Employment and
Social Development Canada

Emploi et
Développement social Canada

REQUEST FOR INFORMATION FOR A LINGUISTIC SERVICES REQUEST MANAGEMENT SYSTEM (LSRMS) FOR EMPLOYMENT AND SOCIAL DEVELOPMENT CANADA

Request for information (RFI) No.: 100026030

Issued : 2024-03-14

Question Deadline : 2024-04-05

Addenda (answers provided) deadline : 2024-04-10

Submission Deadline : 2024-04-13

Address Inquiries to RFI contact : David Priori (nc-solicitations-gd@hrsdc-rhdcc.gc.ca)

TABLE OF CONTENTS

REQUEST FOR INFORMATION FOR A LINGUISTIC SERVICES REQUEST MANAGEMENT SYSTEM (LSRMS) FOR EMPLOYMENT AND SOCIAL DEVELOPMENT CANADA

1.0   Background

Employment and Social Development Canada (ESDC) is soliciting industry feedback for a web-based Linguistic Services Request Management System (LSRMS) Solution, to replace its current solution.

ESDC has had a LSRMS Solution (Multi-Trans Prism) for many years that provided a secure and complete LSRMS Solution that performed and managed ESDC's end-to-end translation and interpretation services, processes and activities in an integrated manner with **Protected B** security level classification for information, assets and business intelligence.

Unfortunately, the current LSRMS Solution is no longer supported by its provider and ESDC needs to replace the Solution to meet its linguistic requirements across the department. The urgency is to replace MultiTrans Prism, which is the translation memory software. It is important to know all the features that are currently available for translation memory software. In addition, ESDC is interested in learning about the functionality currently available for the request management platforms of LSRMS Solutions, the workload and workflow management tools and what tools can be included in the LSRMS Solutions that combines the translation memory and AI-driven translation that could be accessible to non-linguistic personnel. The tool would need to first draw on the translation memory, for consistency and quality purposes, and once it has gotten everything it could out of the translation memories, the non-translated parts of the text would be translated through neural translation (AI).

2.0   Purpose of the RFI

The purpose of this RFI is to:

a. To identify what is the current state of the functionality and technology available for a Linguistic Services Request Management System Solution and in particular for the translation memory software;
b. To determine if there is an existing commercial off the shelf (COTS) product that would be able to meet a majority of the non-technical and technical requirements for a Solution;
c. To assess what would be the potential development cost and time required to fully meet the requirement if there is not an existing COTS product that meets the majority of the requirements; and
d. To refine planning and cost estimates.

3.0   Overall components and services of the current LSRMS Solution

The current LSRMS Solution includes:

1. Portal for the resources and clients;

2. Workflow management;
3. Workload management;
4. Terminology management;
5. Computer Aided Translation (CAT) tools;
6. Quality Assurance tools;
7. Analytics, Reporting and Auditing functions;
8. Financial Management Interoperability;
9. Security management;
10. Scalability over the life of the existing contract; and
11. Document management.

The current Solution has 2 components: Flow which is hosted on the Contractor's servers and is used to create translation requests and the system which handles the textbase/ termbase storage which is hosted internally at ESDC. Translators use the internal component for their work. The component which is hosted on the vendor's servers is and must continue to be entirely hosted in Canada which includes Contractor or Sub-Contractor data centres, the underlying service infrastructure, network, database, web, application servers, operating systems, virtual machines, and storage. In the future, attributes that are of interest include the functionality to search based on reportable fields, document attributes, and metadata.

The LSRMS Solution is and is expected to continue to be:

- Customizable web-based and interactive tool that can be readily configured by users to reflect their specific requirements;
- Allow for the definition of user roles, access rights and permission for the solution, suite of tools, features and functionalities;
- Have workflow and business rules to be configured by the User to support a wide variety of processes, activities and functions;
- Allow for the effective management of the metadata and data for example any and all data will be entered once and validated within the solution, with the ability to re-use and leverage data throughout the solution and across its functionalities;
- Allow for seamless data sharing within the solution and other related systems hosted by the Contractor;
- To support the re-use of commonly required data in a secure manner across the solution and other ESDC systems; and
- Allow for constant change and real-time access to data, reporting and analytic information to support the effective management and business decision-making, monitoring and tracking of processes and performance.

Key components of the current and future Solution are:

a. **Translation Memory** which:

- Stores documents so that translators/editors/ linguistic specialists can build a textbase, including translations done in the past or from sources external to the Solution,
- Includes a termbase, for terminology;
- Allows for maintenance of the text and termbases (correction and manipulation of text within the memory itself, rather than having to go back into the file to correct a mistake and download it again in the translation memory);

- Is accessible off network (in case the VPN is not accessible for some reason); and
- Includes all the basic features of a translation memory.

b. **Request Management Platform** which:

- Allows for management of requests, along with clients and providers profiles (updating, editing, suppression). It has to be accessible off network.

c. **Workflow and Workload Management** which:

- Allows a User with the proper role, access rights and permissions to configure the Workflow to support a variety of processes, activities and functions.

d. **Tools for non-linguistic personnel** which:

- Combines the translation memory and AI-driven translation that could be accessible to non-linguistic personnel (such as developers). The tool would first draw on the translation memory, for consistency and quality purposes, and once it has gotten everything it could out of the translation memories, the non-translated parts of the text would be translated through neural translation (AI) and stored in the Translation Memory (for future consultation and review).

4.0   Availability, Transaction Volume, Data and Privacy

Availability:

The Solution currently is required to be accessible to the User 24 hours a day x 7 days a week. It is expected that this will need to continue in the future.

Number of Transactions:

In terms of the volume of current transactions, on an annual basis **there are thousands of translation requests per year (all linguistic services teams combined) and hundreds of thousands (at least) of texts stored in the memory, not including the terminology bases.**

Data and Information:

All data and information that is migrated, archived, backed up, stored on media, created and or associated to the LSRMS Solution currently and in the future resides and will remain the property of Canada at all times and as such is required to be encrypted based on Government of Canada Security requirements. The format of the data must remain in its native format and must not be converted to a proprietary format as ESDC must have the ability to access its data at any time.

In the future, ESDC would be interested in having functionality for a User with the proper role, access rights, and permission to be able to tailor and configure the User interface and attributes, control business behaviour (such as conditions that should be met before User can amend a service request) using business rules and input validation.

5.0   System Access and User Interface

Web-based Access: The LSRMS Solution features and functionalities for Translation, Terminology and Interpretation are currently and will require in the future to be Web-based and include portals (client, internal and external resource(s)), dashboards, workflow, workload, terminology, security management, computer aided translation (CAT) tools, Translation memories, TermBase, analytics, reports, and business intelligence.

In the future for the User Interface, ESDC would be interested in the ability to configure the User Interface by:

a) Adding new attributes or modify functionality of existing attributes;
b) Setting attribute types such as number, free text, pick list, and Boolean;
c) Setting attribute GUI position and tab order;
d) Setting attribute level behaviour and properties such as labels, mouse over help, mandatory/optional, visibility, default value;
e) Creating business rules and input validation;
f) Setting print layout;
g) Specifying which data attributes are pre-populated when the artifact is created (such as prepopulate User data from the requester's User profile on a requisition when a request is created);
h) Specifying the behaviour using business rules, validation rules that apply when the business process is modified;
i) Tracking and be able to display changes (history) for each input and business transaction;
j) Modifying information, changing workflow approval or denial, changing submissions to external resource(s), and confirmation;
k) Configuring the User interface layout of a portal; and
l) Identifying and submitting to the Contractor changes to hard coded values, attributes, and data fields in the User interface.

