual clause G1005C (2008-05-12), Insurance

14. Government Site Regulations

SACC Manual Clause A9068C (2010-01-11), Government Site Regulations

ANNEX “A”

STATEMENT OF WORK

PCI Advisor

PWGSC FILE NO. EN891-121307

1.0 Card Acceptance Overview

Public Works and Government Services Canada (PWGSC), on behalf of the Receiver General (RG) for Canada, is responsible for putting in place the infrastructure needed to collect revenues and to reconcile revenue received at the financial institutions with deposits made at the Bank of Canada, balancing accounting and banking records, and compensating participating financial services organizations for fees. PWGSC also provides daily deposit details to departments based on information received from financial service organizations.

As such, the RG, being responsible for the establishment and maintenance of all banking arrangements on behalf of federal organizations that operate within the Consolidated Revenue Fund, established the card acceptance services contract which enables federal organizations to accept credit and/or debit cards as forms of payment for federal goods and services. As part of this contract, Canada is bound to be compliant with the Payment Card Industry Data Security Standard (PCI DSS).

The departments and agencies that accept credit and/or debit cards as a form of payment are responsible for the programs under which the goods and services are produced and sold. They are also responsible for providing the services to purchasers and for accounting for the revenues and related expenditures in both their departmental financial systems and to the Accounts of Canada. Departments reconcile the transaction detail information to their internal records and to the deposit details provided to them by the RG.

Departments provide a variety of goods and services on a cost-recovery basis. Examples of goods and services currently sold in this fashion range from passport fees, Visas, campsites in national parks, to fuel, budget papers and radio licenses. The purchasers of the goods and services include the general public, companies, corporations and other levels of government. Some locations only accept sales in person, while others accept sales by telephone, mail, over the Internet, or through unstaffed stations. Some operations are available twenty-four hours a day, seven days a week or year-round; some are available only during normal office hours, and others are seasonal. The services offered by departments are changing for a number of reasons including customer demand, legislative requirements, and to improve efficiency.

The protection of customer account information from misuse or fraudulent activity is of utmost concern for the Government of Canada. A security violation on the government's database will have not only financial liabilities including steep fines, but will also result in the suspension and revocation of the privilege to accept credit cards. In addition, a breach of the public trust will have long term effects on the stewardship functions of the government.

Currently, 38 federal government departments and agencies accept credit and/or debit cards at different locations across Canada. Credit card payments for the period April 1, 2010 to March 31, 2011, were approximately $736 million. The PCI process currently consists of having departments complete and sign a self-assessment questionnaire (SAQ), perform a vulnerability scan on all Internet Protocol (IP) lines and sign an Attestation of Compliance or complete an action plan with a timeline towards compliancy. The RG is leading a PCI remediation and compliance management project to review and strengthen current security practices and controls regarding cardholder information.

2.0 Overview of the Requirement

The RG requires the advice and knowledge transfer of a contractor that has an in depth understanding of the PCI DSS best practices. While individual requirements will be specified in each Task Authorization (TA) the RG requires qualified resources to provide the following services on an as and when requested basis:

a) An in depth review of departmental business flows and security controls to provide PCI compliance audit readiness and ultimately, ensure each federal department is either fully PCI DSS compliant or has a clear timeline for compliancy

b) Ensure knowledge to oversee the PCI project is transferred to the RG PCI project office and governance body;

c) Provide guidance in the effective establishment and management of competitive contractual arrangements to obtain the services of:

a Qualified Security Assessor (QSA),
an Approved Scanning Vendor (ASV); and/or
the acquisition of PCI DSS tools.

3.0 Scope of Work

The Contractor must deliver PCI advisory services on an as and when requested basis, for all locations requested by the RG across Canada. Please refer to Appendix B for a summary of the current locations.

3.1 Achieving PCI DSS Compliancy:

The contractor must provide the following services on an as and when requested basis:

- Review individual departments' cardholder data flows;
- Provide PCI compliance audit readiness assessments in order to:
    - Identify the current degree of PCI compliance in the Government;
    - Identify gaps in the current Government PCI process;
    - Provide recommendations on options to closing compliance gaps;
    - Implement the necessary tools to be used for testing controls.
- Identify security measures and internal controls over financial reporting in each department;
- Tailor the PCI assessments available from the PCI Security Standards Council (SSC) to the individual departments' business processes including the appropriate application of compensating controls;
- Implement and develop PCI reports including gap closure plans in a pre-approved format, acceptable to both the Acquirer and the Card Brands;
- Design and implement a government PCI compliance and reporting program to assess overall risk to government and to monitor individual departmental compliance.
- Provide PCI compliance audit readiness assessments to identify the current degree of compliance for the in-scope projects/environments, nature of gaps, and recommendations. The PCI audit readiness assessments are to help identify gaps in the current PCI project and to identify the extent to which the project has enabled the government to achieve compliance, based on a priority risk based approach to PCI, and to provide recommendations on options the project team can consider for closing compliance gaps;
- Provide advisory and assurance services on PCI DSS issues to the Receiver General PCI project office and governance body;
- Provide guidance in communication with departments, acquirers and card brands;
- Draft a risk methodology to share with departments;
- Draft an audit program to share with departments.

3.2 Knowledge Transfer

The contractor must provide the following services on an as and when requested basis:

- Provide knowledge transfer to the RG PCI project office and governance body ensuring that the Project Authority (PA) is able to take control of the PCI project in a reasonable time frame. This includes:
    - Conducting individual meetings with departments;
    - Training the RG and departments on using compensation controls;
    - Coaching the RG towards managing the PCI DSS.
- Provide the PA with documentation of the PCI compliancy program designed and implemented across the government; and
- Upon request deliver presentations to the governance body and/or to departments' executives.

3.3 Further QSA and ASV Procurement Requirements

The contractor must provide the following services on an as and when requested basis:

- Provide guidance and assist in the development of a Statement of Work (SOW) and Evaluation Criteria to contract the services of:
    - a Qualified Security Assessor (QSA);
    - an Approved Scanning Vendor (ASV); and/or
    - the acquisition of PCI tools.
- This requires undertaking the following activities:
    - Advise and assist PWGSC on the formulation of questions to be asked and presentations to be made;
    - Advise and assist PWGSC on making changes that may be necessary to the SOW and related evaluation criteria; and
    - Provide assistance if requested, with the Request for Proposal (RFP) Questions and Answers.

4.0 Contractor Resources

The Contractor must provide the following resources to carry out the work as described in the SOW:

4.1 Senior PCI Advisor

The Contractor must provide one (1) Senior PCI advisor to carry out the work outlined at sections 3.1, 3.2, 3.3 and 4.1.1, and provide the deliverables to the satisfaction of the PA.

4.1.1 The Senior PCI Advisor must assist the PA and ensure the efficient and timely delivery of the required services and output, including but not limited to the following:

- Plan and organize the work to be carried out by the Contractor;
- Participate in scheduled progress meetings and other meetings with the PA and/or with delegated authorities;
- Provide regular and ad-hoc reports to the PA; and

- Provide an adequate level of quality control over all work and all deliverables; and
- Prepare and maintain work plans and schedules.

4.2 PCI Advisors

The Contractor must provide up to two (2) PCI Advisors to assist the Senior PCI Advisor in carrying out the work outlined herein on an as and when requested basis and provide the deliverables to the satisfaction of the PA.

5.0 Contractor Resource Requirements

The following table defines the minimum qualifications of each of the required Resource Categories.

Resource Category	Minimum Resource Qualifications
Senior PCI Advisor	The Senior PCI Advisor must have completed a bachelor's degree in the field of Finance, Accounting, Administration, Information Technology, Security or equivalent and must have acquired five (5) years of full-time professional work experience, within the last 10 years, conducting PCI Analysis related activities, as defined in the Statement of Work, in at least four (4) of the following areas: • Policy/procedure, • Risk, • Information Security, • PCI audits, • Compensating Controls, or • Strategies for fraud prevention. **OR** The Senior PCI Advisor must have acquired seven (7) years of full-time professional work experience, within the last 10 years, conducting PCI Analysis related activities, as defined in the Statement of Work, in at least four (4) of the following areas: • Policy/procedure, • Risk, • Information Security, • PCI Audits • Compensating Controls, or • Strategies for fraud prevention.

PCI Advisors	The PCI Advisors must have completed a bachelor's degree in the field of Accounting, Commerce, Business Administration, Information Technology, Security or equivalent and must have acquired five (5) years of full-time professional work experience, within the last 10 years, conducting PCI related activities, as defined in the Statement of Work, in the at least two (2) of the following: • Risks; • PCI audits; • Compensating controls; or • Financial analysis,. **OR** The PCI Advisors must have acquired seven (7) years of full-time professional work experience, within the last 10 years, conducting PCI related activities, as defined in the Statement of Work, in the at least two (2) of the following: • Risks; • PCI Audits; • Compensating controls; or • Financial analysis.

6.0 Deliverables

All written material must be provided in hard and/or soft copy as requested by the PA and prepared in accordance with the instructions provided by the PA. Unless otherwise specified, the soft copy must be provided in the current version of the RG PCI Project Office's approved desktop software (currently PC-based Microsoft Office).

In accordance with the activities defined in section 3.0 Scope of Work of this SOW and the specific requirements of any TA, deliverables under any resulting TA may include, but are not limited to:

- Descriptive of each department cardholder data workflow;
- Review of each department PCI compliancy;
- PCI compliance audit readiness assessments identifying the current state of compliance for each project/environment;
- Reports and recommendations including, but not limited to:
    - Progress Reports in electronic format, of the work performed, to the PA including:
        - A brief summary of progress, including explanations for any delays in reaching milestones or in producing deliverables;
        - A brief report on current issues; and
        - An updated assessment of risks.
    - Final Progress Report including:
        - a summary of the project activities;
        - an assessment of the overall performance and results achieved;
        - identify key lessons learned;
        - Gap closure plans;

- Documentation of the PCI compliancy program designed and implemented across the government; and
- Fit gap analysis of Government security policy and standards as compared to PCI DSS, if required.

7.0 General Requirements

7.1 Data Security and Integrity

The Contractor must provide “industry standard” levels of data security, integrity and availability, including complying with security and privacy requirements as may be specified from time-to-time by the financial services industry and by the card associations.

The Contractor’s systems operational, technical and management security procedures and measures must protect the integrity and proper functioning of those databases and systems critical to the operation of the card program. The databases and information processing systems containing government information must have security measures to protect against deliberate or inadvertent loss, degradation, alteration, or damage from unauthorized access resulting from accidents and natural hazards.

