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

Part - Partie 1 of - de 2
See Part 2 for Clauses and Conditions
Voir Partie 2 pour Clauses et Conditions

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Quebec
K1A 0S5
Bid Fax: (819) 997-9776

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Comments - Commentaires

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

Issuing Office - Bureau de distribution
Mainframe & Business Software Procurement Division / Div des achats des ordi principaux et des logiciels de gestion
11 Laurier St. / 11, rue Laurier
4C1, Place du Portage III
Gatineau
Quebec
K1A 0S5

Title - Sujet CLOUD RFI	
Solicitation No. - N° de l'invitation EN578-151297/B	**Date** 2014-12-02
Client Reference No. - N° de référence du client 20151297	**GETS Ref. No. - N° de réf. de SEAG** PW-$EEM-033-28243
File No. - N° de dossier 033eem.EN578-151297	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à** 12:00 PM **on - le** 2015-01-21	**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: Cayer, Natalie	**Buyer Id - Id de l'acheteur** 033eem
Telephone No. - N° de téléphone (819) 956-1380 ( )	**FAX No. - N° de FAX** (819) 953-3703
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

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

Canada

Further to the Industry Event Notice published under EN578-151297/A, this is a Request for Information (RFI) (see attached PDF document) pertaining to the Industry Cloud Computing Consultation, which is an initiative to aid the Government of Canada (GC) build a strategy for adopting cloud solutions.

The Government of Canada is seeking feedback from industry on the following subject matter:

(i) The questions provided in Part II of this RFI;
(ii) Industry's recommendations for a low risk approach for deciding which opportunities are appropriate for the Cloud;
(iii) The ability to meet anticipated (draft) security requirements in Annex E; and
(iv) The ability to meet the proposed contract clauses, terms and conditions in Annex C.

The GC intends to use feedback from (i), (ii), (iii), and (iv) to solidify its Cloud Strategy and help determine the "way forward" for how Cloud solutions should be acquired, delivered, and managed.

Organizations are encouraged to not feel bound by the questions in Part II, but to provide feedback on any portion of the RFI or add additional information or clarification that may aid Canada in structuring its strategy or learning from case studies and experiences of organizations.

One-on-One meetings:
Following the close of the RFI, at Canada's discretion, meetings may be held with Respondents to seek further clarification or elaboration on their RFI response.

Government of Canada Gouvernement du Canada

CANADA’S CLOUD CONSULTATION

REQUEST FOR INFORMATION
CLOUD COMPUTING SOLUTIONS
EN578-151297/B

Contents

BACKGROUND 3

PURPOSE 3

PART I: REQUEST FOR INFORMATION 5

Nature of Request for Information 5

Nature and Format of Responses Requested 5

Response Costs 5

Treatment of Responses 5

Contents of this RFI 6

Format of Responses 6

Enquiries .... **Error! Bookmark not defined.**

Submission of Responses 7

PART II: QUESTIONS 8

Policy Questions 8

Business Questions 10

Procurement Questions 13

Security and Privacy Questions 14

ANNEXES 17

Annex A - Key Performance Indicators 17

Service Availability 17

Service Availability (Recovery Point Objective) 17

Service Availability (Recovery Time Objective) 18

Incident Management (Mean Time to Resolve) 19

Incident Management (Service Desk Availability) 19

Incident Management (Client Satisfaction) 20

Release Management (Notification) 21

Release Management (Updates) 21

Annex B - Application Service Models 22

Annex C - Proposed Contract clauses, terms and conditions 23

Annex D – Proposed GC Cloud Deployment Decision Matrix 29

Annex E – Sample Security Requirements 32

BACKGROUND

Canada is taking steps to better position itself to access the potential technological and economic benefits of cloud computing. Specifically, Canada is seeking industry input on how to bring business opportunities to tender in a consistent manner while mitigating risks associated with the Cloud.

In April 2014, The Honourable Tony Clement, President of the Treasury Board, announced that Canada would undertake a cloud consultation process with Industry.

"Cloud computing offers the federal government a way to maximize the efficiency of our IT investments. We're looking for input from industry experts on how we can use cloud computing to achieve those savings." Tony Clement, President of the Treasury Board, April 7, 2014 – Banff, AB

This Request for Information (RFI) marks the beginning of a consultation process that will pave the way to increasingly deliver services to Canadians leveraging Cloud solutions. As the information technology industry evolves, new methods of delivering services and accessing technologies are emerging. Canada has seen an increased amount of services being offered through cloud computing solutions via a variety of delivery and deployment models. As the industry moves toward cloud-based technology applications, platforms, and services, Canada is seeking feedback from the industry in order to ensure its contracting practices, vehicles, and terms and conditions evolve to reflect this new method of delivery.

Canada would therefore like to engage in a dialog with industry related to cloud computing solutions and understand its influence on:

- Policy: How our policy framework supports or impedes accessing Cloud technologies
- Business: New service delivery enablers, service Levels Agreements, on-boarding and off-boarding, business vocabulary, technical terminology, evaluation methods, and how to mitigate risks associate with the Cloud.
- Procurement: future Request for Proposals (RFPs), Statement of Work or Requirement (SOW, SOR), and resulting Contract Terms and Conditions used by the industry and the Government.
- Security: Consideration for our current and potential future security accreditation processes, certifications, and controls.

PURPOSE

The purpose of this RFI is to receive feedback, ideas and suggestions from suppliers on how future solicitation and resulting contracts for cloud computing solutions might be structured. Information that will be received from industry will be used to assist Canada in developing its policies, service agreements, solicitation documents, the resulting contract terms and conditions.

The main objectives of this RFI are to allow industry to:

a. Share views and influence the direction Canada should take with respect to cloud computing;

b. Comment on the risks associated with accessing cloud computing solutions and mitigation strategies for reducing those risks;

c. Influence the parameters Canada must consider when determining when/if a business opportunity is a right fit for the Cloud market;

d. Comment on the framework used by Canada to ensure its security and privacy risks are reduced;

e. Provide ideas and suggestions as to how Canada could evolve its security and privacy framework in light of the Cloud;

f. Assess and comment on the adequacy and clarity of the existing resulting Contract Standard Acquisitions Contracting Clauses, Terms and Conditions as currently expressed; and

g. Provide ideas and suggestions regarding potential alternative business vocabulary, technical terminology, procurement processes and methods of supply that would better meet the requirements of cloud computing solutions.

As part of Canada's Cloud consultation process, both Government of Canada (GC) and Public Sector Chief Information Council (PSCIOC) steering committees have been created to govern this consultation process. The GC steering committee is comprised of a representative sample of departmental Chief Information Officers, legal, communications, and procurement experts. The PSCIOC steering committee is comprised of IT leaders amongst GC and Provincial Governments. One potential outcome of this consultation process will be the exploration of Pan-Canadian Cloud opportunities, including the potential for procurement on behalf of provinces or other levels of government.

There is no obligation for a respondent to answer all questions within this RFI. Do not feel confined to the questions included within the document; respondents are encouraged to provide information aligned to the spirit of this consultation process.