The LSRMS Solution component's interface provides brief User instructions and tips in a consistent manner across all controls and displays. The LSRMS Solution component's interface follows a standard, theme, and text tone across the component. It supports customizable colour selection and other visual configuration options to enable ESDC to brand the interface.

Availability in English and French:

The entire LSRMS Solution is currently available in both of Canada's **Official Languages** and includes the following; web and application User interface, system, tools, documentation, training, service desk. The LSRMS Solution tools and applications provide all Users with the ability to set a preferred default language for their use, if the User has not indicated a preference. In the future, the Solution User interface elements should be available in both of Canada's Official Languages and include:

a) Input Controls: checkboxes, radio buttons, dropdown lists, list boxes, buttons, toggles, text fields, date field, text terminal window;
b) Navigational Components: breadcrumb, slider, search field, pagination, slider, tags, icons, tabs;
c) Informational Components: tooltips, icons, progress bar, notifications, message boxes or windows, dialog box, modal windows (pop up);
d) Menus: menu bar, menu, context menu, extra menus, primary and secondary menus:
e) Browser: such as Edge, Chrome, and Firefox;

f) Landing page, homepage, welcome or login page - Should be configurable but at this point in time Protected B information is not allowed; and

g) When using the LSRMS Solution tools and applications the User should be able to toggle between either of Canada's Official Languages.

It is expected that in the future, the LSRMS Solution tools and applications will allow certain input control fields to be entered in both Canada's Official Languages, regardless of the individual User's language of choice. It should be capable of integrating both Canada's official language information in its database(s). Reports generated from the LSRMS Solution, by Users and resource(s) should also be available in both Canada's Official Languages.

6.0 Description and Number of current Users

There are four types of Users currently accessing the Solution:

a. System Administrators for the Solution who perform typical roles of assigning rights and privileges to the various types of Users;

b. Full-fledged users (**translators/editors/ linguistic specialists only**) who use translation memory and maintain and feed the bases. There are approximately 100 to 150 of this type of User using the system concurrently and they are considered the most important user for any future Solutions. This type of User is expected to be the minimum number of this type of User. The number is expected to grow.

The services used by the Translators/ Linguistic Specialists include:

Service	Description
Adaptation	Translating a document and making changes to tailor the message to its target audience. Also includes coming up with possible translations for programs, initiatives, projects, etc., as well as translation of transcriptions.
Administrative services	Handling a request that requires an unusual amount of administrative processing. Example: request with many files, processing files that are complex and/or require extra processing (such as PDF and JPG files), merging files, searching for already translated documents.
Comparative revision	Carefully comparing a translation with the original text and correcting the content and style of the translation.
Editing (unilingual)	Improving an original text by correcting the grammar or style or by suggesting solutions to make the text easier to read and understand.
Light editing	Reviewing of a text to correct basic errors, as well as flagging illogical or unclear sentences and inconsistencies.
Linguistic advice	Providing advice on translation problems and language questions and issues (grammar, style, punctuation, terminology, etc.) without a document being necessary.
On-site translator	Providing the services of a language professional who can work exclusively and autonomously for a client or a group of clients in our offices.
Plain language editing	Reworking and restructuring a text to make it easy to read, understand and use. Working in close collaboration with the author, communications advisor or subject-matter expert.
Project management	Planning, organizing, directing, controlling and monitoring a complex linguistic or translation project.

Proofreading	Reading a text, identifying any errors or typos, and indicating changes to be made.
Terminology services	Developing customized glossaries (for the use of our team, clients and branch), participating to terminology committees and projects.
Translation	Rewriting a text in another language, taking into account the tone, style and terminology used by the author.
Translation of modified documents	Translating changes made to an already translated document.
Translator on stand-by	Providing the services of a language professional who can be reached on short notice at any time for a specific period to carry out a client's work. The translator can carry out other activities during this time.
Writing assistance	Drafting a text in collaboration with a client and providing linguistic advice on translation problems and language issues (grammar, style, punctuation, terminology, etc.)

c. Coordinators/project managers, managers/administrators, providers (internal and external), clients (non-linguistic people) who typically access the management platform to make the requests that are sent to the Translators. through the use of Multi Trans Flow and Terminotix. There are approximately 50 – 100 of this type of User.

d. Non-linguistic personnel who need ad-hoc translation or urgent translation that their own linguistic services team is not able to handle, for one reason or another. They require access to a mix of the translation memory/AI-driven translation part of the Solution for the work that is not already translated by the translation memory of the Solution. There are approximately 200 of this type of User but dependent upon the tools available in a new Solution, this type of User could grow significantly. Depending upon the tools available in a new Solution, the number of this type of User may significantly expand from the current base.

7.0   ESDC Technical Environment

The LSRMS Solution must be accessible using Microsoft Windows 10 and 11, Sharepoint and Office 365 and through various browsers such as Edge, Chrome, and Firefox. All relevant financial information in the Solution is transferred between the LSRMS Solution and SIGMA (SAP), using file import and export functionality to and from a secure landing pad.

The LSRMS Solution currently provides the functionality to:

a) Import data, files, reports, analytics, query results into LSRMS Solution in various formats that include; MS Word (doc, docx), MS Excel (xls, xlsx), txt, pdf, xml, tmx, tbx, xliff, and csv; and
b) Export data, files, reports, analytics, query results from LSRMS Solution in various formats that includes; MS Word (doc.docx), MS Excel (xls, xlsx), txt, pdf, xml, tmx, tbx, xliff, and csv.

It supports Secure File Transfer Protocol.

The current Solution provides secure log-in access for clients, internal and external resources based on the government of Canada IT Security Standards and security control profiles.

The current Solution is compliant with:

a. The current TBS Directive on the Management of Projects and Programs: Directive on the Management of Projects and Programmes- Canada.ca;
b. Standard on Web Accessibility: Standard on Web Accessibility- Canada.ca;
c. Web Content Accessibility Guidelines, Version 2, Level AA (WCAG 2 AA);
d. The TBS Policy on Privacy Protection and related Privacy Directives;
e. Information Technology Standard Guideline (ITSG) - 33 on IT Security Risk Management;
f. The Government of Canada Cloud Security (GC cloud adoption strategy, GC Cloud Guardrails, GC Tiered Assurance model, cloud security risk management ITSM.50.062, security controls, trust boundaries, standard interfaces and security protocols, techniques used for token management – authentication and authorization, encryption methods, security logging); and
g. Cloud Security Assessment and Authorization ITSP.50.105.

8.0   Request for Information (RFI)

This is not a bid solicitation. This RFI will not result in 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 in this RFI.

8.1   Nature and Format of Responses Requested

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

8.2   Response Costs

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

8.3   Treatment of Responses

Use of Responses: Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify procurement strategies or any draft documents contained in this RFI. ESDC will review all responses received by the RFI closing date. ESDC may, in its discretion, review responses received after the RFI closing date.

Review Team: A review team composed of representatives of ESDC will review the responses. ESDC reserves the right to hire any independent consultant or use any Government resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

Confidentiality: Suppliers who respond should mark any portions of their response that they consider proprietary or confidential. ESDC will handle the responses in accordance with the Access to Information Act.

Suppliers are advised that any information submitted to ESDC in response to this RFI may be used by ESDC in the finalization of a competitive solicitation.

All industry consultations will be documented, and this information is subject to the Access to Information Act. Suppliers should identify any submitted information that is to be considered as either company confidential or proprietary. ESDC will not reveal any designated confidential or proprietary information to the public and/or third parties.