7.2 Information Technology Security Requirements IT Technical Document

The Contractor must ensure compliance with the Information Technology Security Requirements identified in the attachment to Annex C, SRCL.

7.3 Location of Work and Travel

Unless otherwise stated, the Contractor's work must take place primarily at the Contractor's premises. Certain meetings will be conducted in person at the Receiver General's headquarters in the National Capital Area (NCA) or at departments’ locations

The contractor will be informed, in writing, at least seven (7) days prior to any meeting. The Contractor is responsible for their own cost of travel to attend the meetings in the NCA

There may be occasional travel requirements for meetings at department locations outside the NCA: Refer to Appendix B for a list of locations. Those Travel Requirements will be identified and specified by the PA in the TA documents. The cost of travel outside the NCA, under a TA, is billable as per Treasury Board rates and is not to exceed Canada’s total liability for authorized travel and living expenses detailed in Annex B, Basis of Payment.

7.4 Language of Work

The Contractor must provide services in English, but at least one PCI Advisor resource must be able to provide services in both official languages of Canada. Deliverables and documentation such as rules, regulations and material, must be provided in English and when available, in French.

7.5 Contractor Responsibilities / Constraints

The Contractor must supply all of its own tools, facilities, equipment and software required for completion of the work, unless otherwise directed by the PA.

7.6 Reporting Requirements

- The Contractor must facilitate and maintain regular communication with the PA regarding the progress of the work completed under any resulting TA. Specific Contractor reporting requirements will be further identified by the PA , as required, within each TA;
- Upon request from the PA, the Contractor must provide ad hoc written or oral status updates relating to any work in progress under any TA; and
- The Contractor must immediately notify the PA of any issues, problems or areas of concern that could adversely affect the ability of the Contractor to complete the work specified under any TA.

Appendix A

Definitions

The following definitions are applicable to this SOW and may have different meanings in other contexts.

Accounts of Canada: the Receiver General is responsible for preparing the Public Accounts of Canada that include the annual audited financial statements of the Government of Canada.

Ad-Hoc Reports: as opposed to specific reporting, these are reports created when asked for.

Approved Scanning Vendor (ASV): an organization that has been approved by the PCI SSC for validating adherence to certain PCI DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers.

Audit Readiness Assessments: determine if the status of the merchant is ready for an audit by a regulatory body.

Card Associations: network of issuing banks and acquiring banks that process payment cards of a specific brand.

Customer account information: this might include credit card data, Social Insurance Numbers and other personal information collected from customers.

Departments: Government of Canada Departments, Agencies, Crown Corporations, Special Operating Agencies and various affiliated organizations that operate within the Consolidated Revenue Fund.

Departmental Coordinator (DC): a person designated by the department as the contact with the RG.

Industry Standard: rules and regulations imposed by the card associations on merchants accepting payments by credit cards.

Payment Card Industry Data Security Standard (PCI DSS): provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.

PCI QSA readiness assessments: An in-depth series of self-guided questionnaires for preparing the organization for compliance. It helps understand scope, deficiencies within the existing security infrastructure, and lays the groundwork for successful compliance with the PCI DSS framework. Readiness assessments are conducted off-site, thus minimizing disruption to departmental operations.

PCI Security Standards Council (SSC): is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards.

Project Authority (PA): The PA represents the department (PWGSC/RG), for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract.

Qualified Security Assessor (QSA): QSA companies are organizations that have been qualified by the PCI SSC to have their employees assess compliance to the PCI DSS standard. Qualified Security

Assessors are employees of these organizations who have been certified by the Council to validate an entity's adherence to the PCI DSS.

Receiver General PCI project office and governance body: will be responsible to oversee the PCI remediation and compliance management project in order to review and strengthen current security practices and controls regarding cardholder information.

Self-assessment questionnaire (SAQ): is a validation tool for merchants and service providers that are not required to undergo an on-site data security assessment. It assists organizations in self evaluating compliance with the PCI.

Task Authorization (TA): a document that provides authorization of services to be performed on an As-and-When-Requested Basis.

Appendix B

(see attached spreadsheet)

Appendix C

Current Set-Ups and Configurations

Number of Departments	38
Number of Physical Locations (approx.)	1492

A) **Setups**

Staffed/fixed basic POS workstations (i5310, vx510, vx570)	1824
Unstaffed POS workstations (Tender retail)	4
Wireless/mobile Terminals (mobile – NBS5600, i7780)	292
Touch Tone Capture (TTC - accessible by merchants)	160
Receiver General Buy Button	14
PC Software Licenses (SPW, SMFT – Web plug-in)	39
Internet Software Licenses (SWPP) (Will move to RGBB or may stay with 3rd party)	4
Total connections:	**2337**

Annex A, Appendix A

Definitions

The following definitions are applicable to this SOW and may have different meanings in other contexts.

Accounts of Canada: the Receiver General is responsible for preparing the Public Accounts of Canada that include the annual audited financial statements of the Government of Canada.

Ad-Hoc Reports: as opposed to specific reporting, these are reports created when asked for.

Approved Scanning Vendor (ASV): an organization that has been approved by the PCI SSC for validating adherence to certain PCI DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers.

Audit Readiness Assessments: determine if the status of the merchant is ready for an audit by a regulatory body.

Card Associations: network of issuing banks and acquiring banks that process payment cards of a specific brand.

Customer account information: this might include credit card data, Social Insurance Numbers and other personal information collected from customers.

Departments: Government of Canada Departments, Agencies, Crown Corporations, Special Operating Agencies and various affiliated organizations that operate within the Consolidated Revenue Fund.

Departmental Coordinator (DC): a person designated by the department as the contact with the RG.

Industry Standard: rules and regulations imposed by the card associations on merchants accepting payments by credit cards.

Payment Card Industry Data Security Standard (PCI DSS): provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.

PCI QSA readiness assessments: An in-depth series of self-guided questionnaires for preparing the organization for compliance. It helps understand scope, deficiencies within the existing security infrastructure, and lays the groundwork for successful compliance with the PCI DSS framework. Readiness assessments are conducted off-site, thus minimizing disruption to departmental operations.

PCI Security Standards Council (SSC): is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards.

Project Authority (PA): The PA represents the department (PWGSC/RG), for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract.

Qualified Security Assessor (QSA): QSA companies are organizations that have been qualified by the PCI SSC to have their employees assess compliance to the PCI DSS standard. Qualified Security Assessors are employees of these organizations who have been certified by the Council to validate an entity's adherence to the PCI DSS.

Annex A, Appendix A

Definitions

Receiver General PCI project office and governance body: will be responsible to oversee the PCI remediation and compliance management project in order to review and strengthen current security practices and controls regarding cardholder information.

Self-assessment questionnaire (SAQ): is a validation tool for merchants and service providers that are not required to undergo an on-site data security assessment. It assists organizations in self evaluating compliance with the PCI.

Task Authorization (TA): a document that provides authorization of services to be performed on an As-and-When-Requested Basis.

APPENDIX B

Department's locations

Dept #	Departments	Dept acronym	Head Quarters location	Number of locations
005	Foreign Affairs and International Trade	DFAIT / INTERNATIONAL	125 Sussex, Ottawa, ON, K1A 0G2	2
005	Passport Canada	PPTC	70 Cremazie, Gatineau, QC, K1A 0G3	42
006	Finance Canada	FINANCE	300 ave Laurier O, Ottawa, ON, K1A 0R5	1
007	Environment Canada	EC	70 Cremazie, Gatineau, QC, K1A 0H3	18
008	Governor General	GG	1, promenade Sussex, Ottawa, ON, K1A 0A1	1
011	Office of Superintendant of Financial Institutions	OSFI	255, Albert, Ottawa, ON, K1A 0H2	1
014	Human Resources & Skills Development Canada	HRSDC	140 promenade Portage, Gatineau, QC, K1A 0J9	479
015	Chief Electoral Office	ELECTIONS	257 rue Slater, Ottawa, ON, K1A 0M6	1
017	Library of Parliament	PARL	Édifices du Parlement, Ottawa, ON, K1A 0A9	1
018	National Defence	FORCES/ DND	25, rue Nicholas, Ottawa, ON, K1A 0K2	31
022	Health Canada	HC	2932, ch. Baseline, Ottawa, ON, K1A 0K9	2
030	Royal Canadian Mounted Police	RCMP	73 Leikin Drive, Ottawa, ON, K1A 0R2	3
033	Industry Canada	IC	300, Slater, Ottawa, ON, K1A 0C8	13
034	Transport Canada	TC	330 Sparks, Ottawa, ON, K1A 0N5	56
035	National Research Council of Canada	NRC	1200, ch de Montréal, Ottawa, ON, K1A 0R6	8
038	Canada Border Services Agency - Admin (Customs)	CBSA	219 av. Laurier O, Ottawa, ON, K1A 0L8	229
039	National Film Board	NFB	3155, ch de la Côte-de-Liesse, Montreal, QC, H4N 2N4	5
041	Natural Resources	NRCAN	615 Booth, Ottawa, ON, K1A 0E9	31
042	Indian Affairs and Northern Development	INAC / AADNC	10 Wellington, Gatineau, QC, K1A 0H4	2
047	Canadian Nuclear Safety Commission	CNSC	1601 Télésat Court, Ottawa, ON, K1P 5S9	1
050	Citizenship and Immigration	CIC	300 Slater, Ottawa, ON, K1A 1L1	42
052	Canada School of the Public Service	CSPS	425 boul. St-Joseph, Gatineau, QC, K1N 6Z2	1
053	Correctional Service	CSC	340 av. Laurier O, Ottawa, ON, K1A 0P9	2
054	Statistics Canada	STAT	100 promenade Tunney's Pasture, Ottawa, ON, K1A 0T6	2
056	Treasury Board Secretariat	TBS	300 ave Laurier O, Ottawa, ON, K1A 0R5	1
080	Supreme Court of Canada	SCC	301 Wellington, Ottawa, ON, K1A 0J1	1
086	Fisheries and Oceans	DFO	200 Kent, Ottawa, ON, K1A 0E6	36
100	Occupational Health and Safety	CCOHS	135 Hunter Est, Hamilton, ON, L8N 1M5	2
102	National Battlefields Commission	CCBC / NBC	390, Ave de Bernieres, Quebec, QC, G1R 2L7	5
108	Hazardous Materials Information Review Commission	HC / HMIRC	427, ave. Laurier Ouest, Ottawa, ON, K1A 1M3	1
122	Canada Revenue Agency - Tax	CRA	750 Heron, Ottawa, ON, K1A 0L5	51
124	Parks Canada Agency	PC	25 Eddy, Gatineau, QC, K1A 0M5	307
127	Public Works and Government Services Canada	PWGSC	11 Laurier, Gatineau, QC, K1A 0S5	20
133	Canadian Grain Commission	GRAINS	303 Main, Winnipeg, MB, R3C 3G8	6
135	Heritage Canada	PCH	15 Eddy, Gatineau, QC, K1A 0M5	2
136	Canadian Food Inspection Agency	INSPECTION / CFIA	33 Weldon, Moncton, NB, E1C 0N5	70
144	Courts Administration Service	CAS	90 Sparks, Ottawa, ON, K1A 0H9	12
145	Library and Archive Canada	LAC	395 Wellington, Ottawa, ON, K1A 0N4	4
		38		1492