PART I: REQUEST FOR INFORMATION

Nature of Request for Information

This is not a bid solicitation. This RFI will not result in any direct request for proposal or the award of any contract. As a result, potential suppliers of any goods or services described in this RFI should not reserve stock or facilities, nor allocate resources, as a result of any information contained in this RFI. Nor will this RFI result in the creation of any source list. Therefore, whether or not any potential supplier responds to this RFI will not preclude that supplier from participating in any future procurement. Also, the procurement of any of the goods and services described in this RFI will not necessarily follow this RFI. This RFI is simply intended to solicit feedback from industry with respect to the matters described within this document.

Nature and Format of Responses Requested

Respondents are requested to provide their comments, suggestions, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this RFI could be satisfied. Respondents are invited to respond to Canada's questions and provide comments regarding the content, format of any draft documents included in this RFI. Respondents should explain any assumptions they make in their responses.

Response Costs

Canada will not reimburse any respondent for expenses incurred in responding to this RFI.

Treatment of Responses

1. **Use of Responses**: The responses received may be used by Canada, Provinces, and Territories to develop or modify procurement strategies and/or any contracting documents, clauses, terms and conditions. Canada will review all responses received by the RFI closing date. Canada may, in its discretion, review responses received after the RFI closing date.
2. **Review Team**: A review team composed of representatives of the Government of Canada and Provincial Governments will review the responses. Canada reserves the right to hire an independent consultant (Gartner Inc.), if Canada considers it necessary, to review any response received as a result of this RFI. Not all members of the review team will necessarily review all responses.
3. **Confidentiality**: Respondents should mark any portions of their response that they consider proprietary or confidential. Canada will handle the responses in accordance with the *Access to Information Act*.
4. **Follow-up Activity**: Canada may, in its sole discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response.
5. **One-on-one meetings:** Canada may, in its sole discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response during one on ones meetings.

Contents of this RFI

This document remains a work in progress and respondents should not assume that new clauses or requirements will not be added to any bid solicitation that is ultimately published by Canada. Nor should respondents assume that none of the clauses or requirements will be deleted or revised. Comments regarding any aspect of the draft document are welcome. If respondents feel a question or key area has been missed, we welcome comments or information to this fact in their response.

Format of Responses

1. **Cover Page**: If the response includes multiple volumes, respondents are requested to indicate on the front cover page of each volume the title of the response, the solicitation number, the volume number and the full legal name of the respondent.

2. **Title Page**: The first page of each volume of the response, after the cover page, should be the title page, which should contain:

   2.1. The title of the respondent’s response and the volume number;
   2.2. the name and address of the respondent;
   2.3. the name, address and telephone number of the respondent’s contact;
   2.4. the date; and
   2.5. the RFI number.

3. **Numbering System**: Respondents are requested to prepare their response using a numbering system corresponding to the one in this RFI. All references to descriptive material, technical manuals and brochures included as part of the response should be referenced accordingly.

4. **Number of Copies**: Canada requests that respondents submit electronically by email 1 copy of their responses.

Enquiries

Because this is not a bid solicitation, Canada will not necessarily respond to enquiries in writing or by circulating answers to all potential suppliers. However, respondents with questions regarding this RFI may direct their enquiries to:

Natalie Cayer
A/Manager
Software and Shared Systems Procurement Directorate
Acquisitions Branch
Public Works and Government Services Canada
Natalie.cayer@tpsgc-pwgsc.gc.ca

Submission of Responses

1. **Time and Place for Submission of Responses**: Suppliers interested in providing a response should send it by email to TPSGC.ConsultationsINformatiqueenNuage-CloudConsultations.PWGSC@tpsgc-pwgsc.gc.ca by January 21, 2015 at 12:00 EDT. Suppliers wishing to submit their responses via a channel other than email need to contact the procurement manager indicated above.

2. **Responsibility for Timely Delivery**: Each respondent is solely responsible for ensuring its response is submitted on time to the correct email address.

3. **Identification of Response**: Each respondent should ensure that the response is identified and that the name and email address, the RFI number and title appear legibly in the email.

PART II: QUESTIONS

Consultation Process Question

1. Does your organization wish to participate in the planned one-on-one consultations that will take place after the RFI responses have been collected and reviewed? Please indicate either, “yes” for we would like to participate or “no” for we do not wish to participate.

Policy Questions

2. Are there any policies or legislation in place now in Canada, either at, the Federal level or at Provincial/Territorial/Municipal level that limit or create barriers for industry related to the provision of cloud solutions? If so what are they and what is their impact? Please indicate in the response what level of government you are discussing.

3. What tools (policy, guidance, strategies) could Canada’s Governments (Federal/Provincial/Territorial/Municipal) develop to facilitate the efficient adoption of cloud solutions?

4. Canada is in the process of establishing a GC Cloud (See: Annex D for definition). One of the key advantages of this cloud is that it will be fully certified to the Federal Government’s security requirements. If Canada were to position this cloud as the preferred, or even only, IaaS provider for SaaS or PaaS vendors:
    a. What are the barriers to this approach?
    b. How could Canada, when receiving responses to RFPs, evaluate proposals that use the GC Cloud vs. those that use Private or Public Clouds;
        i. Technically (i.e. time to certify Cloud environments, level of protection, service levels)?
        ii. Financially (i.e. compare costs of GC and Industry provided infrastructure)?
    c. What prerequisites would need to exist for P/SaaS vendors to use the GC Cloud?

5. The following strategies have been suggested for reducing Canada’s risks associated with contracting cloud services. How would you address each of these strategies? For example, are they viable, do you foreseen challenges or are there alternative solutions Canada should be considering?
    a. Require that all domestic data traffic be routed exclusively through Canada;
    b. Require that all databases in which the data is stored be running on servers located in Canada;
    c. Ensure that there are no connections from the Canadian database(s)/servers to any supplier database located outside Canada, with no way (short of hacking) of accessing the Canadian database(s) from a location outside of Canada;

d. Encrypt the data (in transit and at rest) and ensure that encryption keys are held only by Canada;
e. Require physical segregation of Canada's data as part of the design of the solution;
f. Require robust auditing functions and actually perform audits regularly to detect unauthorized access, including by the contractor;
g. Require the contractor to identify specific individuals who will have access to the information and require those individuals to sign separate non-disclosure agreements and be cleared to an appropriate level;
h. Include provisions in the contract that make it clear that Canada owns and controls all data and that the contractor does not;
i. Make it a breach of contract to access the data except as necessary to perform the contract. Make it a breach to print the data, copy the data, provide access to the data to any third party, etc.; and
j. Prohibit subcontracting without consent and ensure, before giving consent that the subcontractor must adhere to all the other defined controls.

6. What policy amendments would specifically enable Pan-Canadian (Federal, Provincial, Territorial, Municipal) cloud enabled business opportunities?

Business Questions

Opportunities

7. How can cloud solutions be used to deliver innovative services to Canadians with greater agility?
    a. Can you provide case studies from other public sector jurisdictions?
    b. What best practices should be employed in leveraging cloud solutions to successfully drive efficiencies within a business domain?

8. How can Canada encourage the growth of a Canadian Cloud market? Is this realistic or needed? What is a reasonable amount of time required for developing this market?