Follow-up Activity: ESDC may meet with the Respondents who respond to the RFI and indicate in their responses that they wish to participate in a follow-up virtual meeting. At this meeting each Respondent to the RFI will be asked demonstrate the functionality of their Solution and in particular to identify how the translators/editors/ linguistic specialists would access and use the Solution. Notification of the date and time of the follow-on virtual meeting will be provided to the suppliers a minimum of 10 working days in advance of the meeting and the meeting is expected to be held during regular working hours and last no longer than 90 minutes.

Provision of Supporting Documentation

Any other documentation that a Supplier believes will provide relevant information of their proposed Solution, tool suite or supporting third party applications is welcome.

8.4   Contents of this RFI

This RFI contains specific questions addressed to industry representatives and provides a respondent submission form for representatives to fill out.

8.5   Format of Responses

a)   **Cover Page**: If the response includes multiple volumes, suppliers who respond 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 supplier.

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

- the title of the supplier's response and the volume number;
- the name and address of the supplier;
- the name, address and telephone number of the supplier's contact;
- the date; and
- the RFI number.

Numbering System: Suppliers who respond 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.

8.6   Enquiries

Because this is not a bid solicitation, ESDC 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:

Contracting Authority: David Priori
E-mail Address: NC-SOLICITATIONS-GD@hrsdc-rhdcc.gc.ca

8.7   Submission of Responses

a) **Time and place for submission of responses**: Suppliers interested in providing a response should email their response to the Contracting Authority identified above by the time and date indicated on the cover page of this document.
b) **Responsibility for timely delivery:** Each supplier who responds is solely responsible for ensuring its response is delivered on time to the correct location.

Annex A Questions for Industry

A1. General Questions

Question	Supplier Information
1. Provide a brief description of your company, headquarter location, the number of staff you employ, how long your company has been in business, and identify the number of facilities and locations (including office space(s), data storage facilities, location(s) of cloud servers, etc.).	
2. Identify the types of linguistic services products and services you provide (e.g., etc.), how long these Solutions have been provided and the typical client and number of Users for each type of Solution.	
3. Provide the name and history of the proposed Solution and provide an overview of the functionality of the proposed Linguistic Services Request Management System (LSRMS) Solution you would offer to ESDC as a replacement solution. Identify if the proposed Solution has been provided to any Canadian public sector clients, when and for how long.	

4. Identify for your proposed Solution which of the following functionality is included without any additional development and provide details on the specific functionality:
 	
  a. Portal for the resources and clients;
  b. Workflow management;
  c. Workload management;
  d. Terminology management;
  e. Computer Aided Translation (CAT) tools;
  f. Quality Assurance tools;
  g. Analytics, Reporting and Auditing functions;
  h. Financial Management Interoperability;
  i. Security management;
  j. Scalability over the life of the existing contract; and
  k. Document management.	

Question	Supplier Information
5. Beyond the functionality identified in support of Question 4 above, does the proposed solution have any additional functionality or features not listed above that the respondent feels would be of interest by ESDC.	
6. Identify how developmental work will be performed (e.g., with in-house capabilities, or external contracting), and if external contracting will be used, who will retain ownership of development source codes.	
7. Identify if there are any limitations on the number of transactions that can be managed by your proposed Solution on a daily basis or by a single User?	
8. Identify the availability requirements for the Solution to optimally operate.	
9. Identify the approach provided to clients for your proposed Solution in terms of: a) Implementation; b) Customization; c) Training; d) User and System Documentation; and e) Support.	
10. Provide details on where the Solution is hosted, and your data retention policy (e.g., where is data stored, on local servers, on cloud services, etc.; according to the policy, who owns the data?	
11. Describe the data security allowance of your Solution and whether your company has secured any IT audits compliant to Canadian federal government standards.	

Question	Supplier Information
Identify which security certifications and attestation standards (FedRAMP, ISO, SOC, etc.) the organizations have. For more information on the security standards for cloud required by the Government of Canada, see Annex B attached to this RFI.	
12. Identify the licensing model that would be required for your proposed Solution. Is there any minimum or maximum contract period typically?	
13. Describe the annual Software Life Cycle approach that will be recommended for the proposed Solution and how Product Life Cycle will be determined? Include how clients are notified and the typical advance notification they receive?	
14. Provide a description of the Technical Environment within which the proposed Solution optimally operates?	

A2. Specific Questions related to the Non-Technical and Technical Requirements

Question	Supplier Information
1. Identify the type of Users and how they would access the proposed Solution in light of the current ESDC Solution.	
2. Describe subject matter specialists such as translators/editors/ linguistic specialists typically use the proposed solution and how they would be able to provide the types of services identified in Article 6.0 of the RFI.	

Question	Supplier Information
3. Provide a description of all of the features and if possible, product specifications for the Translation Memory Component of the proposed Solution, including what is included, how it is accessed etc.	
4. Provide a description of all of the features and if possible, product specifications for the Request Management Platform of the proposed Solution and how the management of requests can be typically managed for the proposed Solution.	
5. Provide a description of all of the features and if possible, product specifications for the Workflow Management of the proposed Solution.	
6. Identify what tools are included in the proposed Solution for non-linguistic personnel to use to undertake for example quick translations.	
7. Identify the language(s) that the support, User and system documentation, user tutorials/ training and User screens without any additional development to the Solution.	
8. Describe the functionality that the proposed Solution provides to ensure the quality of User output e.g. highlighting incomplete requests etc.	
9. Describe the audit and reporting functions available as part of the proposed Solution.	
10. Confirm if the proposed Solution meets the Web Content Accessibility Guidelines, Version 2.2 level AA (WCAG 2.2 AA). If possible, identify the timeframe within which the Solution's Information and Communication Technology (ICT) was accessed by a third party or a qualified accessibility specialist.	

Question	Supplier Information
11. Identify if the Respondent has professional services available to help with the implementation of the proposed Solution, assist with any required modifications to the Solution, and address accessibility requirements.	
12. Provide a description of the feedback mechanism in place to receive tickets related to the use of the Solution, possible defects etc. and the service levels to have them resolved. Confirm the language in which the process will work.	
13. Identify if there are any components or the proposed Solution for which the respondent does not have control on the source code.	

Annex B – Schedule 1 – Security Obligations for Commercial Cloud Services (up to and including Protected B)

<center>(for information purposes only)</center>

General

    1.1   *Purpose*

The purpose of this Schedule is to set forth the obligations of the Contractor relating to the proper management of Canada's Data, including protection from unauthorized modification, access or exfiltration, in accordance with the Agreement, this Schedule, and the Contractor's Security Measures (collectively, the "**Security Obligations**").

    1.2   *Flow-Down of Security Obligations*

The obligations of the Contractor contained in these Security Obligations must be flowed down by the Contractor to any Sub-processors and/or Subcontractors to the extent applicable.

    1.3   *Change Management*

The Contractor must, throughout the Contract, take all steps required to update and maintain the Security Requirements as needed to comply with the security best practices and industry standards as set forth in this Schedule.

The Contractor must advise Canada of all changes that materially degrades or may have an adverse affect to the Cloud Services offerings in this Contract, including technological, administrative or other types of changes or improvements. The Contractor agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

Acknowledgments

The parties acknowledge that:

(a)   Canada's Data is subject to these Security Obligations.

(b)   Notwithstanding any other provision of this Schedule, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Canada's Data.

(c)   The Contractor must not have or attempt to gain custody of Canada's Data, nor permit any Cloud Services Personnel to access Canada's Data prior to the implementation of the Security Requirements as required under this Schedule on or before Contract Award.

(d)   Security Obligations apply to **Commercial Cloud Services** (up to and including Protected B / Medium Integrity, Medium Availability or Medium Injury), unless otherwise specified.