Annex A, Appendix C

Current Set-Ups and Configurations

Number of Departments		38
Number of Physical Locations (approx.)		1492
A)	**Setups**	
	Staffed/fixed basic POS workstations (i5310, vx510, vx570)	1824
	Unstaffed POS workstations (Tender retail)	4
	Wireless/mobile Terminals (mobile – NBS5600, i7780)	292
	Touch Tone Capture (TTC - accessible by merchants)	160
	Receiver General Buy Button	14
	PC Software Licenses (SPW, SMFT – Web plug-in)	39
	Internet Software Licenses (SWPP) (Will move to RGBB or may stay with 3rd party)	4
	Total connections:	**2337**

ANNEX B
BASIS OF PAYMENT

A - The period of the Contract is two (2) years commencing from date of contract.

During the period of the Contract, for Work performed in accordance with the Contract, the Contractor will be paid as specified below.

1.0 Professional Fees

The Contractor will be paid all inclusive fixed time rates as follows:

	PERIOD	ALL-INCLUSIVE FIXED HOURLY RATE (in Cdn $)
Contract Period: Year 1 and Year 2		
1a	Senior PCI Advisor	$
1b	PCI Advisor	$

2.0 Cost Reimbursable Expenses

2.1 Authorized travel and living expenses for Work performed outside the National Capital Region (NCR) only.

For the requirements relative to travel described in section 7.2 of the Statement of Work in Annex A:

The Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and administrative overhead, in accordance with the meal, private vehicle and incidental expenses provided in Appendices B, C and D of the Treasury Board Travel Directive, and with the other provisions of the directive referring to "travelers", rather than those referring to "employees".

All travel must have the prior authorization of the Project Authority.

The authorized travel and living expenses will be paid upon submission of an itemized statement supported by receipt vouchers. All payments are subject to government audit.

Canada will not accept any travel and living expenses for:

a. Work performed within the National Capital Region (NCR). The NCR is defined in the National Capital Act, R.S.C. 1985, c. N-4, S.2. The National Capital Act is available on the Justice Website: http://laws.justice.gc.ca./en/N-4/ ;
b. Any travel between the Contractor's place of business and the NCR; and
c. Any relocation of resources required to satisfy the terms of the Contract.

3.0 Total Estimated Cost - Contract Period: $ _____.

ANNEX B
BASIS OF PAYMENT

B - Option to Extend the Term of the Contract

This section is only applicable if the option to extend the Contract is exercised by Canada.

During the extended periods of the Contract specified below, the Contractor will be paid as specified below to perform all the Work in relation to the Contract extensions.

B- 1.0 Extended Contract - Option Period 1 (additional one year period)

1.0 Professional Fees

The Contractor will be paid all inclusive fixed time rates as follows:

	PERIOD	ALL-INCLUSIVE FIXED HOURLY RATE (in Cdn $)
Option Period 1: Year 3		
2a	Senior PCI Advisor	$
2b	PCI Advisor	$

2.0 Cost Reimbursable Expenses

2.1 Authorized travel and living expenses for Work performed outside the National Capital Region (NCR) only.

For the requirements relative to travel described in section 7.2 of the Statement of Work in Annex A:

The Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and administrative overhead, in accordance with the meal, private vehicle and incidental expenses provided in Appendices B, C and D of the Treasury Board Travel Directive, and with the other provisions of the directive referring to "travelers", rather than those referring to "employees".

All travel must have the prior authorization of the Project Authority.

The authorized travel and living expenses will be paid upon submission of an itemized statement supported by receipt vouchers. All payments are subject to government audit.

Canada will not accept any travel and living expenses for:

a. Work performed within the National Capital Region (NCR). The NCR is defined in the National Capital Act, R.S.C. 1985, c. N-4, S.2. The National Capital Act is available on the Justice Website: http://laws.justice.gc.ca./en/N-4/ ;
b. Any travel between the Contractor's place of business and the NCR; and
c. Any relocation of resources required to satisfy the terms of the Contract.

3.0 Total Estimated Cost - Option Period 1: $ _____.

ANNEX B
BASIS OF PAYMENT

B- 2.0 Extended Contract - Option Period 2 (additional one year period)

1.0 Professional Fees

The Contractor will be paid all inclusive fixed time rates as follows:

	PERIOD	ALL-INCLUSIVE FIXED HOURLY RATE (in Cdn $)
Option Period 2: Year 4		
3a	Senior PCI Advisor	$
3b	PCI Advisor	$

2.0 Cost Reimbursable Expenses

2.1 Authorized travel and living expenses for Work performed outside the National Capital Region (NCR) only.

For the requirements relative to travel described in section 7.2 of the Statement of Work in Annex A:

The Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and administrative overhead, in accordance with the meal, private vehicle and incidental expenses provided in Appendices B, C and D of the Treasury Board Travel Directive, and with the other provisions of the directive referring to "travelers", rather than those referring to "employees".

All travel must have the prior authorization of the Project Authority.

The authorized travel and living expenses will be paid upon submission of an itemized statement supported by receipt vouchers. All payments are subject to government audit.

Canada will not accept any travel and living expenses for:

a. Work performed within the National Capital Region (NCR). The NCR is defined in the National Capital Act, R.S.C. 1985, c. N-4, S.2. The National Capital Act is available on the Justice Website: http://laws.justice.gc.ca./en/N-4/ ;
b. Any travel between the Contractor's place of business and the NCR; and
c. Any relocation of resources required to satisfy the terms of the Contract.

3.0 Total Estimated Cost - Option Period 2: $ _____.

Annex C

Security Requirements Check List (SRCL)

Liste de vérification des exigences relatives la sécurité (LVERS)

Government of Canada / Gouvernement du Canada

Revision2

Contract Number / Numéro du contrat
EN891 12 1307
Security Classification / Classification de sécurité UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Public Works and Government Services Canada

2. Branch or Directorate / Direction générale ou Direction: BAD / ABC

3. a) Subcontract Number / Numéro du contrat de sous-traitance

3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

To solicite the provision of advice and knowledge transfer of consultants who have knowledge of the Payment Card Industry (PCI) best practices to train the RG PCI project office to ensure the Gov is fully PCI compliant.

5. a) Will the supplier require access to Controlled Goods? / Le fournisseur aura-t-il accès à des marchandises contrôlées? — [✓] No / Non [ ] Yes / Oui

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

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

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? / Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) / (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) — [ ] No / Non [✓] Yes / Oui

6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. / Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. — [✓] No / Non [ ] Yes / Oui

6. c) Is this a commercial courier or delivery requirement with no overnight storage? / S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit? — [✓] No / Non [ ] Yes / Oui

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

Canada		NATO / OTAN		Foreign / Étranger	

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

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

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

Canada		NATO		Foreign / Étranger	
PROTECTED A / PROTÉGÉ A	[ ]	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	[ ]	PROTECTED A / PROTÉGÉ A	[ ]
PROTECTED B / PROTÉGÉ B	[✓]	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	[ ]	PROTECTED B / PROTÉGÉ B	[ ]
PROTECTED C / PROTÉGÉ C	[ ]	NATO CONFIDENTIAL / NATO CONFIDENTIEL	[ ]	PROTECTED C / PROTÉGÉ C	[ ]
CONFIDENTIAL / CONFIDENTIEL	[ ]	NATO SECRET / NATO SECRET	[ ]	CONFIDENTIAL / CONFIDENTIEL	[ ]
SECRET / SECRET	[ ]	COSMIC TOP SECRET / COSMIC TRÈS SECRET	[ ]	SECRET / SECRET	[ ]
TOP SECRET / TRÈS SECRET	[ ]			TOP SECRET / TRÈS SECRET	[ ]
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	[ ]			TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	[ ]

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
EN891 12 1307
Security Classification / Classification de sécurité UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

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

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☐ RELIABILITY STATUS COTE DE FIABILITÉ	☐ CONFIDENTIAL CONFIDENTIEL	☑ SECRET SECRET	☐ TOP SECRET TRÈS SECRET
☐ TOP SECRET– SIGINT TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL NATO CONFIDENTIEL	☐ NATO SECRET NATO SECRET	☐ COSMIC TOP SECRET COSMIC TRÈS SECRET
☐ SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

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

10. b) May unscreened personnel be used for portions of the work? — ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — ☑ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

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

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

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

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

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

Baseline Requirements: The Contractor must not utilize its Information Technology (IT) Systems to electronically process, produce or store protected or classified information or data until the Baseline Security Requirements, identified herein, are met and CISD has issued written approval.

Supplemental Requirements: The Supplemental Security Requirements, identified herein, must be met no later than six (6) months after receipt of written approval from CISD.

The Baseline and Supplemental Requirements require the Contractor to fill in blanks and/or to provide additional information with respect to the security requirement for the associated domain. This information will be required at the time of Inspection(s) and is not a prerequisite to obtaining approval.

1.1 Access Control (AC)

Following table lists the ITSR related to the AC domain for the PCI Advisor Service.