9. What prerequisites should Canada have in place before acquiring cloud solutions?

Software Services

10. It is Canada's view that software services can be provided by Industry in a number of models (See Annex B). While similarities exist between these models, it is Canada's view that they need to be governed under different contractual agreements.
    a. Has Canada correctly defined each of the software services models?
    b. What elements of acquiring SaaS do you feel apply to these other models?

Service Level Agreements

11. Canada believes that Service Level Agreements (SLAs) are a key component of any contractual agreement with a cloud vendor.
    a. Please state your views on this statement
    b. Are there other methods to enforce a cloud service agreement (SaaS, PaaS, IaaS) you feel Canada should consider?

12. Annex A provides a minimum set of Key Performance Indicators (KPIs) Canada would likely consider in a Statement of Work when procuring SaaS and PaaS.
    a. Are these an appropriate set of KPIs?
    b. Can you suggest additional KPIs?
    c. Can you suggest improvements to these KPIs?
    d. Would using these KPIs have a negative impact on your business offerings?

13. Annex A provides a minimum set of Key Performance Indicators Canada would likely use in a Statement of Work when procuring SaaS and/or PaaS. From these KPIs, Canada would select Critical Performance Indicators (CPIs) used to calculate Service Credits for service level non-compliance.
    a. Can use suggest which KPIs should become CPIs and why?
    b. Can you suggest a weighting of CPIs?

14. As part of cloud service contracts, Canada would like to include a system of Service Credits for service level non-compliance.
    a. Can you suggest a methodology for calculating Service Credits

15. As part of Cloud service contracts Canada would like to monitor the performance of service levels.
    a. Can you suggest methods that Canada can employ to monitor performance throughout the life cycle of the service agreement?
    b. How can Canada be certain that performance is being correctly demonstrated by the vendor?

Cloud Sprawl

16. As Canada increases its usage of cloud solutions the number of logical and physical locations of data storage will increase.
    a. Is this a problem in your view? If so, how do you suggest Canada manages issues such as, data management or interoperability?
    b. Can you suggest practical measures to mitigate Cloud Sprawl?

17. How can Canada ensure integration with existing legacy or other cloud solutions?
    a. Can you suggest integration standards and approaches?
    b. Please state your views on the availability of integration standards amongst the different cloud service offerings (SaaS, PaaS, IaaS). Should Canada be adopting an integration standard?

Vendor Qualifications

18. Canada frequently uses the number of years of providing services to clients in a production environment as a method of evaluation.
    a. Please state your views on using this evaluation method for the cloud market
    b. Can you suggest other methods of quantitatively evaluating cloud vendors?

19. How can Canada mitigate the risks associated with cloud vendor lock-in?
    a. What strategies can Canada employ when migrating from one cloud provider to another?
    b. How can Canada lower the cost of migration?
    c. How can Canada ensure its data holdings are transferable from one cloud solution to another, including Shared Services Canada?

Accessing Cloud

20. How can Canada repatriate its data in the event of contract non-performance, shift in Canada strategic choices, or vendor bankruptcy?

21. What are your company's views on engaging a third party to acquire and manage cloud vendors (i.e Cloud Broker) for Cloud solutions?

22. Is the management of disaster recovery different with cloud solutions? If so, how does one plan for and manage disaster recovery with cloud solutions? What are the risks and how are they mitigated?

Procurement Questions

Standard Acquisition Clauses and Conditions

23. What standard acquisition clauses, contract terms and conditions and definitions should be included in a cloud solution contract. Please see the proposed Terms and Conditions attached at Annex C and provide feedback and comments.

Financial

24. What pricing structure, unit of measure, basis of payment, method of payment, evaluation methodologies and contract period length (including amount of options years) should Canada consider as part of Request for Proposals or Limited tendering requirements? What are the benefits and drawbacks of each?

Procurement Process

25. How can Canada make the procurement process required to acquire cloud solutions easier for all parties engaged in the process?
    a. What challenges are faced currently?
    b. What methods of supply would best meet the needs of Canada and the industry: prequalified competitive supply arrangements, RFP‘s resulting in multi-departmental contract, others?

Technology, Trends & Contract Clauses

26. How should Canada address the quick change in technology, from a contractual perspective, in order to ensure continuity of business, best services and cost?

27. How do we ensure we can move data between services or back to Canada when contracts are concluded?

28. How do we future-proof investments in cloud solutions so that efficiency gains in technology are passed back to the customer, without retendering a contract?

Cloud Sourcing

29. What factors should Canada consider when determining which cloud service models (e.g. SaaS, PaaS, IaaS) would best meet our requirements and which service models offer the most opportunity for competition when taking into account the availability of solutions?
    a. Which service models can offer the most benefit to Canada, taking into consideration socio-economic benefits (e.g. related to small and medium enterprise, environment, savings, job creation and Innovation, cost savings and security)?

30. What is the recommended approach for categorization of cloud software (current Software Licensing Supply Arrangement Categories, United Nations Standard Products and Services Code etc), what categorization/coding method is most commonly used and what categories/codes are most commonly available?

Security and Privacy Questions

Security and Privacy Background

Canada has begun to standardize security and privacy requirements for cloud procurements. As an example, Annex E contains security requirements prepared for a system that will process unclassified information with low data integrity and availability requirements. We are seeking input into our current security approach for cloud computing and wish to explore alternative or additional approaches with Industry.

31. Annex D contains a proposed decision making matrix meant as a tool for guiding departmental CIOs as to which opportunities are appropriate for the cloud.
    a. Are the parameters of Information Confidentiality Rating and Mission Criticality appropriate for determining which business opportunities are right for the cloud?
    b. Do you believe there are cloud deployment models Canada has neglected to consider?
    c. Do you foresee any issues with adopting this decision making matrix?

32. Data Sovereignty is considered a key requirement to ensure only the laws of Canada apply to its data holdings.
    a. What is your opinion as to whether Canada's privacy risk mitigations can be adequately fulfilled in a scenario where the information is hosted in a facility NOT located in Canada?
    b. What is your opinion as to whether Canada's privacy risk mitigations can be adequately fulfilled in a scenario where the information is hosted in Canada BUT by a foreign owned organization?
    c. Are there any strategies/tools that you consider adequate to provide data sovereignty protection to information in either;
        a. locations in Canada but where the data is hosted by foreign owned organizations; or
        b. locations outside of Canada?
    d. For which Information Confidentiality Rating do you think these strategies/tools would be adequate? What is your rationale for this opinion?

Current Approach

33. Currently, Canada is developing a series of security control profiles for specific Information Technology implementations, including cloud computing. Using an approach inspired by the US Government's FedRAMP program as well as other cloud security best practices, security controls will be scaled to the sensitivity of the data being stored or manipulated in the cloud and formulated in a list of security requirements known as 'profiles'.

a. Are there any specific areas of the baseline FedRAMP profiles (Available at http://cloud.cio.gov/documents/fedramp-security-controls) that would create what you consider to be undue costs to Canada or hardships to the service providers in meeting these requirements? Hardship could include:
    a. Implementation time
    b. Cost of implementation
    c. Cost of operations

b. Are there any areas of the security requirements that have been developed for current Canadian cloud initiatives (Annex E) that your company would be unable to meet by July 2015?