Securing Canada's Data

(1)   The Contractor must protect Canada's Data from unauthorized access, modification, or exfiltration. This includes implementing and maintaining appropriate technical and organizational security measures including information security policies, procedures, and security controls to preserve the confidentiality, integrity, and availability of Canada's Data.

Roles and Responsibilities for Security

(1)   The Contractor must clearly delineate the roles and responsibilities for the security controls and features of the Cloud Services between the Contractor and Canada. This includes, at a minimum, the

roles and responsibilities for: (i) account management; (ii) boundary protection; (iii) asset and information system backup; (iv) incident management; (v) System monitoring; and (vi) vulnerability management.

(2)   The Contractor must provide to Canada an up-to-date document that delineates the roles and responsibilities: (i) at contract award; (ii) on an annual basis; (iii) when there are significant changes to such roles and responsibilities as a result of a Change to the Cloud Services; or (iv) upon request of Canada.

Third-Party Assurance: Certifications and Reports

(1)   The Contractor must ensure that Canada's Data, Contractor Infrastructure (including any IaaS, PaaS or SaaS Service provided to Canada) and Service Locations are secured with appropriate security measures that comply with the requirements set forth the Contractor's security practices and policies.

(2)   The Contractor must demonstrate that the measures comply with the requirements set forth in the following certifications and audit reports by providing independent third-party assessment reports or certifications that addresses each service layer (e.g. IaaS, PaaS, SaaS) within the Cloud Service offering, including:

(a)   ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Certification achieved by an accredited certification body (or subsequent versions); AND

(b)   ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services achieved by an accredited certification body (or subsequent versions); AND

(c)   AICPA Service Organization Control (SOC) 2 Type II Audit Report 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality - issued by an independent Certified Public Accountant.

(3)   Each certification or audit report provided must: (i) identify the legal business name of the Contractor or applicable Sub-processor; (ii) identify the Contractor's or Sub-processor's certification date and the status of that certification; (iii) identify the services included within the scope of the certification report. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

(4)   Each audit will result in the generation of an audit report which must be made available to Canada. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor and provide Canada with supporting evidence of the remediation measures taken or confirmation from the auditor that issues have been remediated to the satisfaction of the auditor.

(5)   Each SOC 2 Type II audit report must have been performed within the 12 months prior to the start of the contract. A bridge letter may be provided to demonstrate that the Contractor is in process of renewal where there is a gap between the service organization's report date and the user organization's year-end (i.e., calendar or fiscal year-end).

(6)   The Contractor is expected to maintain its certification of ISO 27001, ISO 27017, and/or SOC 2 Type II as applicable for the duration of the contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

Auditing Compliance

(1)   The Contractor must ensure that privacy and security audits of the security of the computers, computing environment and physical data centers that it uses in processing and protecting Canada's Data are conducted as follows   :

   (a)   Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

   (b)   Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and

   (c)   Each audit will be performed by independent, third-party auditors that (i) are qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conform to the ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

(2)   Each audit will result in the generation of an audit report that must be made available to Canada. The audit report must clearly disclose any material findings by the third-party auditor. The Contractor must, at its own expense, promptly remediate issues and correct deficiencies raised in any audit report to the satisfaction of the auditor.

(3)   Upon request of Canada, additional supplementary evidence from the Contractor, including system security plans, designs, or architecture documents that provide a comprehensive system description, may be provided by the Contractor or a Sub-processor to supplement the certification and audit reports described in Section 5 (Third Party Assurance) in order to demonstrate the Contractor's compliance with the required industry certifications. This includes the situation where the Contractor is a SaaS or PaaS provider using physical data centers that are provided by a third-party IaaS provider.

Cloud Service Provider (CSP) IT Security Assessment Program

(1)   The Contractor must demonstrate compliance with the security requirements selected in the Canadian Centre for Cyber Security (CCCS) Annex B Cloud Control Profile – Medium of the Guidance on Security Categorization of Cloud-Based Services (ITSP.50.103) (https://www.cyber.gc.ca/en/guidance/guidance-security-categorization-cloud-based-services-itsp50103) for the scope of the Cloud Services provided by the Contractor. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third-party assessments.

   Compliance will be assessed and validated through the CCCS CSP Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100).

   The Contractor must demonstrate that they participated in the process by successfully on-boarded, participated in, and completed the program. This includes providing the following documentation:

   (i)   A copy of the most recent completed assessment report provided by Canada; and
   (ii)   A copy of the most recent summary report provided by Canada.

   The Contractor should contact the procuring GC department for any additional information related to the CSP IT Assessment Program.

    It is the continuous obligation of the Contractor of the proposed Cloud Services to notify GC procuring department when there are significant changes to its delivery of the IT Security services supporting the Contractor offering.

(2)   In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with Section 5 - Third-Party Assurance and Section 7 - Cloud Service Provider (CSP) IT Security Assessment Program, sub-sections (1) and (2) the SaaS provider must provide

Canada with a copy of an email provided by the Canadian Centre for Cyber Security (CCCS) confirming that the Bidder has completed the CCCS CSP ITS Assessment Program. The email must state that the CSP has been assessed by the CSP ITS Assessment Program and that the CSP has received a final report with regards to the assessment. For any questions, CCCS can be contacted by email at contact@cyber.gc.ca.

Data Protection

(1)   The Contractor must:

    (a)   Implement encryption of data at rest for the Cloud Services hosting Canada's Data where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, in accordance with Section 13 - Cryptographic Protection.

    (b)   Transmit Canada's Data in a secure manner including ability for the GC to implement encryption for data in transit for all transmissions of Canada's Data, in accordance with Section 13 - Cryptographic Protection and Section 21- Network and Communications Security.

(2)   The Contractor must:

    (a)   Implement security controls that restricts administrative access to Canada's Data and Systems by the Contractor and provides the ability to require the written approval of Canada before the Contractor can access Canada's Data to perform support, maintenance or operational activities.

    (b)   Take reasonable measures to ensure that Contractor Personnel do not have standing or ongoing access rights to Canada's Data, and access is restricted to Contractor Personnel with a need-to-know, including resources that provide technical or customer support, based on approval from Canada.

(3)   The Contractor must not make any copies of databases or any part of those databases containing Canada's Data outside of regular service resilience capabilities and within approved regional spaces or zones within Canada.

(4)   The Contractor must not move or transmit approved copies outside of agreed upon service regions except when written approval is obtained from Canada.

(5)   Upon request of Canada, the Contractor must provide Canada with a document that describes all additional metadata created from Canada's Data.

Data Segregation

(1)   The Contractor must implement controls to ensure appropriate segregation of resources such that Canada's Data are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Cloud Services and Contractor Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support:

    (a)   The separation between Contractor's internal administration from resources used by its customers;

    (b)   The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another; and

    (c)   (For IaaS) Ability for the GC to support isolation within GC-managed tenant environment.

(2)   Upon request of Canada, the Contractor must provide Canada with a document that describes the approach for ensuring appropriate segregation of resources such that Canada's Data are not co-mingled with other tenant data, while in use, storage or transit.

Data Location

(1)   The Contractor must have the ability to store and protect Canada's Data, at rest, including data in backups or maintained for redundancy purposes. This includes the ability to isolate data in Canada in approved data centers. An approved Data Centre is defined as the following:

          (a)   A data centre that meets all security requirements and certifications identified in Section 30 for Physical (Data Centre / Facilities) Security;

          (b)   Ensures the infeasibility of finding a specific customer's data on physical media; and

          (c)   Employs encryption to ensure that no data is written to disk in an unencrypted form, in accordance with Section 13 - Cryptographic Protection.