Table C-1: AC Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
AC- 1	ACCESS CONTROL POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	✓	
		• The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	✓	
AC- 2	ACCOUNT MANAGEMENT	• The contractor manages information system accounts, including identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary). • The contractor manages information system accounts, including establishing conditions for group membership. • The contractor manages information system accounts, including identifying authorized users of the information system and specifying access privileges. • The contractor manages information system accounts, including requiring appropriate approvals for requests to establish accounts. • The contractor manages information system accounts, including establishing, activating, modifying, disabling, and removing accounts. • The contractor manages information system accounts, including specifically authorizing and monitoring the use of	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		guest/anonymous and temporary accounts. • The contractor manages information system accounts, including notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes. • The contractor manages information system accounts, including deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users. • The contractor manages information system accounts, including granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by The contractor or associated missions/business functions. • The contractor manages information system accounts, including reviewing accounts Annually.		
		• The contractor employs automated mechanisms to support the management of information system accounts. • The information system automatically terminates temporary and emergency accounts after [time period] _____ for each type of account. • The information system automatically disables inactive accounts after [time period] _____.		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals. • The contractor : (a) Requires that system automatically logs out the users when 15 minutes of inactivity; (b) Determines normal time-of-day and duration usage for information system accounts; (c) Monitors for atypical usage of information system accounts; and (d) Reports atypical usage to designated organizational officials. • The contractor : (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and (b) Tracks and monitors privileged role assignments.		
AC- 3	ACCESS ENFORCEMENT	• The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	✓	
		• The information system enforces a Discretionary Access Control (DAC) policy that: (a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both; (b) Limits propagation of access rights; and (c) Includes or excludes access to the granularity of a single user.		✓
AC- 4	INFORMATION FLOW ENFORCEMENT	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	✓	
AC- 5	SEPARATION OF DUTIES	• The contractor separates duties of individuals as necessary, to prevent malevolent activity without collusion. • The contractor documents separation of duties. • The contractor implements separation of duties through assigned	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		information system access authorizations.		
AC- 6	LEAST PRIVILEGE	• The contractor employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	✓	
		• The contractor explicitly authorizes access to [list of security functions] _____ (deployed in hardware, software, and firmware) and security-relevant information. • The contractor requires that ○ users of information system accounts, or ○ roles, with access to security functions or ○ security-relevant information, use non-privileged accounts, or ○ roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or ○ roles, for such functions [list of system/security functions] _____ . _____. • The contractor limits authorization to super user accounts on the information system to designated system administration personnel.		✓
AC- 7	UNSUCCESSFUL LOGIN ATTEMPTS	• The information system enforces a limit of THREE consecutive invalid login attempts by a user during a day.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		The information system automatically: • Locks the account/node for an [Time period] _____. • Locks the account/node until released by an administrator.		
		• Delays next login prompt according to [delay algorithm] _____ when the maximum number of unsuccessful attempts is exceeded regardless of whether the login occurs via a local or network connection.		
AC- 8	SYSTEM USE NOTIFICATION	• The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the TBS Policy on the Use of Electronic Networks • The information system retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system. • The information system, for publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	✓	
AC- 9	PREVIOUS LOGON (ACCESS) NOTIFICATION	• The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).	✓	
		• The information system notifies the user, upon successful logon/access, and the number of unsuccessful logon/access attempts since the last		✓

ID	Requirement Title	Description	Baseline	Supplemental
		successful logon/access. • The information system notifies the user of the number of successful logon/access and unsuccessful logon/access [list types] _____ during [Time period] _____. • The information system notifies the user of [list of security-related changes] _____ to the user's account during [time period] _____.		
AC-11	SESSION LOCK	• The information system prevents further access to the system by initiating a session lock after [time period] _____ of inactivity or upon receiving a request from a user. • The information system retains the session lock until the user re-establishes access using established identification and authentication procedures.	✓	
		• The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.		✓
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	• The contractor identifies specific user actions that can be performed on the information system without identification or authentication. • The contractor documents and provides supporting rationale in the operations security plan for the information system, user	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		actions not requiring identification and authentication.		
		• The contractor permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.		✓
AC-16	SECURITY ATTRIBUTES	• The information system supports and maintains the binding of [list of security attributes] _____ to information in storage, in process, and in transmission.	✓	
		• The information system allows authorized entities to change security attributes. • The information system allows authorized users to associate security attributes with information. • The information system displays security attributes in human-readable form on each object output from the system to system output devices to identify [list of special dissemination, handling, or distribution instructions] _____ using [list of human readable, standard naming conventions] _____.		✓
AC-17	REMOTE ACCESS	• The contractor documents allowed methods of remote access to the information system. • The contractor establishes usage restrictions and implementation guidance for each allowed remote access method. • The contractor monitors for unauthorized remote access to the information system. • The contractor authorizes remote access to the information system prior to connection. • The contractor enforces requirements for remote connections to the information system.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor ensures that all employees working off site safeguard information as per the minimum requirements in accordance with the TBS Operational Security Standard on Physical Security		
		• The contractor employs automated mechanisms to facilitate the monitoring and control of remote access methods. • The contractor uses cryptography to protect the confidentiality and integrity of remote access sessions. The cryptography must be compliant with the requirements of control SC-13. • The information system routes all remote accesses through a limited number of managed access control points. • The contractor authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. • The contractor monitors for unauthorized remote connections to the information system Annually, and takes appropriate action if an unauthorized connection is discovered. • The contractor ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor ensures that remote sessions for accessing [list of security functions and security-relevant information] _____ employ [list of additional security measures] _____ and are audited.		
		• The contractor disables [list of deemed non-secure networking protocols] _____ within the information system except for explicitly identified components in support of specific operational requirements. • Remote access to privileged accounts is performed on dedicated management consoles governed entirely by the system's security policies and used exclusively for this purpose (e.g. Internet access not allowed).		
AC-18	WIRELESS ACCESS	• The contractor establishes usage restrictions and implementation guidance for wireless access. • The contractor monitors for unauthorized wireless access to the information system. • The contractor authorizes wireless access to the information system prior to connection. • The contractor enforces requirements for wireless connections to the information system.	✓	
		• The information system protects wireless access to the system		✓

ID	Requirement Title	Description	Baseline	Supplemental
		using authentication and encryption. • The contractor monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points Annually, and takes appropriate action if an unauthorized connection is discovered. • The contractor does not allow users to independently configure wireless networking capabilities. • The contractor disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.		
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	• The contractor establishes usage restrictions and implementation guidance for organization-controlled mobile devices. • The contractor authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems. • The contractor monitors for unauthorized connections of mobile devices to organizational information systems. • The contractor enforces requirements for the connection of mobile devices to organizational information systems. • The contractor disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction. • The contractor issues specially configured mobile devices to individuals traveling to locations that the contractor deems to be of significant risk in accordance with organizational policies and procedures. • The contractor applies [list of inspection and preventative measures] _____ to mobile devices returning from locations that the contractor deems to be of significant risk in accordance with organizational policies and procedures.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor restricts the use of writable, removable media in organizational information systems. • The contractor prohibits the use of personally owned, removable media in organizational information systems. • The contractor prohibits the use of removable media in organizational information systems when the media has no identifiable owner. • The contractor ensures that users turn off wireless devices with a voice transmission capability or physically disable the microphone when attending a meeting at which Protected B, Protected C or classified information is being shared as per the TBS Operational Security Standard - Management of Information Technology Security		✓
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	• The contractor establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems. • The contractor establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store, and/or transmit organization-controlled information using the external information systems.	✓	
		• The contractor permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when The contractor : (a) Can verify the implementation of required security controls on the external system as specified in The contractor 's information security policy and security plan; or (b) Has approved information system connection or processing agreements with The contractor al entity hosting the external		✓

ID	Requirement Title	Description	Baseline	Supplemental
		information system. • The contractor limits the use of organization-controlled portable storage media by authorized individuals on external information systems.		
AC-21	USER-BASED COLLABORATION AND INFORMATION SHARING	• The contractor facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [list information sharing circumstances] _____ .	✓	
		• The contractor employs [list of information sharing circumstances] _____ of organization-defined information sharing circumstances and automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.		
		• The contractor ensures, through written agreements, the appropriate safeguarding of sensitive information shared with other governments and organizations.		✓
AC-22	PUBLICLY ACCESSIBLE CONTENT	• The contractor designates individuals authorized to post information onto an organizational information system that is publicly accessible. • The contractor trains authorized individuals to ensure that publicly accessible information does not contain confidentially sensitive information. • The contractor reviews the proposed content of publicly accessible information for confidentially sensitive information prior to posting onto The contractor al information system. • The contractor reviews the content on the publicly accessible organizational information system for confidentially sensitive	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		information Annually. • The contractor removes confidentially sensitive information from the publicly accessible organizational information system, if discovered		

1.2 Awareness & Training (AT)

Following table lists the ITSR related to the AT domain for the PCI Advisor Service.

Table C-2: AT Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	✓	
AT-2	SECURITY AWARENESS	The contractor provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and Annually thereafter.	✓	
AT-3	SECURITY TRAINING	The contractor provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) Annually thereafter.	✓	
AT-4	SECURITY TRAINING RECORDS	• The contractor documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. • The contractor retains individual training records for [time period] _____.	✓	

1.3 Audit & Accountability (AU)

Following table lists the ITSR related to the AU domain for the PCI Advisor Service.

Table C-3: AU Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
AU- 1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	✓	
AU- 2	AUDITABLE EVENTS	• The contractor determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [list of auditable events] _____ . • The contractor coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events. • The contractor provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [list subset of the auditable events along with the frequency of (or situation requiring) auditing for each identified event] _____ .		
		• The contractor reviews and updates the list of auditable events Annually. • The contractor includes execution of privileged functions in the list of events to be audited by the information system.		✓
AU- 3	CONTENT OF AUDIT RECORDS	• The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	✓	
		• The information system includes [list detailed audit event information] _____ in the audit records for audit events identified by type, location, or subject.		✓
AU- 4	AUDIT STORAGE CAPACITY	The contractor allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	✓	
AU- 5	RESPONSE TO AUDIT PROCESSING FAILURES	• The information system alerts designated organizational officials in the event of an audit processing failure. • The information system takes the following additional actions: [list of actions to be taken] _____ e.g., shut down information system, overwrite oldest audit records, stop generating audit records.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The information system provides a warning when allocated audit record storage volume reaches [percentage] _____ of maximum audit record storage capacity.		✓
AU- 6	AUDIT REVIEW, ANALYSIS, AND REPORTING	• The contractor reviews and analyzes information system audit records Annually for indications of inappropriate or unusual activity, and reports findings to designated organizational officials. • The contractor adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information, or other credible sources of information.	✓	
		• The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. • The contractor analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. • The information system centralizes the review and analysis of audit records from multiple components within the system. • The contractor specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.		✓
AU- 7	AUDIT REDUCTION AND REPORT GENERATION	• The information system provides an audit reduction and report generation capability.	✓	
		• The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.		✓

ID	Requirement Title	Description	Baseline	Supplemental
AU- 8	TIME STAMPS	• The information system uses internal system clocks to generate time stamps for audit records.	✓	
		• The information system synchronizes internal information system clocks Annually with [authoritative time source] _____.		✓
AU- 9	PROTECTION OF AUDIT INFORMATION	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	✓	
		• The information system backs up audit records Annually onto a different system or media than the system being audited. • The contractor : (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.		✓
AU-10	NON-REPUDIATION	• The information system protects against an individual falsely denying having performed a particular action.	✓	
		• The information system associates the identity of the information producer with the information. • The information system validates the binding of the information producer's identity to the information. • The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released. • The information system validates the binding of the reviewer's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain. • The contractor employs cryptography compliant with the requirements of control SC-13 to implement digital signatures.		✓
AU-11	AUDIT RECORD	The contractor retains audit records for [time period	✓	

ID	Requirement Title	Description	Baseline	Supplemental
	RETENTION	consistent with records retention policy] _____ to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.		
AU-12	AUDIT GENERATION	• The information system provides audit record generation capability for the list of auditable events defined in AU-2 at [list of information system components] _____ . • The information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system. • The information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	✓	
		• The information system compiles audit records from [list of information system components] _____ into a system-wide (logical or physical) audit trail that is time-correlated to within [list level of tolerance for relationship between time stamps of individual records in the audit trail] _____ . • The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.		✓

1.4 Certification' Accreditation and Security Assessment (CA)

Following table lists the ITSR related to the CA domain for the PCI Advisor Service.