34. Supply chain integrity is the process of managing an organization's internal capabilities, as well as its partners and suppliers, to ensure all elements of an integrated solution are of high assurance. The need for integrity in the supply chain is necessary, whether the solution is developed in-house or purchased from a third party. The term "supply chain" often has implications of physical goods. In the technology sector, it relates to hardware, such as computers, networking equipment, mobile devices and servers.
    a. How can Canada be assured that supply chain security practices meet our standards?
    b. Should they be applied to all cloud solutions?

35. Currently, federal contract clauses dictate the type and level of facility and personnel security clearances that need to be maintained in order to provide goods or services to Canada.
    a. What challenges could be encountered with this approach and what are the costs to your organization of obtaining clearance in a cloud environment?
    b. How could those challenges be overcome yet ensure the security and privacy of the Government's data?
    c. What type of IT inspection would be appropriate for a cloud environment in order to determine the security of the hosting environment?
    d. Many SaaS/PaaS provider offerings are deployed on another IaaS provider's infrastructure. How best can Canada fulfill its requirement for a facilities clearance in this situation?

Approaches under Investigation

36. Canada is considering aligning its approach to Cloud security with certifications commonly found in the market.
    a. Do you think Canada should develop its own certification approach aligned with one currently available in the market such as:
        i. US (FedRAMP) Authority to Operate (ATO);
        ii. UK (GCloud) Pan Government Accreditation;
        iii. and more generally under the guise of certifications such as ISO 27001, or;

iv. Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) certification?

b. What are the benefits of aligning to one of the above certification approaches?

c. How can Canada offset the cost of implementing such a security program?

d. Do you feel there are disadvantages to Canada seeking strong evidence of security capability in provider offerings? What are they?

37. If Canada adopts a certification process, how do you see this being implemented to enable and facilitate procurement of cloud services for departments? What do you foresee as the level of interest amongst the Cloud industry to undertake such a certification process?

ANNEXES

Annex A - Key Performance Indicators

Service Availability

Property	Description
Description	Parameter used to measure the Availability of the production systems and their various components (including , interfaces and Content Stores), including all production environments within or supporting the Services application
Formula	percentage Availability = [(total minutes in a calendar month – total minutes Unavailable) / total minutes in a calendar month] x 100
Target Performance	100%
Performance Requirement	≥ 99.50%
Measurement Interval	Monthly
Effective Date	Service Commencement Date
Operating Hours	Extended Business Hours
Service Credits	99.49 to 95.50% availability, a credit of 5% of monthly service fee shall apply 95.49 to 90.50% availability, a credit of 8% of monthly service fee shall apply Less or equal to 90.49% availability, a credit of 15% of monthly service fee shall apply

Service Availability (Recovery Point Objective)

Property	Description
Description	Parameter used to measure the maximum tolerable period for which data

Property	Description
	may not be recovered due to a major incident.
Target Performance	0 hours
Performance Requirement	1 hour
Measurement Interval	Monthly
Effective Date	Service Commencement Date
Operating Hours	Extended Business Hours
Service Credits	1.01 to 2 hours loss of data, a credit of 10% of monthly service fee shall apply 2.01 to 4 hours loss of data, a credit of 20% of monthly service fee shall apply Greater than or equal to 4.01 hours loss of data, a credit of 40% of monthly service fee shall apply

Service Availability (Recovery Time Objective)

Property	Description
Description	Parameter used to measure the maximum tolerable period of time to recover due to a major incident or loss of service.
Target Performance	0 hours
Performance Requirement	4 hour
Measurement Interval	Monthly
Effective Date	Service Commencement Date
Operating Hours	Extended Business Hours

Service Credits	4.01 to 6 hours to recover, a credit of 10% of monthly service fee shall apply 6.01 to 8 hours to recover, a credit of 20% of monthly service fee shall apply Greater than or equal to 8.01 hours to recover, a credit of 40% of monthly service fee shall apply

Incident Management (Mean Time to Resolve)

Property	**Description**
Description	Parameter used to measure the Mean Time to Resolve an incident having occurred in the production systems and their various components (including , interfaces and Content Stores), including all production environments within or supporting the Services application
Formula	(Time incident is resolved - Time incident is reported)
Performance Requirement	Severity Level 1; 95% < 4 hours / 100% < 8 hours Severity Level 2; 95% < 6 hours / 100% < 24 hours Severity Level 3; 95% < 2 business days / 100% < 5 business days Severity Level 4; 75% < 5 business days / 100% < 10 business days
Measurement Interval	Monthly
Effective Date	Service Commencement Date
Operating Hours	Extended Business Hours

Incident Management (Service Desk Availability)

Property	**Description**
Description	Parameter used to ensure a minimum number of hours of operation of the service desk to report incidents (tele-phone or text).

Property	Description
Data Capture	Receive Date / Time, Resolution Date / Time, Close Date / Time Incident Resolutions Incident Description Incident Assignments Effort spend on Incidents
Performance Requirement	6:00 am to 8:00 pm EST
Measurement Interval	Monthly
Effective Date	Service Commencement Date

Incident Management (Client Satisfaction)

Property	Description
Description	Parameter used to measure the satisfaction of service received from clients of the Service Desk.
Survey Method	After-call survey or Outbound survey to determine satisfaction as: Very Satisfied Satisfied Somewhat Satisfied Not Satisfied
Performance Requirement	75% Satisfied or Very Satisfied
Measurement Interval	Monthly
Effective Date	Service Commencement Date

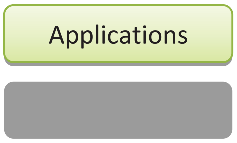
Release Management (Notification)

Property	Description
Description	Parameter used to measure the minimum tolerable period of time between notification of a change occurring to the service and the change becoming effective in a production environment
Formula	(date of change occurring in production – date of change notification being issued)
Performance Requirement	20 business days for changes that have an impact on users or application features 3 business days for changes that have no impact to users or application features
Measurement Interval	Monthly
Effective Date	Service Commencement Date

Release Management (Updates)

Service Level	Notification of Available Patches, Updates, Releases Service Level
Description	Parameter used to measure the maximum tolerable period of time between a release of a patch or update becoming commercially available and it becoming effective in the production environment
Target Performance	• Patches: Within 120 Standard Operating Hours following announcement of availability • Other Updates: Within 30 elapsed days following announcement of availability
Performance Requirement	• Patches: ≥ 99% • Other Updates: ≥ 95%
Measurement Interval	Monthly
Effective Date	Service Commencement Date

Annex B - Application Service Models



Annex C - Proposed Contract clauses, terms and conditions

Suppliers of the industry are invited to review the proposed additional contract terms, conditions and clauses for Cloud-Based Software Services, provide comments and/or suggestion on other appropriate clauses, business vocabulary and/or technical wording.

The following proposed clause, terms and conditions are not in order and do not constitute all the clauses, terms and conditions that will be in future resulting Contracts.