(2)   The Contractor must certify that the delivery and provisioning of Cloud Services under this contract is from countr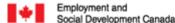ies within the North Atlantic Treaty Organization (NATO) (https://www.nato.int/cps/en/natohq/nato_countries.htm) or the European Union (EU) (https://europa.eu/european-union/about-eu/countries_en), or from countries with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

(3)   The Contractor must have the ability for Canada to isolate Canada's Data hosted in Cloud Services in data centers that are geographically located in Canada.

(4)   Upon request of Canada, the Contractor must:

          (a)   Provide the GC with an up-to-date list of the physical locations, including city, which may contain Canada's Data for each data centre that will be used to provide the Cloud services; and

          (b)   Identify which portions of the Cloud Services are delivered from outside of Canada, including all locations where data is stored and processed and where the Contractor manages the service from.

(5)   It is the continuous obligation of the Contractor of the proposed Cloud Services to provide written notification to Canada when there are updates to the list of physical locations which may contain Canada's Data.

Data Transfer and Retrieval

The Contractor must provide the capability including tools and services that allow Canada to:

       (a)   Extract all online, nearline, and offline Canada's Data, including, but not limited to, databases, object and file storage, system configurations, cloud activity logs, source code hosted in a Canada code repository, and network configurations such that any Canada End User can use these instructions to migrate from one environment to another environment; and

       (b)   Securely transfer all Canada's Data, including content data and associated metadata, in a machine-readable and usable format, including CSV format, and in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://library-archives.canada.ca/eng/services/government-canada/information-disposition/guidelines-information-management/pages/guidelines-file-formats-enduring-value.aspx).
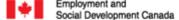
Data Disposition and Returning Records to Canada

(1)   The Contractor must securely dispose or reuse resources (e.g. equipment, data storage, files, and memory) that contain Canada's Data and ensure that previously stored data cannot be accessed by other customers after it is released. This includes all copies of Canada's Data that are made through replication for high availability and disaster recovery. The Contractor's disposal or reuse of resources must be aligned with one of the following:
(i) National Industrial Security Program Operating Manual (DoD 5220.22-M6); (ii) Guidelines for Media Sanitization (NIST SP 800-88); or (iii) Clearing and Declassifying Electronic Data Storage Devices (CSE ITSG-06). Upon request of Canada, the Contractor must provide a document that describes the Contractor's process for disposal or reuse of resources.

(2)   The Contractor must provide Canada with written confirmation that demonstrates successful erasing, purging or destruction of all resources, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once Canada discontinues its use of the Cloud Services.

Cryptographic Protection

The Contractor must:

(a)   Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic parameter sizes, key lengths and key crypto periods as specified in "Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information" (ITSP.40.111) and "Guidance on Securely Configuring Network Protocols" (ITSP.40.062) and remain consistent with any subsequent versions published on https://cyber.gc.ca/;

(b)   Use CSE-approved cryptographic algorithms that have been validated by the Cryptographic Algorithm Validation Program (CAVP) (https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program), with cryptographic parameter sizes and key lengths, as specified in "Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information" (ITSP.40.111) and remain consistent with any subsequent versions published on https://cyber.gc.ca/;

(c)   Ensure that the use of cryptographic algorithms, cryptographic parameter sizes, key lengths and crypto periods are configurable and can be updated within protocols, applications and services to be consistent with transition guidance in time to meet specified transition dates in "Cryptographic Algorithms for Unclassified, Protected A, and Protected B" (ITSP.40.111) and "Guidance on Securely Configuring Network Protocols" (ITSP.40.062) and remain consistent with any subsequent versions published on https://cyber.gc.ca/. Contractors should support the transition to quantum-safe cryptography in accordance with the guidance in ITSP.40.111 and ITSP.40.062 and their subsequent versions.

(d)   Ensure that Cryptographic Module Validation Program (CMVP)-validated Cryptographic Modules are used when cryptography is required, and are implemented, configured, and operated in in accordance with the cryptographic module security policy listed on the CMVP-validated modules list (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules), in an either approved or an allowed mode to provide a high degree of certainty that the CMVP-validated cryptographic module is providing the expected security services in the expected manner; and

(e)   Ensure that any cryptographic modules in use have an active, current, and valid CMVP certification. CMVP-validated products will have certificate numbers listed on the CMVP-validated modules list (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules).

Key Management

The Contractor must provide Canada with a key management service aligned with CCCS Guidance on Cloud Service Cryptography (ITSP.50.106) (https://cyber.gc.ca/en/guidance/guidance-cloud-service-cryptography-itsp50106) and their subsequent versions published on https://cyber.gc.ca/, that includes:

(a) Ability to create/generate and delete encryption keys if required by the GC.

(b) Definition and application of specific policies that control how keys can be used;

(c) Protection of access to the key material including prevention from Contractor access to the key material in unencrypted fashion;

(d) Ability to audit all events related to key management services, including Contractor access for Canada's review;

(e) Ability to securely import GC generated keys from GC-managed on-premise hardware security module (HSM) without exposure of key plaintext during the import process;

(f) Ability to prevent the Cloud Service Provider to recover plaintext copies of the GC generated keys; and

(g) Ability to delegate key use privileges for use by the Cloud Services used for the GC managed services.

Endpoint Protection

The Contractor must implement, manage, and monitor security-hardened endpoints with active host-based protections to prevent against malware, attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing.

Secure Development

The Contractor must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO 27034, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing. Upon request of Canada, the Contractor must provide a document that describes the Contractor's documented software and system development lifecycle approach and process.

Identity and Access Management

(1) The Contractor must have the ability for Canada to support secure access to Cloud Services including ability to configure:

(a) Phishing-resistant multi-factor authentication in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3) using GC-approved credentials;

(b) Role-based access;

(c) Access controls on objects in storage; and

(d) Granular authorization policies to allow or limit access.

(2)   The Contractor must have the ability to establish organization-wide defaults to manage tenant-wide policies.

Federation

(1)   The Contractor must have the ability for Canada to support federated identity integration including:

(a)   Support for open standards for authentication protocols such as Security Assertion Markup Language (SAML) 2.0 (or subsequent versions) and OpenID Connect 1.0 (or subsequent versions) where the End User credentials and authentication to cloud services are under the sole control of Canada; and

(b)   Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding Cloud Service user account(s).

Privileged Access Management

(1)   The Contractor must:

(a)   Implement access control policies and procedures that address onboarding, off-boarding, transition between roles, regular access reviews to identify excessive privileges, limitations and usage control of administrator privileges;

(b)   Manage and monitor privileged access to the Cloud Services to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services;

(c)   Restrict and minimize access to the Cloud Services and Canada's Data to only authorized devices and End Users with an explicit need to have access;

(d)   Enforce and audit authorizations for access to the Cloud Services and Canada's Data;

(e)   Constrain all access to service interfaces that host Canada's Data to uniquely identified, authenticated and authorized End Users, devices, and processes (or services);

(f)   Implement password policies to protect credentials from compromise by either online or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CCCS's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(g)   Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CCCS's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(h)   Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Canada's Data;

(i)   Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles;

(j)   Adhere to the principles of least privilege and need-to-know when granting access to the Cloud Services and Canada's Data;

(k)   Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Cloud Services and Contractor Infrastructure;

(l)   Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and

(m)   Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.

(2)   Upon request of Canada, the Contractor must provide a document that describes the Contractor's approach and process for managing and monitoring privileged access of the Cloud Services.

Remote Management

(1)   The Contractor must manage and monitor remote administration of the Contractor's Cloud Service that are used to host GC services and take reasonable measures to:

(a)   Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CCCS's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(b)   Employ cryptographic mechanisms to protect the confidentiality of remote access sessions, in accordance with Section 13 (Cryptographic Protection);

(c)   Route all remote access through controlled, monitored, and audited access control points;

(d)   Expeditiously disconnect or disable unauthorized remote management or remote access connections;

(e)   Authorize remote execution of privileged commands and remote access to security-relevant information.