Table C-4: CA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	✓	
CA-2	SECURITY ASSESSMENTS	• The contractor develops a security assessment plan that describes the scope of the assessment including: (a) Security controls and control enhancements under assessment; (b) Assessment procedures to be used to determine security control effectiveness; and (c) Assessment environment, assessment team, and assessment roles and responsibilities. • The contractor assesses the security controls in the information system Annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security control requirements for the system. • The contractor produces a security assessment report that documents the results of the assessment. • The contractor provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.	✓	
		• The contractor includes as part of security control		✓

ID	Requirement Title	Description	Baseline	Supplemental
		assessments, Annually, ☐ announced ☐ unannounced ☐ in-depth monitoring ☐ malicious user testing ☐ penetration testing ☐ red team exercises [list other forms of security testing] _____ .		
CA-3	INFORMATION SYSTEM CONNECTIONS	• The contractor authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements. • The contractor documents, for each connection, the interface characteristics, security control requirements, and the nature of the information communicated. • The contractor monitors the information system connections on an ongoing basis verifying enforcement of security control requirements.	✓	
CA-5	PLAN OF ACTION AND MILESTONES	• The contractor develops a plan of action and milestones for the information system to document The contractor 's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. • The contractor updates existing plan of action and milestones Annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	✓	
CA-6	SECURITY AUTHORIZATION	• The contractor assigns a senior-level executive or manager to the role of authorizing official for the information system. • The contractor ensures that the authorizing official authorizes the information system for processing before commencing operations. • The contractor updates the security authorization Annually.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
CA-7	CONTINUOUS MONITORING	• The contractor establishes a continuous monitoring strategy and implements a continuous monitoring program that includes a configuration management process for the information system and its constituent components. • The contractor establishes a continuous monitoring strategy and implements a continuous monitoring program that includes a determination of the security impact of changes to the information system and environment of operation. • The contractor establishes a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security control assessments in accordance with the contractor's continuous monitoring strategy. • The contractor establishes a continuous monitoring strategy and implements a continuous monitoring program that includes reporting the security state of the information system to appropriate organizational officials Annually.	✓	
		• The contractor plans, schedules, and conducts assessments Annually, ☐ announced ☐ unannounced ☐ in-depth monitoring ☐ malicious user testing ☐ penetration testing ☐ red team exercises [list other forms of security assessment] _____ to ensure compliance with all vulnerability mitigation procedures.		✓

1.5 Configuration Management (CM)

Following table lists the ITSR related to the CM domain for the PCI Advisor Service.

Table C-5: CM Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually a formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	✓	
CM-2	BASELINE CONFIGURATION	• The contractor develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	✓	
		• The contractor reviews and updates the baseline configuration of the information system: (a) Annually; (b) When required due to [list of circumstances] _____; and (c) As an integral part of information system component installations and upgrades. • The contractor employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor : (a) Develops and maintains [list of software programs authorized to execute on the information system] _____; and (b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system. • The contractor maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.		
CM-3	CONFIGURATION CHANGE CONTROL	The contractor employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.	✓	
		• The contractor determines the types of changes to the information system that are configuration controlled. • The contractor approves configuration-controlled changes to the system with explicit consideration for security impact analyses. • The contractor documents approved configuration-controlled changes to the system. • The contractor retains and reviews records of configuration-controlled changes to the system. • The contractor audits activities associated with configuration-controlled changes to the system. • The contractor coordinates and provides oversight for configuration change control activities through [list of configuration change control element] _____ that convenes ☐ Annually [list of configuration change conditions] _____ .	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor tests, validates, and documents changes to the information system before implementing the changes on the operational system. • The contractor requires an information security representative to be a member of the [list of configuration change control element] _____ .		
CM-4	SECURITY IMPACT ANALYSIS	• The contractor analyzes changes to the information system to determine potential security impacts prior to change implementation.	✓	
		• The contractor analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. • The contractor , after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security control requirements for the system.		✓
CM-5	ACCESS RESTRICTIONS FOR CHANGE	• The contractor defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. • The contractor conducts audits of information system changes Annually and when indications so warrant determining whether unauthorized changes have occurred. • The contractor (a) Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and (b) Reviews and re-evaluates information system developer/integrator privileges Annually. • The contractor limits privileges to change software resident within software libraries (including privileged programs). • The information system automatically implements [list of safeguards and countermeasures] _____ if security functions (or mechanisms) are changed inappropriately.		✓

ID	Requirement Title	Description	Baseline	Supplemental
CM-6	CONFIGURATION SETTINGS	• The contractor establishes and documents mandatory configuration settings for information technology products employed within the information system using [list of security configuration checklists] _____ that reflect the most restrictive mode consistent with operational requirements. • The contractor implements the configuration settings. • The contractor identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements. • The contractor monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	✓	
		• The contractor employs automated mechanisms to centrally manage, apply, and verify configuration settings. • The contractor employs automated mechanisms to respond to unauthorized changes to [list of configuration settings] _____ .		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor incorporates detection of unauthorized, security-relevant configuration changes into The contractor 's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes. • The information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.		
CM-7	LEAST FUNCTIONALITY	• The contractor configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [list of prohibited or restricted functions, ports, protocols, and/or services] _____ .	✓	
		• The contractor reviews the information system Annually to identify and eliminate unnecessary functions, ports, protocols, and/or services. • The contractor ensures compliance with [list details of ports, protocols, and services] _____ registration requirements.		✓

ID	Requirement Title	Description	Baseline	Supplemental
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	• The contractor develops, documents, and maintains an inventory of information system components that accurately reflects the current information system. • The contractor develops, documents, and maintains an inventory of information system components that is consistent with the authorization boundary of the information system. • The contractor develops, documents, and maintains an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting. • The contractor develops, documents, and maintains an inventory of information system components that includes [list details of information deemed necessary to achieve effective property accountability] _____ . • The contractor develops, documents, and maintains an inventory of information system components that is available for review and audit by designated organizational officials.	✓	
		• The contractor updates the inventory of information system components as an integral part of component installations, removals, and information system updates. • The contractor employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. • The contractor : (a) Employs automated mechanisms Annually to detect the addition of unauthorized components/devices into the information system; and (b) Disables network access by such components/devices or notifies designated organizational officials.		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor includes in property accountability information for information system components, a means for identifying by: ☐ name ☐ position ☐ role individuals responsible for administering those components. • The contractor verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system. • The contractor includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.		
CM-9	CONFIGURATION MANAGEMENT PLAN	• The contractor develops, documents, and implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures. • The contractor develops, documents, and implements a configuration management plan for the information system that defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management. • The contractor develops, documents, and implements a configuration management plan for the information system that establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	✓	

1.6 Contingency Planning (CP)

Following table lists the ITSR related to the CP domain for the PCI Advisor Service.

Table C-6: CP Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
CP- 1	CONTINGENCY PLANNING POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. • The contractor develops an audit cycle for the contingency plan program as the basis of regular reporting to TBS.	✓	
CP- 2	CONTINGENCY PLAN	• The contractor develops a contingency plan for the information system that: (a) Identifies essential missions and business functions and associated contingency requirements; (b) Provides recovery objectives, restoration priorities, and metrics; (c) Addresses contingency roles, responsibilities, and assigned individuals with contact information; (e) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; (e) Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and (f) Is reviewed and approved by designated officials within The contractor .	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor distributes copies of the contingency plan to [list of key contingency personnel (identified by name and/or by role) and organizational elements] _____ .		
		• The contractor coordinates contingency planning activities with incident handling activities. • The contractor reviews the contingency plan for the information system Annually. • The contractor revises the contingency plan to address changes to The contractor , information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. • The contractor communicates contingency plan changes to [list of key contingency personnel (identified by name and/or by role) and organizational elements] _____ . • The contractor coordinates contingency plan development with organizational elements responsible for related plans. • The contractor conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. • The contractor plans for the resumption of essential missions and business functions within [time period] _____ of contingency plan activation.		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor plans for the full resumption of missions and business functions within [time period] _____ of contingency plan activation. • The contractor plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites. • The contractor provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.		
CP- 3	CONTINGENCY TRAINING	• The contractor trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training Annually.	✓	
		• The contractor incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.		✓
CP- 4	CONTINGENCY PLAN TESTING AND EXERCISES	• The contractor tests and/or exercises the contingency plan for the information system Annually using [list of tests and/or exercises] _____ to determine the plan's effectiveness and The contractor 's readiness to execute the plan. • The contractor reviews the contingency plan test/exercise results and initiates corrective actions.	✓	
		• The contractor coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.		
CP- 6	ALTERNATE STORAGE SITE	• The contractor establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. • The contractor identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.	✓	
CP- 7	ALTERNATE PROCESSING SITE	• The contractor establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [time period consistent with recovery time objectives] _____ when the primary processing capabilities are unavailable. • The contractor identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.	✓	
		• The contractor ensures that the alternate processing site provides information security measures equivalent to that of the primary site.		✓
CP- 8	TELECOMMUNICATIONS SERVICES	The contractor establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [time period] _____ when the primary telecommunications capabilities are unavailable.	✓	
		• The contractor :		✓

ID	Requirement Title	Description	Baseline	Supplemental
		(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with The contractor 's availability requirements; and (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. • The contractor obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services. • The contractor obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.		
CP- 9	INFORMATION SYSTEM BACKUP	• The contractor conducts backups of user-level information contained in the information system [list details of frequency consistent with recovery time and recovery point objectives] _____ . • The contractor conducts backups of system-level information contained in the information system [list details of frequency consistent with recovery time and recovery point objectives] _____ . • The contractor conducts backups of information system documentation including security-related documentation system [list details of frequency consistent with recovery time and recovery point objectives] _____ .	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor protects the confidentiality and integrity of backup information at the storage location in accordance with the TBS Operational Security Standard on Physical Security • The contractor determines retention periods for essential business information and archived backups.		
		• The contractor uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing. • The contractor stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system. • The contractor transfers information system backup information to the alternate storage site [time period and transfer rate consistent with the recovery time and recovery point objectives] _____ .		✓
CP- 9	INFORMATION SYSTEM BACKUP	The contractor tests backup information Annually to verify media reliability and information integrity.	✓	
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	• The contractor provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	✓	
		• The information system implements transaction recovery for systems that are transaction-based.		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor provides the capability to re-image information system components within [restoration time-periods] _____ from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components. • The contractor protects backup and restoration hardware, firmware, and software.		