1. Definitions:

a. Cloud Computing: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

b. Hosted software: A third-party manages and operates software on behalf of the Government of Canada off-premises within the privately owned data-centres.

c. Managed Software: A third-party manages and operates software on behalf of the Government of Canada on-premises within the Government of Canada owned data-centres.

d. Software as a Service: is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software". SaaS is typically accessed by users using a thin client via a web browser. The term "software as a service" (SaaS) is considered to be part of the nomenclature of cloud computing, along with infrastructure as a service (IaaS), platform as a service (PaaS), desktop as a service (DaaS), backend as a service (BaaS), and information technology management as a service (ITMaaS).

e. Cloud Service Provider: is responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment are also the responsibilities of the Service Provider. The Cloud Computing Service Provider is the Contractor for this Contract.

2. Requirement: The Contractor agrees to supply to Canada the services described in the Contract including all annexes, in accordance with and at the price set out in the Contract. This includes:

   i) Granting the license to access and use the commercially available (cloud, hosted, managed, software services) solution;

   ii) Providing the (cloud, hosted, managed, software services) solution documentation;

   iii) Granting the (cloud, hosted, managed, software services);

iv) Providing commercial off the shelf Online training as part of the solution, if available;

v) Providing access to forums and frequently asked questions if available;

vi) Providing professional services as requested by Canada (if applicable); and

vii) Providing Support on the (cloud, hosted, managed, software services) solution.

3. Ownership of the (Cloud, Software, Service) solution: Canada acknowledges that the ownership of the (Cloud, Software, Service) solution belongs to the Contractor or its licensor and is not transferred to Canada. As a result, any reference in the Contract to any part of the (Cloud, Software, Service) as a deliverable must be interpreted as a reference to the (services/license/right to use or access) to the (Cloud, Software, Service) solution and not to own the (Cloud, Software, Service) solution.

4. Ownership of Data: Canada owns all right, title and interest in its data related to the services provided by the Contract.

5. Disabling Code warranty: The Cloud Computing Service Provider (the Contractor) must provide to Canada , in advance and on a ongoing basis, if Canada is not in default of its obligations regarding the use of the service, all the information required by Canada to use and continue to use the Service provided under the Contract if the Services provided contains any features, functions or characteristics (Disabling Codes) that might cause the Service to be unusable by Canada without passwords, authorization codes or similar information.

6. Transferability: The (license or right to use or access) the (Cloud, Solution, Software, Service) solution under the Contract is transferable by Canada under the same conditions of the Contract, to any Canadian government department, corporation or agency, as defined in the Financial Administration Act, R.S.C. 1985, c.F-11, as amended from time to time, or to any other party for which the Department of Public Works and Government Services Canada has been authorized to act under section 16 of the Department of Public Works and Government Services Act, S.C. 1996, c.16, as long as Canada informs the Contractor of the transfer within thirty(30) days of the transfer occurring.

7. Partners identification: The Contractor must identify all of its strategic business partner related to the services provided under this Contract, including but not limited to the subcontractors, entities and individuals who may be a party to this contract, a joint venture or similar agreement with the service provider, who will be involved in any application development and / or operations related to the service provided under this Contract.

8. Notice of partnership: The Contractor must inform Canada of Outsources functions and receive approval from Canada before entering into an arrangement with a subcontractor or partner in the performance of duties related to the Contract / Services provided.

9. Responsibility: The Contractor remains directly responsible for all aspects of the Contract and its compliance despite any outsourced components unless otherwise approved in writing by the Contracting Authority.

10. No assignment: The Contractor may not assign the Contract or transfer any part of the agreement without express written consent from Canada.

11. Business continuity and Disaster Recovery: The Contractor must possess adequate disaster recovery and business continuity processes from a manmade or natural disaster. The Contractor must provide their business continuity and disaster recovery plan to Canada upon request. The plans must include but is not limited to:

    i. How long it would take to recover from a disruption,

    ii. How long it will take to switch to a backup site,

    iii. The level of service and functionality provided by the backup site; and within what time frame the provider will recover the primary data and service; and,

    iv. A report on how and how often the data are backed up.

12. Non-public and sensitive data: The Contractor must encrypt all non-public Canada data that resides on any of the Services Providers mobile devices during the life of the Contract.

13. Staff Integrity Provisions: The Contractor must conduct criminal background check and not utilize any staff, including subcontractor, to fulfill the obligations of the contract who has been convicted of any crime or dishonesty. The Contractor must promote and maintain an awareness of the importance of securing Canada' s information among the Contractor employees and agents.

14. Separation of duties: The Contractor must enforced separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of Canada's data to that which is absolutely needed to perform to work.

15. Advance notice of change: An advance notice of change must be given to Canada 30 days prior to any major upgrade or system changes that the Contractor will be performing. A major upgrade is a replacement of the hardware , software, or firm ware with a new or better version, in order to bring the system up to date or to improve its characteristics and usually includes a new version number. Canada reserves the right to not accept any functionality changes, upgrade or replacement and shall have the right to replace or terminate the Contract for convenience.

16. Suspension of Services: The Contractor must not suspend any part of the Services where Canada is reasonably disputing any amount due to the Contractor; and/or any unpaid but undisputed

amount to the Contractor is less than 90 business days in arrears. During the any period of suspension, the Contractor must not take any actions to intentionally erase any of Canada data.

17. Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the Contractor must not take any action to intentionally erase any of Canada's data for a period of 90 days after the effective date of termination.

18. Secure disposal of Data: When requested by Canada, the provider must destroy all requested data in all of its form, for example, electronic, online, disk, CD, DVD, backup tape, and paper. Data must be permanently deleted and must not be recoverable.

19. Personal Information and Records - Ownership and Management: The Contractor acknowledge that is has no rights to the personal information or the records and that Canada owns the Records. On request the Contractor must make the personal information and records available to Canada within 2 Federal Government Working Days where the data reside in the (cloud, services, solution, software, hosted solution..) and within 5 Federal Government Working Days where the data needs to be retrieved from offsite backup media in a format acceptable to Canada.

20. Personal Information Collection and disclosure: The Contractor must only collect personal information required to perform the work and the Contractor must inform the individual of the following: a) that the Personal Information is being collected on behalf of, and will be provided to, Canada, b) the way the Personal Information will be used, c) that the disclosure of Personal Information is voluntary or, if there is a legal requirement to disclose Personal Information, the basis of that legal requirement, d) the consequences, if any, of refusing to provide the Information, e) that the individual has the right to access and correct his own Information; and f) that the Personal Information will form part of a specific personal information bank (with the meaning of Privacy Act), and also with the information about which government institution controls that personal information bank.

21. Safeguard of Canada's information: Protection of personal privacy and sensitive data must be an integral part of the business activities of the Contractor to ensure that there is no inappropriate or unauthorized use of Canada's data and information at any time. To this end the Service Provider must safeguard the confidentiality, integrity, and availability of Canada's information and comply with the following:

22. Personal Information received by the Contractor under this Contract and shall become and remain the property of Canada.

23. At no time any data or information which either belongs to or are intended for the use of Canada, its officer, agents or employees, can be copied, disclosed retained for subsequent use in any transaction that does not include Canada.

24. The Contractor must not use any collected data from Canada in connection with the services performed under this Contract for any other purpose other than fulfilling the service.

25. The Contractor must encrypt all non-public, personal and sensitive data and information in transit to the Cloud during the life of the Contract and 90 days after termination.