(2)   Upon request of Canada, the Contractor must provide a document that describes the Contractor's approach and process for managing and monitoring remote administration of the Cloud Services.

Network and Communications Security

The Contractor must:

(a)   Provide the ability for Canada to establish secure connections to the Cloud Services, including providing data-in-transit protection between Canada and the Cloud Service using TLS 1.2, or subsequent versions;

(b)   Use up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in CCCS's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062configuring-network-protocols-itsp40062) and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111);

(c)   Use correctly configured certificates within the TLS connections in accordance with CCCS guidance.

(d)   Provide the ability for Canada to implement network access controls and security rules that restrict access to only authorized devices and network locations to Canada resources.

Logging and Auditing

(1)   The Contractor must implement log generation and management practices and controls for all Cloud Service components that store or process Canada's Data, and that conform with industry standards and best practices, such as those found in NIST 800-92 (Guide to Computer Security Log Management), or an equivalent standard approved by Canada in writing. Upon request of Canada, the Contractor must provide a document that describes the Contractor's documented log generation and management practices and controls.

(2)   The Contractor must provide the ability for Canada to centrally manage and configure content to be captured in audit records from multiple components (e.g. network, data, storage, compute, etc.) from the

Cloud Services consumed by Canada, to enable Canada to perform security monitoring, reporting, analysis, investigation and implementation of corrective actions, as required. This includes the ability for Canada to:

(a)   log and detect audit events such as (i) successful and unsuccessful account login attempts, (ii) account management, (iii) object access and policy change, (iv) privilege functions and process tracking, (v) system events, (vi) deletion of data, and in accordance with Canada's Event Logging Guidance (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/event-logging-guidance.html);

(b)   record in logs (or log files) audit events that are time synchronized and timestamped in coordinated universal time (UTC) and protected from unauthorized access, modification, or deletion while in transit and at rest;

(c)   provide real-time alerts of failed audit events to personnel with the authority to address the failed audit events; and

(d)   separate Security Incidents and logs for different Canada accounts to enable Canada to monitor and manage events within its boundary that are affecting its instance of an IaaS, PaaS or SaaS Cloud Service provided to it by the Contractor or a Sub-processor.

(3)   The Contractor must provide the ability for Canada to export security events and logs using standardized reporting interfaces, protocols, and data formats (e.g. Common Event Format (CEF), syslog, or other common log formats) and APIs that support log data remote retrieval (e.g. via a database interface using SQL, etc.) for the Cloud Services it consumes, in support of GC operations including monitoring of the Cloud Services and for e-discovery and legal holds.

(4)   For SaaS, the Contractor must provide APIs that provide the ability to:

(a)   Inspect and interrogate data at rest in SaaS applications;

(b)   Assess events such as user access and behaviour, administrator access and behaviour, and changes to third-party API access, stored in SaaS application logs.

Continuous Monitoring

(1)   The Contractor must continually manage, monitor, and maintain the security posture of Contractor Infrastructure and Service Locations hosting Canada's Data throughout the contract, and ensure that the Cloud Services provided to Canada are in a manner that complies with these Security Obligations. As part of this obligation, the Contractor must:

(a)   Actively and continuously monitor threats and vulnerabilities to Contractor Infrastructure, Service Locations, or Canada's Data;

(b)   Conduct regular vulnerability scans and penetration testing of the Contractor Infrastructure and Service Locations, with the aim of identifying deficiencies and remediations in order to prevent unauthorized access to sensitive information, circumvention of access controls and privilege escalation, and exploitation of vulnerabilities to gain access to systems or information.

(c)   Undertake best efforts to prevent attacks through security measures such as denial of service protections;

(d)   Undertake best efforts to detect attacks, Security Incidents, and other abnormal events;

(e)   Identify unauthorized use and access of any Cloud Services, data and components relevant to Canada's IaaS, PaaS or SaaS Cloud Service;

(f)   Manage and apply security-related patches and updates in a timely and systematic manner to mitigate vulnerabilities and remedy any publicly reported issues in the Cloud Services or libraries that the Cloud Services make use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;

(g)   Respond, contain, and recover from threats and attacks against the Contractor Cloud Services; and

(h)   Where required, take proactive countermeasures, including taking both pre-emptive and responsive actions, to mitigate threats.

(2)   The Contractor's Cloud Services must allow for GC application data (for IaaS, PaaS and SaaS) and GC network traffic (for IaaS and PaaS) of cloud hosted GC services to be copied and forwarded to a predetermined location (in the cloud or on GC premises).

(3)   For SaaS, the Contractor's Cloud Services must allow Canada to deploy and operate security software to perform advanced monitoring and mitigations of cyber threats for Canada's Cloud Services for Canada managed components only.

Security Incident Management

(1)   The Contractor Security Incident response process for the Cloud Services must encompass IT security incident management lifecycle and supporting practices for preparation, detection, analysis, containment, and recovery activities. This includes:

(a)   A published and documented Security Incident Response Process for review by Canada that is aligned with one of the following standards: (i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; or (ii) NIST SP800-612, Computer Security Incident Handling Guide; or (iii) GC Cyber Security Event Management Plan (GC CSEMP).

(https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html); or (iv) other best practices from industry standards, if Canada determines, in its discretion, that they meet Canada's security requirements.
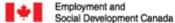
(b)   Documented processes and procedures of how the Contractor will identify, respond, remediate, report, and escalate Security Incidents to Canada, including: (i) the scope of the information security incidents that the Contractor will report to Canada; (ii) the level of disclosure of the detection of information security incidents and the associated responses; (iii) the target timeframe in which notification of information security incidents will occur; (iv) the procedure for the notification of information security incidents; (v) contact information for the handling of issues relating to information security incidents, in alignment with the reporting procedures outlined in the GC CSEMP (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html), and (vi) any remedies that apply if certain information security occur.

(c)   Ability for the Contractor to support Canada's investigative efforts for any compromise of the users or data in the service that is identified.

(d)   Allows only designated, pre-authorized representatives of Customer (e.g. Canadian Centre for Cyber Security, or other GC-approved organizations) authorized by the Technical Authority:

(i)   to request and receive discrete access and information associated with Customer's Data (user data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;

(ii)   the ability for Customer to track the status of a reported information security event.

(e)   Procedures to respond to requests for potential digital evidence or other information from within the Cloud Services environment and conforms to industry standards and best practices including ISO 22095:2020 Chain of custody — General terminology and models (https://www.iso.org/standard/72532.html) including proper forensic procedures and safeguards for:

(i)   the maintenance of a chain of custody for both the audit information, and

(ii)   the collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.

(2)   Within ten days of the effective date of the Contract, the Contractor must provide a document that describes the Contractor's Security Incident Response Process including contact information. This process including contact information must remain up-to-date, and at a minimum, be validated on an annual basis, and be approved by Canada.

(3)   The Contractor must:

(a)   Work with Canada's Security Operations Center(s) (e.g. GC SOC, Departmental IT Security Teams) and GC CSEMP Primary Stakeholders (i.e. CCCS and Treasury Board of Canada Secretariat (TBS)), on Security Incident containment, eradication and recovery, in accordance with the Security Incident Response process and the GC CSEMP (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html).

(b)   Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, the procedure for recovering data or the service, and records of activities related to the management of the security incident including internal communications and external communications (e.g. in the case of a ransomware event, all communications including ransom demands, etc.). This information must be provided to Canada upon request.; and

(c)   Track, or enable Canada to track, disclosure of Canada's Data, including what data has been disclosed, to whom, and at what time.