1.7 Identification & Authentication (IA)

Following table lists the ITSR related to the IA domain for the PCI Advisor Service.

Table C-7: IA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	✓	
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	• The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	✓	
		• The information system uses [list details of replay-resistant authentication mechanisms] _____ for network access to privileged accounts. • The information system uses [list details of replay-resistant authentication mechanisms] _____ for network access to non-privileged accounts. • The information system uses multifactor authentication for remote access to privileged accounts.		✓

ID	Requirement Title	Description	Baseline	Supplemental
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	• The information system uniquely identifies and authenticates [list of specific and/or types of devices] _____ before establishing a connection.	✓	
		• The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based. • The contractor standardizes, with regard to dynamic address allocation, DHCP lease information and the time assigned to devices, and audits lease information when assigned to a device.		✓
IA-4	IDENTIFIER MANAGEMENT	• The contractor manages information system identifiers for users and devices by receiving authorization from a designated organizational official to assign a user or device identifier. • The contractor manages information system identifiers for users and devices by selecting an identifier that uniquely identifies an individual or device. • The contractor manages information system identifiers for users and devices by assigning the user identifier to the intended party or the device identifier to the intended device. • The contractor manages information system identifiers for users and devices by preventing reuse of user or device identifiers for [time period] _____ .	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor manages information system identifiers for users and devices by disabling the user identifier after [time period of inactivity] _____ .		
		• The contractor prohibits the use of information system account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address). • The contractor requires that registration to receive a user ID and password include authorization by a supervisor, and be done in person before a designated registration authority. • The contractor requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority. • The contractor manages user identifiers by uniquely identifying the user as [list characteristic identifying user status] _____.		✓

ID	Requirement Title	Description	Baseline	Supplemental
IA-5	AUTHENTICATOR MANAGEMENT	• The contractor manages information system authenticators for users and devices by verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator. • The contractor manages information system authenticators for users and devices by establishing initial authenticator content for authenticators defined by The contractor . • The contractor manages information system authenticators for users and devices by ensuring that authenticators have sufficient strength of mechanism for their intended use. • The contractor manages information system authenticators for users and devices by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators. • The contractor manages information system authenticators for users and devices by changing default content of authenticators upon information system installation. • The contractor manages information system authenticators for users and devices by establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate).	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor manages information system authenticators for users and devices by changing/refreshing authenticators [time period] _____ by authenticator type. • The contractor manages information system authenticators for users and devices by protecting authenticator content from unauthorized disclosure and modification. • The contractor manages information system authenticators for users and devices by requiring users to take, and having devices implement, specific measures to safeguard authenticators.		
		• The information system, for password-based authentication: • (a) Enforces minimum password complexity of [list] _____ requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type;		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• (b) Enforces at least a [number of changed characters] _____ when new passwords are created; (c) Encrypts passwords in storage and in transmission; • (d) Enforces password minimum and maximum password lifetime restrictions of [numbers for lifetime minimum, lifetime maximum] _____; and • (e) Prohibits password reuse for [number] _____ generations. • The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the user account. • The contractor requires that the registration process to receive [list types of and/or specific authenticators] _____ be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).		

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor protects authenticators commensurate with the sensitivity and criticality of the information and information system being accessed. • The contractor ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. • The contractor takes [list of measures] _____ to manage the risk of compromise due to individuals having accounts on multiple information systems.		
IA-6	AUTHENTICATOR FEEDBACK	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	✓	
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable CSEC guidance for such authentication.	✓	
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	✓	

1.8 Incident Response (IR)

Following table lists the ITSR related to the IR domain for the PCI Advisor Service.

Table C-8: IR Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. • The contractor 's incident response policy and procedures facilitate the incorporation of heightened levels of readiness during emergency and heightened IT threat situations in accordance with the TBS Operational Security Standard - Readiness Levels for Federal Government Facilities and the TBS Operational Security Standard - Management of Information Technology Security.	✓	
IR-2	INCIDENT RESPONSE TRAINING	• The contractor trains personnel in their incident response roles and responsibilities with respect to the information system. • The contractor provides refresher training Annually.	✓	
		• The contractor incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.		✓
IR-3	INCIDENT RESPONSE TESTING AND EXERCISES	The contractor tests and/or exercises the incident response capability for the information system Annually using [list of tests and/or exercises] _____ to determine the incident response effectiveness and	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		documents the results.		
IR-4	INCIDENT HANDLING	• The contractor implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. • The contractor coordinates incident handling activities with contingency planning activities. • The contractor incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	✓	
		• The contractor identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. • The contractor correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.		✓
IR-5	INCIDENT MONITORING	The contractor tracks and documents information system security incidents.	✓	
IR-6	INCIDENT REPORTING	The contractor requires personnel to report suspected security incidents to the contractor incident response capability within THREE (3) months of the incident.	✓	
		• The contractor reports security incident information to designated authorities. • The contractor reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.	✓	
IR-7	INCIDENT RESPONSE ASSISTANCE	The contractor provides an incident response support resource, integral to The contractor incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
IR-8	INCIDENT RESPONSE PLAN	• The contractor develops an incident response plan that: (a) Provides The contractor with a roadmap for implementing its incident response capability; (b) Describes the structure and organization of the incident response capability; (c) Provides a high-level approach for how the incident response capability fits into the overall organization; (d) Meets the unique requirements of The contractor , which relate to mission, size, structure, and functions; (e) Defines reportable incidents; (f) Provides metrics for measuring the incident response capability within The contractor ; (g) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and (h) Is reviewed and approved by designated officials within The contractor . • The contractor distributes copies of the incident response plan to [list of incident response personnel (identified by name and/or by role) and organizational elements] _____ . • The contractor reviews the incident response plan Annually. • The contractor revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor communicates incident response plan changes to [list of incident response personnel (identified by name and/or by role) and organizational elements] _____ .		

1.9 System Maintenance (MA)

Following table lists the ITSR related to the MA domain for the PCI Advisor Service.

Table C-9: MA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	✓	
MA-2	CONTROLLED MAINTENANCE	• The contractor schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or contractor specifications and/or organizational requirements. • The contractor controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. • The contractor requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. • The contractor sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs. • The contractor checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	✓	
		• The contractor maintains maintenance records for the information system that include: (a) Date and time of maintenance;		✓

ID	Requirement Title	Description	Baseline	Supplemental
		(b) Name of the individual performing the maintenance; (d) Name of escort, if necessary; (e) A description of the maintenance performed; and (e) A list of equipment removed or replaced (including identification numbers, if applicable).		
MA-3	MAINTENANCE TOOLS	• The contractor approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.	✓	
		• The contractor checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.		✓
MA-4	NON-LOCAL MAINTENANCE	• The contractor authorizes, monitors, and controls non-local /remote maintenance and diagnostic activities. • The contractor allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system. • The contractor employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions. • The contractor maintains records for non-local maintenance and diagnostic activities.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions. • The contractor documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections. • The contractor : (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system. • The contractor protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either: (a) Physically separated communications paths; or (b) Logically separated communications paths based upon encryption compliant with the requirements of control SC-13.		✓

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor requires that: (a) Maintenance personnel notify [list of personnel] _____ when non-local maintenance is planned (i.e., date/time); and (b) A designated organizational official with specific information security/information system knowledge approves the non-local maintenance. • The contractor employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.		
MA-5	MAINTENANCE PERSONNEL	• The contractor establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel. • The contractor ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	✓	
		• The contractor maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not Canadian citizens, that include the following requirements: (a) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;		✓

ID	Requirement Title	Description	Baseline	Supplemental
		(b) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all non-volatile storage media are removed or physically disconnected from the system and secured; and (c) In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.		

1.10 Media Protection (MP)

Following table lists the ITSR related to the MP domain for the PCI Advisor Service.

Table C-10: MP Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	✓	
MP-2	MEDIA ACCESS	• The contractor restricts access to [list types of digital and non-digital media] _____ to [list of authorized individuals] _____ using [list of security measures] _____ .	✓	
		• The contractor employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. • The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.		✓
MP-3	MEDIA MARKING	• The contractor marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor exempts [list of removable media types] _____- from marking as long as the exempted items remain within [list of controlled areas] _____ .		
MP-4	MEDIA STORAGE	• The contractor physically controls and securely stores [types of digital and non-digital media] _____ within [list ofcontrolled areas] _____ and in accordance with the RCMP G1-001, Security Equipment Guide • The contractor physically protects and securely stores Classified and Protected information system media awaiting destruction (either on- or off-site) using approved equipment, techniques, and procedures.	✓	
		• The contractor employs cryptographic mechanisms to protect information in storage.		✓
MP-5	MEDIA TRANSPORT	• The contractor protects and controls [list types of digital and non-digital media] _____ during transport outside of controlled areas using [list of security measures] _____ in accordance with the TBS Operational Security Standard on Physical Security and the RCMP Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor maintains accountability for information system media during transport outside of controlled areas. • The contractor restricts the activities associated with transport of such media to authorized personnel.		
		• The contractor documents activities associated with the transport of information system media. • The contractor employs cryptographic mechanisms compliant with the requirements of control SC-13 to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.		✓
MP-6	MEDIA SANITIZATION	• The contractor sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse. • The contractor employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.	✓	
		• The contractor tracks, documents, and verifies media sanitization and disposal actions. • The contractor tests sanitization equipment and procedures to verify correct performance Annually. • The contractor sanitizes information system media containing sensitive information in accordance with applicable GC policies, standards, and procedures. • The contractor destroys information system media that cannot be sanitized.		✓

1.11 Physical & Environmental (PE)

Following table lists the ITSR related to the PE domain for the PCI Advisor Service.