26. The Services Provider (the Contractor) must not store any non-public, personal or sensitive data and information outside of Canada. This includes backup data and disaster recovery locations.

27. Return of Canada's Data: At the end of the contract period, the Contractor must provide Canada, within thirty business days, without charge and without any conditions, a final extract of the Canada's Data in the format specified by Canada. Further, the Contractor must certify to Canada the destruction of Canada's Data within the possession or control of Contractor but such destruction must only occur after the Data has been returned to Canada. This Section survives the termination of this Agreement.

28. Loss of Data: In the event of any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise the security, confidentiality, or integrity of Canada's Data or the physical, technical , administrative, or organisational safeguards put in place by the Contractor that relate to the protection of the security, confidentiality, integrity of Canada's Data, the Contractor must, as applicable, a) notify Canada as soon as possible, but no later than 24 hours of becoming aware of such occurrence; b) cooperate with Canada in investigating the occurrence, including making available all relevant records, files, data reporting, and other materials required to comply with applicable law pr as otherwise required by Canada; c) perform or take any actions required to comply with applicable law as a result of the occurrence; d) indemnify, defend, and hold harmless Canada for any and all claims, including reasonable attorney's fees, costs, and expenses incidental thereto, which may be suffered by. Accrued against, charged to , or recoverable from Canada in connection with the occurrence; e) recreate the lost Data in the manner and on the schedule set by Canada without charge to Canada; and f) provide Canada a detailed plan within 10 calendar days of the occurrence describing the measures the Contractor will undertake to prevent a future similar occurrence to happen.

29. Data Privacy and Information Security: Without limiting Contractor's obligations of confidentiality under this Contract, the Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, administrative , and organisational safeguards, that are designed to: a) ensure the security and confidentiality of Canada's Data; b) protect against any anticipated threats or hazards to the security or integrity of Canada's Data; c) protect against any unauthorized disclosure, access or use of Canada's Data; d) ensure proper disposal of Canada's Data; and e) ensure that all employees, agents, and subcontractors of the Contractor, if any, comply with all of the foregoing.

30. SACC clause 9122C: Protection and Security of Data Stored in Databases

31. Protection and Security of Data Stored in Databases for Canadian and Foreign Suppliers:

(i) The Contractor and/or any and all subcontractors must ensure that all the databases used by organizations to provide the services described in the Contract containing any Personal Information, related to the Work, are located in Canada, the United States (US), the European Union (EU) or in the following additional countries with which Canada has a Bilateral and Multinational Memorandum of Understanding and Industrial Security Arrangement: Australia, Israel, New Zealand, Norway, and Switzerland.

(ii) The Contractor and/or any and all subcontractors must control access to all databases, referred to in subsection 1, on which any Personal Information related to the Work is stored so that only individuals with the appropriate security clearance are able to access the database, either by using a password or other form of access control.

(iii) The Contractor must ensure that all databases on which any data relating to the Contract is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases, unless those databases are located in Canada (or in another country approved by the Contracting Authority ((in collaboration with the Canadian DSA) under subsection 1) and otherwise meet the requirements of this article.

(iv) The Contractor must ensure that all data relating to the Contract is processed only in Canada or in another country approved by the Contracting Authority (in collaboration with the Canadian DSA) under subsection 1.

(v) Despite any section of the General Conditions relating to subcontracting, the Contractor and/or any and all subcontractors must not subcontract (including to a parent, subsidiary or affiliate) any function, relating to the provision of services described in Annex A - SOR, that involves providing a subcontractor with access to any Personal Information related to the Work unless the Contracting Authority (in collaboration with the Canadian DSA) first consents in writing.

Annex D – Proposed GC Cloud Deployment Decision Matrix

Data at rest location	*Information Confidentiality rating*			
In Canada	Classified and Protected C	GC Cloud Deployment	GC Cloud Deployment	GC Cloud Deployment
	Protected B	Private, Hybrid, Community, GC Cloud Deployment	Private, Hybrid, Community, GC Cloud Deployment	Private, GC Cloud Deployment
	Protected A	Public, Private, Hybrid, Community, GC Cloud Deployment	Public, Private, Hybrid, Community, GC Cloud Deployment	Private, Hybrid, Community, GC Cloud Deployment
Anywhere	Unclassified	Public, Private, Hybrid, Community, GC Cloud Deployment	Public, Private, Hybrid, Community, GC Cloud Deployment	Public, Private, Hybrid, Community, GC Cloud Deployment
Mission Criticality		Low	Medium	High

Definitions:

Classified

Information is “classified” if its disclosure could harm the “national interest”. The “national interest” concerns the defence and maintenance of the social, political and economic stability of Canada. When information is classified in the national interest, a further judgement is needed to determine the classification level. The level depends on the gravity of the detrimental effects that might reasonably be expected to occur from compromise.

The levels of classification are as follows:

- Top secret: applies to the very limited amount of information that, if compromised, could reasonably be expected to cause exceptionally grave injury to the national interest;
- Secret: applies to information that, if compromised, could reasonably be expected to cause serious injury to the national interest; and
- Confidential: applies when compromise could reasonably be expected to cause injury to the national interest.

Designated

Information is “designated” if its disclosure could harm interests other than harm to the “national interest.” There are three levels of designated information which are identified as:

- Protected C (extremely sensitive): applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the national interest, for example, loss of life.
- Protected B (particularly sensitive): applies to information that, if compromised, could reasonably be expected to cause serious injury outside the national interest, for example, loss of reputation or competitive advantage.
- Protected A (low-sensitive): applies to information that, if compromised, could reasonably be expected to cause injury outside the national interest, for example, disclosure of an exact salary figure.

Mission Critical

Mission Critical applications support Critical Services and Products

Critical Services and Products: the outputs of program services and products whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the effective functioning of the government.

Maximum Allowable Downtime: the longest period of time for which a critical service and product can be unavailable or degraded before a high degree of injury results

- High: 0-4 hours
- Medium: 4-48 hours
- Low: 2-6 days

Cloud Deployment Models (based on NIST)

GC cloud. The cloud infrastructure is provisioned by Shared Services Canada for exclusive use by the Government of Canada comprising multiple departments and Agencies. It is owned, managed, and operated by the Government of Canada and exists on premises.

Private cloud. The cloud services are provisioned for exclusive use by the Government of Canada comprising multiple departments and agencies. It is owned, managed, and operated by a private company and exists off premises.

Community cloud. The cloud services are provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. An example would be a partnership between different public sector governments.

Public cloud. The cloud services are provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud services are a composition of two or more distinct cloud infrastructures (GC, private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Data at Rest Location

Anywhere: Any location contingent on achieving the required security verifications by the Industrial Security Program.

In Canada: Any location within the geographical boundaries of Canada contingent on achieving the required security verifications by the Industrial Security Program.