(4)   To support security investigations, Canada may require forensic evidence from the Contractor to assist in a GC investigation. The Contractor must:

(a)   retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed or provide to Canada for retention;

(b)   provide reasonable investigative support to designated, pre-authorized representatives of Canada such as CCCS and Royal Canadian Mounted Police (RCMP);

(c)   maintain chain of custody for evidence in accordance with best practices such as those outlined in ISO 22095:2020;

(d)   support e-discovery; and

(e)   maintain legal holds to meet needs of investigations and judicial requests.

(5)   In the event that the Contractor uses an external company for its incident response activities, the Contractor is expected to ensure that the provisions outlined in this *Section 25 – Security Incident Management* and *Section 26 – Security Incident Response* are also extended to the external incident response team and is documented in the Contractor's Security Incident Response Process.

Security Incident Response

(1)   The Contractor must alert and promptly notify Canada (via phone and email), as per the reporting procedures outlined in sub-section (25), of any compromise, breach or of any evidence such as (i) a security incident, (ii) a security malfunction in any asset, (iii) irregular or unauthorized access to any Asset, (iv) large scale copying of an Information Asset, or (v) another irregular activity identified by the Contractor, that leads the Contractor to reasonably believe that risk of compromise, or a security or privacy breach, is or may be imminent, or if existing safeguards have ceased to function, over the

following period (7 days x 24 hours x 365 days), and will be made without undue delay, in any event, within 72 hours, and within the Contractor's service level commitments.

(2)   If the Contractor becomes aware of and determines a compromise or breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay (i) notify Canada of the Security Incident; (ii) investigate the Security Incident and provide Canada with detailed information about the Security Incident; and (iii) take necessary steps to mitigate the cause and to minimize any damage resulting from the Security Incident.

(3)   Contractors are to report major incidents to the police of jurisdiction when requested by Canada.

Information Spillage

(1)   The Contractor must have a documented process that outlines its approach for an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another industry standard, approved by Canada in writing. Notwithstanding the foregoing, the Contractor's Information Spillage process must include, at a minimum:

(a)   A process for identifying the specific data elements that is involved in a System's contamination;

(b)   A process to isolate and eradicate a contaminated System; and

(c)   A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination.

(2)   Upon request of Canada, the Contractor must provide a document that describes the Contractor's Information Spillage Response Process.

Security Testing and Validation

(1)   The Contractor must have a process to conduct a non-disruptive and non-destructive vulnerability scan or penetration test of the Cloud Services hosting Canada's data. This includes the ability to conduct regular internal and external scanning related to the GC tenancy, and when there are significant changes to the main platform, to identify any potential system vulnerabilities related to the GC tenancy by performing:
    i.   vulnerability scans;
    ii. web application scans; and
    iii. penetration tests.

(2)   The Contractor must develop a plan of action and milestones to document any planned remedial actions to correct weaknesses or deficiencies to the main platform in order to reduce or eliminate known vulnerabilities in the system, or those that could be related to the Cloud Services hosting Canada's data and operation of the GC tenancy.

(3)   Upon request of Canada, the Contractor must provide the results of the testing of the overall platform and the plan of action and milestones documentation for planning and any review purposes.

(4)   The Contractor must provide the ability to enable a self-service security health check or scoring tool that enables the measurement of the security posture of the Cloud Services configured by Canada.

Personnel Security Screening

(1)   The Contractor must implement security measures that grant and maintain the required level of security screening for Contractor Personnel engaged in the provision of the Cloud Services and for Sub-processor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed.

(2)   The Contractor screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada.

(3)   Upon request of Canada, the Contractor must provide a document that describes the Contractor's personnel security screening process. The process must provide, at a minimum:

    (a)   A description of the employee and Sub-processor positions that require access to Customer Data or have the ability to affect the confidentiality, integrity or availability of the Cloud Services;

    (b)   A description of the security screening activities and practices, including notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern;

    (c)   A description of the security awareness and training as part of employment onboarding, when employee and sub-processor roles change, and on an ongoing basis, to ensure that employees and Sub-processors understand, are aware of, and fulfil, their responsibilities for information security;

    (d)   A description of the process that is enforced when an employee or sub-processor changes their role or when employment is terminated;

    (e)   The approach to detecting, responding, and mitigating potential insider threats and the security controls implemented to mitigate the risk of access to GC data and/or affect on the reliability of Cloud Services hosting Canada's data.

Physical (Data Centre / Facilities) Security

(1)   The Contractor must implement physical security measures that ensure the protection of IT facilities and information system assets on which Canada's Data are stored and processed against all forms of tampering, loss, damage, and seizure. Physical protection of all facilities that host Canada's Data, must be applied in accordance with, or use an adequate risk-based approach based on a prevent-detect-respond-recover approach to physical security, aligned with the physical security controls and the practices in the Treasury Board Operational Security Standard on Physical Security (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=procedure&p=C). The security measures required under this include, at a minimum:

    (i)   Sufficient redundancy and recovery capabilities within and between the Contractor's facilities including, being geographically disparate such that the loss of one facility does not prohibit recovery of data and Canada's Data within the prescribed service level commitments;

    (ii)   Proper handling of IT Media;

    (iii)   Controlled maintenance of all information systems and their components to protect their integrity and ensure their ongoing availability;

    (iv)   Controlled access to information system output devices to prevent unauthorized access to Canada's Data;

    (v)   Limiting physical access to Canada's Data and Service Locations to authorized Cloud Services Personnel based on position or role and the need-to-access principle, and validated by two forms of identification;

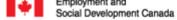   (vi)   Escorting visitors and monitoring visitor activity;

(vii)   Enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites);

(viii)   Recording and monitoring all physical access to Service Locations and all logical access to Systems hosting Canada's Data, using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms; and

(ix)   Performs continuous security checks at the boundary of Service Locations and facilities for unauthorized exfiltration of information or system components.

(2)   Upon request of Canada, the Contractor must provide a document that describes the Contractor's physical security measures.

(3)   If any physical security measures are to change in a way that materially degrades the physical security, the Contractor must inform Canada.

Supply Chain Risk Management

(1)   The Contractor must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide Cloud Services. This includes, but is not limited to protection throughout the systems development lifecycle by designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least privilege access for all personnel within the supply chain; threat awareness, education of the acquisition workforce on threats, risk and required security controls; and requiring supply chain entities to implement necessary safeguards.

(2)   The Contractor must have a supply chain risk management approach including a Supply Chain Risk Management Plan that is aligned with one of the following best practices:

(i)   ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4);

(ii)   NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or

(iii) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan.

(3)   Within 90 days of contract award, the Contractor must:

(a)   Provide proof that the SRCM approach and plan has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime.

          OR

(b)   Provide Canada with a copy of the SRCM Plan on an annual basis, or upon request of Canada.

(4)   In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with the Section 31 - Supply Chain Risk Management requirements, within 90 days of contract award, the SaaS provider using a GC-approved
IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed in the GC-approved IaaS provider environment for a supply chain integrity (SCSI) review. This SCSI review will be conducted no sooner than every three years.

Sub-processors

(1)   The Contractor must provide a list of Sub-processors that could be used to perform any part of the Work in providing Canada with the Service. The list must include the following information (i) the name of the Sub-processor; (ii) the identification of the Work that would be performed by the Sub-processor; and (iii) the location(s) where the Sub-processor would perform the Work.