Table C-11: PE Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
PE- 1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	✓	
PE- 2	PHYSICAL ACCESS AUTHORIZATIONS	• The contractor develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). • The contractor issues authorization credentials. • The contractor reviews and approves the access list and authorization credentials Annually, removing from the access list personnel no longer requiring access.	✓	
		• The contractor authorizes physical access to the facility where the information system resides based on position or role. • The contractor issues an identification card to all personnel, which as a minimum includes the name of The contractor , the bearer's name and photo, a unique card number and an expiry date.		✓
PE- 3	PHYSICAL ACCESS CONTROL	• The contractor controls access to areas officially designated as publicly accessible in accordance with The contractor 's assessment of risk. • The contractor secures keys, combinations, and other	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		physical access devices. • The contractor inventories physical access devices annually. • The contractor changes combinations and keys annually and when keys are lost, combinations are compromised, or individuals are transferred or terminated. • The contractor enforces physical access authorizations to the information system independent of the physical access controls for the facility.		
		• The contractor enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible). • The contractor verifies individual access authorizations before granting access to the facility. • The contractor controls entry to the facility containing the information system using physical access devices and/or guards. • The contractor guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week. • The contractor uses lockable physical casings to protect [list of information system components] _____ from unauthorized physical access.		✓
PE- 4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	The contractor controls physical access to information system distribution and transmission lines within organizational facilities.	✓	
PE- 5	ACCESS CONTROL FOR OUTPUT DEVICES	The contractor controls physical access to information system output devices to prevent unauthorized individuals from obtaining	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		the output.		
PE- 6	MONITORING PHYSICAL ACCESS	• The contractor monitors physical access to the information system to detect and respond to physical security incidents. • The contractor reviews physical access logs Annually. • The contractor coordinates results of reviews and investigations with The contractor ’s incident response capability.	✓	
		• The contractor monitors real-time physical intrusion alarms and surveillance equipment.		✓
PE- 7	VISITOR CONTROL	• The contractor controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	✓	
		• The contractor escorts visitors and monitors visitor activity, when required.		✓
PE- 8	ACCESS RECORDS	• The contractor maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). • The contractor reviews visitor access records Annually.	✓	
		• The contractor maintains a record of all physical access, both visitor and authorized individuals.		✓
PE-13	FIRE PROTECTION	The contractor employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	✓	
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	• The contractor maintains temperature and humidity levels within the facility where the information system resides at [list of acceptable levels] _____ .	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.		
PE-15	WATER DAMAGE PROTECTION	The contractor protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	✓	
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	The contractor positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	✓	

1.12 Security Planning (PL)

Following table lists the ITSR related to the PL domain for the PCI Advisor Service.

Table C-12: PL Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	✓	
PL-4	RULES OF BEHAVIOUR	• The contractor establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behaviour with regard to information and information system usage. • The contractor receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behaviour, before authorizing access to information and the information system. • The contractor includes in the rules of behaviour, explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information.	✓	

1.13 Personnel Security (PS)

Following table lists the ITSR related to the PS domain for the PCI Advisor Service.

Table C-13: PS Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	✓	
PS-3	PERSONNEL SCREENING	• The contractor screens individuals prior to authorizing access to the information system in accordance with the TBS Personnel Security Standard • The contractor rescreens individuals according to [list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening] _____ .	✓	
PS-4	PERSONNEL TERMINATION	• The contractor , upon termination of individual employment terminates information system access. • The contractor , upon termination of individual employment conducts exit interviews. • The contractor , upon termination of individual employment retrieves all security-related organizational information system-related property.	✓	
PS-6	ACCESS AGREEMENTS	• The contractor ensures that individuals requiring access to organizational information and information systems sign	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		appropriate access agreements prior to being granted access. • The contractor reviews/updates the access agreements Annually.		
		• The contractor ensures that access to information with special protection measures is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; and (a) Satisfy associated personnel security criteria.		✓
PS-7	THIRD-PARTY PERSONNEL SECURITY	• The contractor establishes personnel security control requirements including security roles and responsibilities for third-party providers. • The contractor documents personnel security control requirements. • The contractor monitors provider compliance. • The contractor ensures security screening of private sector organizations and individuals who have access to Protected and Classified information and assets, in accordance with the TBS Personnel Security Standard • The contractor explicitly defines government oversight and end-user roles and responsibilities relative to third-party provided services in accordance with the TBS Security and Contracting Management Standard	✓	

1.14 Risk Assessment (RA)

Following table lists the ITSR related to the RA domain for the PCI Advisor Service.

Table C-14: RA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	✓	
RA-2	SECURITY CATEGORIZATION	• The contractor categorizes information and the information system in accordance with applicable GC legislation and TBS policies, directives, and standards. • The contractor documents the security categorization results (including supporting rationale) in the security plan for the information system. • The contractor ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	✓	
RA-3	RISK ASSESSMENT	• The contractor conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits, in accordance with the TBS Security Organization and Administration Standard • The contractor updates the risk assessment Annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
RA-5	VULNERABILITY SCANNING	• The contractor scans for vulnerabilities in the information system and hosted applications [list details of frequency and/or randomly in accordance with organization-defined process] _____ and when new vulnerabilities potentially affecting the system/applications are identified and reported. • The contractor employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: (a) Enumerating platforms, software flaws, and improper configurations; (b) Formatting and making transparent, checklists and test procedures; and (c) Measuring vulnerability impact. • The contractor analyzes vulnerability scan reports and results from security control assessments.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor remediates legitimate vulnerabilities [response times] _____ in accordance with an organizational assessment of risk. • The contractor shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout The contractor to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).		
		• The contractor employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. • The contractor updates the list of information system vulnerabilities scanned Annually or when new vulnerabilities are identified and reported.		✓

1.15 System & Services Acquisition (SA)

Following table lists the ITSR related to the SA domain for the PCI Advisor Service.

Table C-15: SA Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
SA- 1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	✓	
SA- 3	SA- 3 LIFE CYCLE SUPPORT	• The contractor manages the information system using a system development life cycle methodology that includes information security considerations. • The contractor defines and documents information system security roles and responsibilities throughout the system development life cycle. • The contractor identifies individuals having information system security roles and responsibilities.	✓	
SA- 5	INFORMATION SYSTEM DOCUMENTATION	• The contractor obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: (a) Secure configuration, installation, and operation of the information system; (b) Effective use and maintenance of security features/functions; and (c) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. • The contractor obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		(a) User-accessible security features/functions and how to effectively use those security features/functions; (b) Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and (c) User responsibilities in maintaining the security of the information and information system.		
SA- 6	SOFTWARE USAGE RESTRICTIONS	The contractor uses software and associated documentation in accordance with contract agreements and copyright laws.	✓	
SA- 7	USER-INSTALLED SOFTWARE	The contractor enforces explicit rules governing the installation of software by users.	✓	
SA- 8	SECURITY ENGINEERING PRINCIPLES	The contractor applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	✓	
SA- 9	EXTERNAL INFORMATION SYSTEM SERVICES	• The contractor requires that providers of external information system services comply with organizational information security control requirements and employ appropriate security controls in accordance with the TBS Security and Contracting Management Standard • The contractor defines and documents government oversight and user roles and responsibilities with regard to external information system services. • The contractor monitors security control compliance by external service providers.	✓	
		The contractor : (a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and (b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [list details of senior organizational official]_____.		✓

1.16 Security Function Isolation (SC)

Following table lists the ITSR related to the SC domain for the PCI Advisor Service.

Table C-16: SC Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
SC- 1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	✓	
SC- 5	DENIAL OF SERVICE PROTECTION	• The information system protects against or limits the effects of the following types of denial of service attacks: [list of types of denial of service attacks or reference to source for current list] _____ .	✓	
		• The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.		✓
SC- 7	BOUNDARY PROTECTION	• The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. • The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces. • The information system prevents public access into The contractor 's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. • The contractor limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. • The contractor : (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy Annually; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. • The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). • The contractor prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. • The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with		✓

ID	Requirement Title	Description	Baseline	Supplemental
		resources in external networks.		
SC- 8	TRANSMISSION INTEGRITY	• The information system protects the integrity of transmitted information.	✓	
		• The contractor employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. The cryptography must be compliant with the requirements of control SC-13.		✓
SC- 9	TRANSMISSION CONFIDENTIALITY	• The information system protects the confidentiality of transmitted information.	✓	
		• The contractor employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by [list alternative physical measures] _____ . The cryptography must be compliant with the		✓

ID	Requirement Title	Description	Baseline	Supplemental
		requirements of control SC-13.		
SC- 10	NETWORK DISCONNECT	The information system terminates the network connection associated with a communications session at the end of the session or after [time period] _____ of inactivity.	✓	
SC- 12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	• The contractor establishes and manages cryptographic keys for required cryptography employed within the information system.	✓	
		• The contractor maintains availability of information in the event of the loss of cryptographic keys by users.		✓
SC- 13	USE OF CRYPTOGRAPHY	• The information system implements cryptographic protections using cryptographic systems that comply with applicable GC legislation and TBS policies, directives and standards.	✓	
		• The contractor employs [Selection: CMVP-validated; CSEC-approved] cryptography to implement digital signatures.		✓
SC- 14	SC- 14 PUBLIC ACCESS PROTECTIONS	The information system protects the integrity and availability of publicly available information and applications.	✓	
SC- 17	SC- 17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES	The contractor issues public key certificates under a [list details of certificate policy] _____ or obtains public key certificates under an appropriate certificate policy from an approved service provider.	✓	
SC- 19	VOICE OVER INTERNET PROTOCOL	• The contractor establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously. • The contractor authorizes, monitors, and controls the use of VoIP within the information system.	✓	
SC- 22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
	SERVICE			
SC- 23	SESSION AUTHENTICITY	• The information system provides mechanisms to protect the authenticity of communications sessions.	✓	
		• The information system invalidates session identifiers upon user logout or other session termination. • The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages. • The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.		✓
		• The information system generates unique session identifiers with [list randomness requirements] _____ .		
SC- 28	PROTECTION OF INFORMATION AT REST	The information system protects the confidentiality and integrity of information at rest.	✓	

1.17 System & Information Integrity (SI)

Following table lists the ITSR related to the SI domain for the PCI Advisor Service.