Annex E – Sample Security Requirements

Note: requirements extracted from the current Managed Web Services Solution RFP, available at https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EEM-044-28065

Category	Sub-Category	Description
Business Continuity	Contingency Planning	The Contractor must perform backup, recovery and refresh operations on a periodic basis. The Contractor must provide Recovery Point Objective, RPO (e.g. no more than 45 minutes of lost data) and Recovery Time Objective, RTO, (e.g. up within 2 hour of outage) as part of the Service Levels. The Contractor must, at a frequency that is consistent with RTO/RPO: a) Conduct backups of user-level information contained in the MWS; b) Conduct backups of system-level information contained in the MWS; c) Conduct backups of MWS documentation including security-related documentation; and d) Protect the confidentiality and integrity of backup information at the storage location in accordance with media protection requirements.
Security Operations	Configuration Management	The Contractor must develop, document, and maintain under configuration control, a current baseline configuration of the MWS components.
Security Operations	Configuration Management	The Contractor must develop, document, and maintain an inventory of the MWS Service Infrastructure components that: a) accurately reflects their current configuration; b) is at the level of granularity deemed necessary for tracking and reporting; c) includes enough information to achieve effective property accountability; d) is available for review and audit by GC, and e) is updated as an integral part of component installations, removals, and MWS Service.
Security Operations	Configuration Management	The Contractor must manage configuration settings for MWS Service Infrastructure that includes: a) specifying configuration settings to implement least privilege/functionality; b) documenting exceptions to configuration settings, and c) monitoring and controlling changes to the configuration settings in accordance with the Change Management and Configuration Management processes.
Security Operations	Security Monitoring	The Contractor must automatically monitor on a continuous basis events for the MWS to: a) detect attacks, Incidents and abnormal events against the MWS and Hosting Environment; b) identify unauthorized use and access of MWS Data and MWS components, and. c) respond, contain, and recover from threats and attacks against the MWS.

Category	Sub-Category	Description
Security Operations	Security Monitoring	The Contractor must respond to security alerts, advisories, and directives from designated external organizations (i.e SSC) on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by GC; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies GC of the degree of non-compliance.
Security Operations	Security Incident Management	The Contractor must notify GC via phone and email (7 days x 24 hours x 365 days), based on priority as specified by GC, of any suspected or actual Security Incidents, including: i. denial of service attacks; ii. malware; iii. social engineering; iv. unauthorized intrusion or access; v. information breach; and vi. all other security breaches or cyber threats targeting Canada.
Security Operations	Security Incident Management	The Contractor must report all suspected or actual privacy and security violations for MWS Services as Security Incidents.
Security Operations	Security Incident Management	The Contractor must provide all evidence associated with a Security Incident, within a time interval specified by the GC that includes: a) results of historical logs and audit records research associated with one or many Partners based on criteria provided by GC; b) results of analysis of logs and audit records associated with one or many Partners based on criteria provided by GC; c) logs and audit records based on criteria provided by GC, and d) additional information or data as specified by GC.

Security Operations	Security Incident Management	The Contractor must provide a Security Incident post-mortem report to GC, within 72 hours of a request by GC, that includes, but is not limited to:
		a) Security Incident number;
		b) Security Incident opened date;
		c) Security Incident closed date;
		d) description of Security Incident;
		e) scope of Security Incident;
		f) chain of events / timeline;
		g) actions taken by Contractor;
		h) lessons learned;
		i) limitations/issues with MWS; and
		j) recommendations to improve MWS.

Category	Sub-Category	Description
Security Operations	Investigations	The Contractor must implement an audit and investigation process that: a) Allows only specific, pre-authorized representatives of Canada to request and receive discrete access and information associated with MWS Data (user data, event logs, content) for the purposes of conducting investigations; and b) Is approved by GC. The Contractor shall not disclose such access to End Users. The Contractor must report such access to Canada on a monthly basis by Partner organization and by Contractor.

Security Operations	Security Reports	The Contractor must provide GC with summary reports and statistical logs periodically (i.e. weekly, monthly or quarterly) and on-demand including:
		a) Dashboard reporting on system performance
		b) Real-time and historical performance against SLA
		c) Reporting on Utilization Statistics
		d) Security incident reports, post-mortem, adhoc reports, and associated evidence;
		e) security Incident tickets;
		f) user activity reports;
		g) operator activity reports;
		h) access reports;
		i) configuration audit reports;
		j) configuration change reports;
		k) file integrity monitoring reports;
		l) inventory reports;
		m) vulnerability reports;
		n) security threat reports;
		o) Emergency Request For Changes and Request For Changes; and
		p) patches and security patches implemented.

Security Operations	Patch Management	The Contractor must perform patch management appropriate to the scope of their control and adhere to GC standards. This includes: a) ensuring the latest version of applications and operating systems are used; b) ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner; c) prioritizing critical patches and service packs using a risk-based approach; d) taking applications offline and bringing them back online; e) aligning criticality levels for patches as specified by GC; f) rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2; and g) testing and verification methodology to ensure that patches have been implemented properly.

Category	Sub-Category	Description
Security Policy Compliance Monitoring	Vulnerability Management	The Contractor must: a) report any MWS security issues to GC immediately upon learning of their existence; b) track identified security issues in the MWS; and c) report progress to GC until each security issue is fixed or mitigated.
Planning	System Security Plan	Within 45 days after contract award, the Contractor must provide a draft System Security Plan (SSP). The Contractor must develop a security plan for the information system that: a) Is consistent with the Contractor's enterprise architecture; b) Explicitly defines the authorization boundary for the system; c) Describes the operational environment for the MWS; d) Describes the policies and associated requirements for MWS components.; e) Describes relationships with or connections to other information systems; f) Provides an overview of the security control requirements for the system; g) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and h) Is reviewed and approved by the GC prior to plan implementation. The Contractor must review the security plan for the information system on an annual basis. The Contractor must update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments..
Planning	Privacy Impact Assessment	Within 45 days of contract award, the Contractor must actively participate in the conduct of a privacy impact assessment on the MWS information system in accordance with the TBS Privacy Impact Assessment Policy. Contract deliverable.
Risk Management	Authorization Maintenance	The Contractor must maintain the MWS security authorization state through continuous monitoring and annual audit of the implemented security requirements within the MWS Service to determine if the security requirements in the information system continue to be effective over time in light of changes that occur in the MWS Service and its operational environment. The Contractor must provide evidence to support authorization maintenance activities, within 30 days of a request by GC, following all changes to the MWS Service Infrastructure within the Contractor’s control. The Contractor must update security operating procedures as part of authorization maintenance within 30 days of a request by GC.

Category	Sub-Category	Description
Risk Management	Security Assessments - Independent Assessment	The Contractor must employ an independent assessor or assessment team to conduct an assessment of the security controls in the MWS information system.
Risk Management	Security Assessment - Plan of Action and Milestones	The Contractor must develop a plan of action and milestones for the MWS 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 must update existing plan of action and milestones on a quarterly basis, or as specified by the GC, based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. Based on issues discovered during the security assessment
Risk Management	Continuous Monitoring	The Contractor must ensure and demonstrate that the security posture of the MWS Services is maintained by continuously: a) monitoring threats and vulnerabilities; b) monitoring for malicious activities and unauthorized access; and c) where required, taking proactive countermeasures, including taking both pre-emptive and response actions to mitigate threats.
Data Security	Data Governance - Non-Production Data	The Contractor must provide the same security provisions for the development, system test, acceptance test and training environment as those used in the production environment.
Data Security	Data Protection	The Contractor must ensure that the integrity and confidentiality of MWS Data is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by the GC.
Data Security	Data Loss Prevention	The Contractor must implement security mechanisms to prevent data leakage approved by the GC.
Identity, Credential and Access Management	ICAM	The Contractor's Interim ICAM solution must, for system and privileged access, be capable of the following: a) granting access to authorized users based on username and password. b) Validating credentials at each login; c) uniquely identifying and authenticating users and administrators; d) preventing access to MWS components or resources without identification, authentication, and authorization; and e) using strong passwords (e.g., minimum character length of 8 characters, multiple types of characters) and be based on GC password aging and reuse policy).
Identity, Credential and Access Management	ICAM	The Contractor's Interim ICAM Solution must remove all credentials once fully migrated to Canada's GC ICAM solution.