(2)   The Contractor must provide a list of Sub-processors within ten days of the effective date of the Contract. The Supplier must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least 14-days in advance of providing that Sub-processor with access to Customer Data or Personal Data. The Supplier must assist Canada with verification of sub-processors within 10 working days.

Industrial Security Program – Security Requirement for Canadian Suppliers

(1)   The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer/Supply Arrangement, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B , issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC)

(2)   The Contractor/Offeror personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid personnel security screening at the level of SECRET, or RELIABILITY STATUS, as required by the security guide, granted or approved by the CSP, PWGSC.

(3)   The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until written approval has been issued by the client department security authority. After approval has been granted, these tasks may be performed at the level of PROTECTED B (as required) including an IT Link at the level of PROTECTED B (as required).

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

(5)   The Contractor/Offeror must comply with the provisions of the:

        (a)   Security Requirements Check List and security guide (if applicable), attached at Annex B and C;

        (b)   Contract Security Manual (Latest Edition);

        (c)   CSP website: Security requirements for contracting with the Government of Canada, located at www.tpsgc-pwgsc.gc.ca/esc-src

NOTE: There are multiple levels of personnel security screenings associated with this file. In this instance, a security guide must be added to the SRCL clarifying these screenings. The security guide is normally generated by the organization's project authority and/or security authority.

Industrial Security Program – Security Requirements for Foreign Suppliers

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the Industrial Security Sector (ISS), Public Services and Procurement Canada (PSPC), administered by International Industrial Security Directorate (IISD), PSPC. The Canadian DSA is the authority for confirming **Contractor/Subcontractor** compliance with the security requirements for foreign suppliers. The following security requirements apply to the foreign recipient **Contractor/Subcontractor** incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing outside of Canada for the Cloud Services described in the Cloud Solution, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified in the Section entitled Protection and Security of Data Stored in Databases.

(1)   The **Contractor/Subcontractor** certifies that the delivery and provisioning of Cloud Services under the terms of this contract must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which

Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

(2)   The Foreign recipient **Contractor/Subcontractor** must at all times during the performance of the **contract/subcontract** be registered with the appropriate government administered supervisory authority in the country(ies) in which it is incorporated or operating and authorized to do business. The Foreign recipient
Contractor/Subcontractor must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and the Canadian DSA.

(3)   Foreign recipient **Contractor/Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.

(4)   The Foreign recipient Contractor must not begin the work, services or performance until the Canadian Designated Security Authority (DSA) is satisfied that all contract security requirement conditions have been met. Canadian DSA confirmation must be provided, in writing, to the foreign recipient Contractor in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.

(5)   The Foreign recipient **Contractor/Sub-processor/Subcontractor** must identify an authorized Contract Security Officer (CSO) and an Alternate Contract Security Officer (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in this contract. This individual will be appointed by the proponent foreign recipient **Contractor's/Subcontractor's** Chief Executive officer or Designated Key Senior Official, defined as an owner, officer, director, executive, and or partner who occupy a position which would enable them to adversely affect the organization's policies or practices in the performance of the contract.

(6)   The **Contractor/Subcontractor** must not grant access to **CANADA PROTECTED B** information/assets, except to personnel who have a need-to know for the performance of the **contract** and have been screened in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbssct.gc.ca/pol/doc-eng.aspx?id=28115), or use acceptable equivalent measures agreed to by Canada.

(7)   **CANADA PROTECTED** information/assets, provided to the foreign recipient **Contractor/Subcontractor** or produced by the foreign recipient **Contractor /Subcontractor**, must:

        i.   not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the **contract**, without the prior written consent of   Canada. Such consent must be sought from the

             Canadian DSA in collaboration with the Contracting Authority; and

        ii.   not be used for any purpose other than for the performance of the **contract** without the prior written approval Canada. This approval must be obtained by contacting the Contracting Authority (in collaboration with the Canadian DSA).

(8)   The Foreign recipient **Contractor /Subcontractor** MUST NOT remove **CANADA PROTECTED** information/assets from the identified work site(s), and the foreign recipient **Contractor/ Subcontractor** must ensure that its personnel are made aware of and comply with this restriction.

(9)   The Foreign recipient **Contractor /Subcontractor** must not use the **CANADA PROTECTED** information/assets for any purpose other than for the performance of the **contract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

(10)   The Foreign recipient **Contractor/Subcontractor** must, at all times during the performance of the **contract** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED B**.

(11)   The Foreign recipient Contractor must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that CANADA PROTECTED information/ assets pursuant to this contract has been compromised.

(12)   The Foreign recipient Contractor must provide the CANADA PROTECTED information/ assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the Canadian DSA.

(13)   Upon completion of the Work, the foreign recipient Contractor must return to the Government of Canada, all CANADA PROTECTED information/assets furnished or produced pursuant to this contract, including all CANADA PROTECTED information/assets released to and/or produced by its subcontractors.

(14)   The Foreign recipient Contractor requiring access to CANADA PROTECTED information/assets or Canadian restricted sites, under this contract, must submit a Request for Site Access to the Chief Security Officer of Name of Department/Organization of Canada.

(15)   The Foreign recipient Contractor MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system and transfer via an IT link any CANADA PROTECTED B information until authorization to do so has been confirmed by the Canadian DSA.

(16)   Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the Canadian DSA.

(17)   All Subcontracts awarded to a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

(18)   All Subcontracts awarded by a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

(19)   The Foreign recipient **Contractor/Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex B and C.

(20)   Despite any section of the General Conditions relating to subcontracting, the foreign recipient Contractor must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the contract unless the Contracting Authority (in collaboration with the Canadian DSA) first consents in writing.

(21)   Canada has the right to reject any request made separate and apart from the authorization in this Contract in connection with the Contractor delivering Cloud Services to electronically access, process, produce, transmit or store **CANADA PROTECTED** data related to the Cloud Services in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

Physical Transport and Transmittal of Information

(1) The Contractor must implement measures to protect Canada's information in physical form, including assets at rest (for example, in use or in storage), in transit (for example, in transport or in transmittal), and through appropriate destruction. This includes, but is not limited to:

   (a) Ensuring that portable data storage devices are properly secured at all times as appropriate to the highest level of security classification of the information stored on it, in an appropriate security container as defined by the PSPC's Industrial Security Manual Chapters 5 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap5-eng.html) and chapter 8 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap8-eng.html), and the principles outlined in the RCMP's Security Equipment Guide (G1-001) (https://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm) for security container, and ensuring that the security container is protected with strong password and authentication mechanisms;

   (b) Encrypting all Canada's information stored on portable data storage devices using a Cryptographic Module Validation Program certified encryption module, and in accordance with Section 13 – Cryptographic Protection, including use of Common Criteria Program accredited products;

   (c) Ensuring that, prior to connecting the device to the Canada's IT network for the purpose of one-way transfers of information from the Canada's IT networks to the device, that the device is scanned for malicious software each time the device is connected to Canada's IT infrastructure

   (d) Ensuring that all portable devices used to transport Canada's information must be cleared from the device to prevent information recovery, in accordance with the media sanitization requirements outlined in Section 12 (1) - Data Disposition and Returning Records to Canada.

(2) Protected information is considered "in transmittal" until it has reached its intended destination and has been delivered to the Contractor data center facility or opened. If opened, it must then be safeguarded, in accordance with Section 30 – Physical Security, and PSPC's Industrial Security Manual Chapters 5 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap5-eng.html) and chapter 8 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap8-eng.html).

(3) The Contractor must report any real or suspected loss or theft of portable data storage devices, in accordance with Section 26 - Security Incident Response, and PSPC's Industrial Security Manual Chapters 5 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap5-eng.html) and chapter 8 (https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap8-eng.html).