Table C-17: SI Requirements List

ID	Requirement Title	Description	Baseline	Supplemental
SI- 1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	• The contractor develops, disseminates, and reviews/updates Annually a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • The contractor develops, disseminates, and reviews/updates Annually formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	✓	
SI- 2	FLAW REMEDIATION	The contractor identifies, reports, and corrects information system flaws.	✓	
SI- 3	MALICIOUS CODE PROTECTION	• The contractor employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: (a) Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or (b) Inserted through the exploitation of information system vulnerabilities. • The contractor updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. • The contractor configures malicious code protection mechanisms to: (a) Perform periodic scans of the information system Annually and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		(b) ☐ block malicious code ☐ quarantine malicious code ☐ send alert to administrator [list action] _____ in response to malicious code detection. The contractor addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.		
		• The contractor centrally manages malicious code protection mechanisms. • The information system automatically updates malicious code protection mechanisms (including signature definitions). • The information system prevents non-privileged users from circumventing malicious code protection capabilities. • The information system updates malicious code protection mechanisms only when directed by a privileged user. • The contractor does not allow users to introduce removable media into the information system. • The contractor tests malicious code protection mechanisms Annually by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.		✓

ID	Requirement Title	Description	Baseline	Supplemental
SI- 4	INFORMATION SYSTEM MONITORING	• The contractor monitors events on the information system in accordance with [list monitoring objectives] _____ and detects information system attacks. • The contractor identifies unauthorized use of the information system. • The contractor deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to The contractor . • The contractor heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information, or other credible sources of information. • The contractor obtains legal opinion with regard to information system monitoring activities in accordance with GC legislation and TBS policies, directives and standards. • The contractor employs automated tools to support near real-time analysis of events. • The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [list of compromise indicators]_____ . • The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities. • The information system notifies [list of incident response personnel (identified by name and/or by role)] _____ of suspicious events and takes [list of least-disruptive actions to terminate suspicious events] _____ . • The contractor protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.		

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor tests/exercises intrusion monitoring tools [time-period] _____ . • The contractor makes provisions so that encrypted traffic is visible to information system monitoring tools. • The contractor analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies. • The contractor employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [list of inappropriate or unusual activities that trigger alerts] _____ . • The contractor : (a) Analyzes communications traffic/event patterns for the information system; (b) Develops profiles representing common traffic patterns and/or events; and		

ID	Requirement Title	Description	Baseline	Supplemental
		(c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives to [list measure of false positives] _____ and the number of false negatives to [list measure of false negatives] _____ . • The contractor employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. • The contractor employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.		
SI- 5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	• The contractor receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis. • The contractor generates internal security alerts, advisories, and directives as deemed necessary. • The contractor disseminates security alerts, advisories, and directives to [list of personnel (identified by name and/or by role)]_____ . • The contractor implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of non-compliance.	✓	
SI- 7	SOFTWARE AND INFORMATION INTEGRITY	• The information system detects unauthorized changes to software and information.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
		• The contractor reassesses the integrity of software and information by performing Annually integrity scans of the information system. • The contractor employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification. • The contractor employs centrally managed integrity verification tools. • The contractor requires use of tamper-evident packaging for [list of information system components] _____ during ☐ transportation from contractor to operational site ☐ during operation		✓
SI- 8	SPAM PROTECTION	• The contractor employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means. • The contractor updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.	✓	
		• The contractor centrally manages spam protection mechanisms. • The information system automatically updates spam protection mechanisms (including signature definitions).		✓
SI- 9	INFORMATION INPUT RESTRICTIONS	The contractor restricts the capability to input information to the information system to authorized personnel.	✓	

ID	Requirement Title	Description	Baseline	Supplemental
SI-10	INFORMATION INPUT VALIDATION	The information system checks the validity of information inputs.	✓	
SI-11	ERROR HANDLING	• The information system identifies potentially security-relevant error conditions. • The information system generates error messages that provide information necessary for corrective actions without revealing [list details of sensitive or potentially harmful information] _____ in error logs and administrative messages that could be exploited by adversaries. • The information system reveals error messages only to authorized personnel.	✓	
SI-12	INFORMATION OUTPUT HANDLING AND RETENTION	The contractor handles and retains both information within and output from the information system in accordance with applicable GC legislation and TBS policies, directives and standards, and operational requirements.	✓	

TASK AUTHORIZATION FORM -
FORMULAIRE D'AUTORISATION DE TÂCHE
ANNEX - ANNEXE D

Contract Number - Numéro du contrat	
Task Authorization (TA) No. - N° de l'autorisation de tâche (AT)	
Contractor's Name and Address - Nom et adresse de l'entrepreneur	
Original Authorization - Autorisation originale	
Total Estimated Cost of Task (GST/HST extra) before any revisions: Coût estimatif total de la tâche (TPS/TVH en sus) avant toutes révisions :	$
TA Revisions Previously Authorized(as applicable) - Révisions de l'AT autorisées précédemment (s'il y a lieu)	

TA Revision No. - N° de Révision de l'AT :		Authorized Increase or Decrease (GST/HST extra): Augmentation ou réduction autorisée (TPS/TVH en sus) : $
TA Revision No. - N° de Révision de l'AT :		Authorized Increase or Decrease (GST/HST extra): Augmentation ou réduction autorisée (TPS/TVH en sus): $
TA Revision No. - N° de Révision de l'AT :		Authorized Increase or Decrease (GST/HST extra): Augmentation ou réduction autorisée (TPS/TVH en sus): $

New TA Revision (as applicable) - Nouvelle révision de l'AT (s'il y a lieu)		
TA Revision No. - N° de Révision de l'AT :		Authorized Increase or Decrease (GST/HST extra): Augmentation ou réduction autorisée (TPS/TVH en sus): $
Total Estimated Cost of Task (GST/HSTextra) after this revision: Coût estimatif total de la tâche (TPS/TVH en sus) après cette révision :		$

Contract Security Requirements (as applicable) - Exigences du contrat relatives à la sécurité (s'il y a lieu)

This task includes security requirements. - Cette tâche comprend des exigences relatives à la sécurité:

☐ No - Non

☐ Yes. Refer to the Security Requirements Checklist (SRCL) annex of the Contract. Oui. Voir l'annexe du contrat comprenant la Liste de vérification des exigences relatives à la sécurité (LVERS).

Remarks (as applicable) - Remarques (s'il y a lieu):

Required Work - Travaux requis

The content of sections A, B, C and D below must be in accordance with the Contract. Le contenu des sections A, B, C et D ci-dessous doit être conforme au contrat.

SECTION A - Task Description of the Work required - Description de tâche des travaux requis

SECTION B - Applicable Basis of Payment - Base de paiement applicable

☐ Firm Lot Price of $_____for the professional fees identified in Section C below

OR

☐ Limitation of Expenditure of $_____ for the authorized travel and living expenses identified in Section C below

☐ Prix de lot ferme de _____$ pour les honoraires professionnels identifiés à la Section C ci-dessous

OU

☐ Limitation des dépenses de _____$ pour les frais autorisés de déplacement et de subsistance identifiés à la Section C ci-dessous

SECTION C - Cost Breakdown of Task- Ventilation du coût de la tâche

1.0 Professional Fees

Category	All Inclusive Fixed Daily Rate	Level of Effort (Estimated number of days required to perform the Work)

Total Estimated Cost of Professional Fees: $_____ *(insert the applicable amount)*;

2.0 Authorized travel and living expenses for Work performed outside the National Capital Region (NCR)only;

Total Estimated Cost of Authorized travel and living expenses for Work performed outside the National Capital Region (NCR)only: $_____ *(insert the applicable amount)*

1.0 Honoraires professionnels

Catégorie	Taux fixe journalier tout compris	Niveau D'effort (Nombre estimatif de jours requis pour exécuter les travaux)

Coût total estimatif des honoraires professionnels: _____$ *(insérer le montant applicable)*

2.0 Frais autorisés de déplacement et subsistance - travaux exécutés à l'extérieur de la région de la capitale nationale (RCN) seulementl;

Coût total estimatif des frais autorisés de déplacement et subsistance - travaux exécutés à l'extérieur de la région de la capitale nationale (RCN) seulement: _____$ *(insérer le montant applicable)*

SECTION D - Applicable Method of Payment - Méthode de paiement applicable

☐ Milestone Payments for professional fees only

☐ Schedule of Milestone:

The schedule of milestones for which payments will be made in accordance with the Contract is as follows:

MILESTONE	ACTIVITY(IES) TO BE PERFORMED / DELIVERABLE(S) TO SUBMIT	COMPLETION /DELIVERY DATE	FIRM AMOUNT

☐ Monthly payments;

☐ Single payment.

☐ Paiement d'étapes pour les honoraires professionnels seulement

☐ Calendrier des étape:

Le calendrier des étapes selon lequel les paiements seront faits en vertu du contrat est comme suit:

ÉTAPE	ACTIVITÉS À EXÉCUTER/ PRODUITS À LIVRER	DATED'ACHÈVEMEN / DATE DE LIVRAISON	FIRM AMOUNT

☐ Paiements mensuels;

☐ Paiement unique.

Authorization - Authorization

By signing this TA, the Project Authority or the PWGSC Contracting Authority or both, as applicable, certify (ies) that the content of this TA is in accordance with the Contract.

En apposant sa signature sur cette AT, le chargé de projet ou l'autorité contractante de TPSGC ou, s'il y a lieu, les deux atteste(nt) que le contenu de cette AT respecte les conditions du contrat.

Name of Project Authority - Nom du chargé de projet _____

Signature _____ Date _____

Name of PWGSC Contracting Authority -
Nom de l'autorité contractante de TPSGC _____

Signature _____ Date _____

Contractor's Signature - Signature de l'entrepreneur

Name and title of individual authorized to sign for the Contractor
Nom et titre de la personne autorisée à signer au nom de l'entrepreneur

_____

Signature _____ Date _____