Category	Sub-Category	Description
Identity, Credential and Access Management	Authentication	The Contractor must obscure feedback of authentication data (e.g., masking password fields) during the authentication process.
Identity, Credential and Access Management	Access Management	The MWS must display a configurable logon page on the login page of any web-based application.
Identity, Credential and Access Management	Logging and Auditing	The MWS must log the following events: a) successful authentication; and b) unsuccessful authentication.
Identity, Credential and Access Management	Security Management Access	The MWS must use Transport Layer Security (TLS) and information encryption for application-level data transmission purposes.
Network and Communication Security	Encryption	The Federal Information Processing Standard (FIPS) 140-2 specifies the security requirements that must be satisfied by a cryptographic module utilized within a security system, sub-system, or component protecting protected information. Prior to using any cryptographic module, the contractor shall provide a copy of the relevant FIPS 140-2 validation certificate as evidence of FIPS 140-2 validation, or, as a minimum, the validation certificate number. The Contractor must also ensure that the FIPS 140-2 approved cryptographic solutions (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for the MWS use GC approved cryptographic algorithms and cryptographic key sizes and crypto periods.
Network and Communication Security	Boundary Protection and Zoning	The Contractor must monitor and analyze network traffic, in real time, to detect attacks and evidence of compromised MWS Infrastructure components. Specifically, the MWS Service Infrastructure must monitor and control communications at the external boundary of the system and at key internal boundaries within the system. The Contractor must detect attacks including but not limited to: a) denial of service attacks; b) malware; c) social engineering; d) unauthorized intrusion or access; e) information breach; and f) all other security breaches or cyber threats targeting Canada.
Network and Communication Security	DNS	The MWS must be configurable to use DNSSEC for DNS queries.

Category	Sub-Category	Description
Network and Communication Security	Technology Refresh	The Contractor must: a) Comply with technology refresh requirements as required by the GC to ensure security requirements and service level agreements (SLA) are met. b) Comply with the GC requirements that software within the Contractor's Boundary will never be more than two versions behind.
Security Policy Compliance Monitoring	Malware Protection	The Contractor must implement and maintain network protection capabilities to detect and eliminate malicious software and/or unauthorized external connection attempts on network monitoring devices, servers, peripheral devices, and desktop workstations. The MWS must scan all MWS data, for the presence of malware. There should be an active host-protection mechanisms on servers that are actively scanning malware at a frequency greater than once a month. All files uploading to the web service are scanned by MWS.
Security Operations	Logging and Auditing	The MWS must provide the ability to track system and detailed user activity and capture events and audit logs to a centralized audit log system. The MWS audit log system must: a) include centralized and time-synchronised logging of allowed and blocked MWS activity with regular log analysis; b) keep 3 months of events and logs online; c) keep events and logs associated with a security Incident for at least 2 years; and d) store logs for at least 6 months.
Security Operations	Logging and Auditing	The MWS audit records must include: a) what type of audit event occurred; b) when (date and time) the audit event occurred; c) where the audit event occurred; d) the audit source of the event; e) the outcome (success or failure) of the audit event, and f) the identity of any user/subject associated with the audit event.
Security Operations	Logging and Auditing	The Contractor must implement an audit review process that includes: a) review and analysis of MWS audit records annually and within 20 Federal Government Working Days of a request by GC for indications of inappropriate or unusual activity; b) report findings of the audit review process to GC within 10 Federal Government Working Days of completion of the audit, and c) adjust the level of audit review, analysis, and reporting when there is a change in risk or as requested by GC.

Category	Sub-Category	Description

Security Operations	Security Incident Management	The Contractor, for Security Incidents tickets, must include the following information:
		a) Incident Ticket number;
		b) Incident Ticket opened/closed date;
		c) threat vector;
		d) targeted service/protocol/application;
		e) origin/source of attack, and
		f) type and description of attack/event;
		g) whether attack appears to have been successful and impact;
		h) attack scope (to an organization and/or across many organizations);
		i) estimated number of systems affected by organization;
		j) list of systems affected by organization;
		k) apparent source/origin of attack/Incident/event;
		l) date/time of attack/Incident/event;
		m) estimated injury level /sector;
		n) estimated impact level;
		o) attack/Incident/event duration;
		p) actions taken;
		q) status of mitigations, and
		r) applicable logs or evidence data

Security Operations	Security Incident Management	The Contractor must install an automated technical solution (for example, a web-application firewall) that detects and prevents web-based attacks (e.g. injection flaws, buffer overflows, cross-site scripting, etc.) in front of public-facing web applications, to continually check all traffic
Personnel Security	Personnel Screening	• The Contractor must screen individuals prior to authorizing access to the information system in accordance with the *TBS Personnel Security Standard*. • The Contractor must rescreen individuals according to conditions requiring rescreening. • For Foreign Contractors, see Part 6, 6.1(a) – Security and Privacy Requirements for Foreign Suppliers (Personnel Screening).
Personnel Security	Personnel Termination	• The Contractor, upon termination of individual employment, must terminate information system access. • The Contractor, upon termination of individual employment, must conduct exit interviews. • The Contractor, upon termination of individual employment, must retrieve all security-related organizational information system-related property. • The Contractor, upon termination of individual employment must retain access to organizational information and information systems in accordance with the TBS Personnel Security Standard.

Category	Sub-Category	Description
Personnel Security	Access Agreements	• The Contractor must ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access. • The Contractor must review/update the access agreements when necessary.
Personnel Security	Access Agreements	• The Contractor must ensure 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; (b) Satisfy associated personnel security criteria; and (c) Have read, understood, and signed a nondisclosure agreement.
Personnel Security	Third-Party Personnel Security	• The Contractor must establish personnel security control requirements including security roles and responsibilities for third-party providers. • The Contractor must document personnel security control requirements. • The Contractor must monitor provider compliance. • The Contractor must ensure security screening of private sector organizations and individuals who have access to Protected information and assets. • The Contractor must explicitly define government oversight and end-user roles and responsibilities relative to third-party provided services in accordance with the TBS Security and Contracting Management Standard.
Personnel Security	Personnel Sanctions	• The Contractor must employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.
Audit & Accountability	Audit Reduction and Report Generation	• The Contractor must ensure that the information system provides an audit reduction and report generation capability.
Audit & Accountability	Audit Reduction and Report Generation	• The Contractor must ensure that the information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.

Category	Sub-Category	Description
Contingency Planning	Alternate Storage Site	• The Contractor must establish an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. • The Contractor must identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.