Correctional Service Canada   Service correctionnel Canada

REQUEST FOR INFORMATION

THE CORRECTIONAL SERVICE OF CANADA

16-0266- Learning Management System (LMS)

Table of Contents

1.0 Background

1.1 Correctional Service Canada

Correctional Service Canada (CSC) is a Government of Canada (GC) agency within the Public Safety portfolio. This portfolio brings together key federal government organizations involved in public safety, including the Royal Canadian Mounted Police, the Parole Board of Canada, the Canada Border Services Agency, the Canadian Security Intelligence Service, and three review bodies.

CSC contributes to public safety through the custody and reintegration of offenders. More specifically, CSC is responsible for administering court-imposed sentences for offenders sentenced to two years or more. This includes both the custodial and community supervision of offenders with Long Term Supervision Orders (LTSOs) for periods of up to ten (10) years. CSC is currently responsible for approximately 15,500 offenders incarcerated in institutions and 8,700 offenders under supervision in the community.

CSC has a presence from coast to coast to coast, from large urban centres with increasingly diverse populations, to more remote Inuit communities across the North. CSC manages institutions, psychiatric treatment centres, four Aboriginal healing lodges, community correctional centres, community residential facilities and parole offices. In addition, CSC has five regional headquarters that provide management and administrative support and serve as the delivery arm of CSC's programs and services. Additional information can be located on CSC's website (http://www.csc-scc.gc.ca).

1.1.1 CSC's current LMS

The Learning and Development (L&D) Branch is responsible for the delivery, development and tracking of training for over 19,000 employees, as well as over 200 annual, correctional officer recruits.

A web-based Commercial-off-the-Shelf (COTS) Learning Content Management System (LCMS) called ForceTen is CSC's current online learning application which provides electronic content to employees. ForceTen is implemented in 2 different system instances which are hosted on intranet and external website due to the different audiences (employees/recruits).

Procurement of a new Learning Management System (LMS) is required as ForceTen cannot meet CSC's evolving business needs to manage all aspects of training and related assessments (such as, but not limited to online/in-class delivery, e-learning/coaching, virtual classroom, enterprise analytics, automate functions, manage programs, career/learning plans, assessment, etc) within one system nor adhere to the CSC Organizational Priorities and Blueprint 2020 Vision. Furthermore, ForceTen is not supported since September 2017.

1.2 Objectives of this Request for Information

The L&D Branch is exploring options for an organisational learning solution (known henceforth as the “Solution”) that supports CSC’s comprehensive and evolving training needs, specifically:

- Learner management;
- Course offering management (including the management of: catalogues, resources, registrations, calendars, tracking/monitoring);
- Course content management;
- Learning delivery;
- Learning program management;
- Learning provider management;
- Knowledge assessments and evaluations;
- Reporting, notifications and communications;
- Invoicing, costing and financials; and
- General and system requirements.

The key objective of this RFI is to obtain Vendor feedback on available solutions. This will allow CSC to better identify the types of solutions available on the market and their capabilities.

2.0 The RFI Process

2.1 Nature of the 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 may not necessarily follow this RFI. This RFI is simply intended to solicit feedback from the industry with respect to the matters described 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.

2.2 Nature and Format of Responses Requested

Vendors are requested to review *Annex A - Response Requirements* and prepare responses following the structure outlined therein.

Vendors 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. Vendors should review *Annex B – CSC Technical*

Environment Information and explain any assumptions made in preparation of their responses.

Responses from Vendors will assist CSC in formulating a procurement strategy that meets the business and operational requirements of CSC.

Vendors are free to submit information on other software applications, which are related to the proposed Solution, or work in conjunction with the proposed Solution, to support offender rehabilitation (e.g. limited internet access).

2.3 Response Parameters

Vendors may submit comments, concerns, suggestions, and, where applicable, alternative recommendations regarding how the requirement may be satisfied.

2.4 Response Confidentiality

Vendors are requested to clearly identify those portions of their response that are proprietary to the Vendor. The confidentiality of each Vendor's response will be maintained.

2.5 Response Costs

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

2.6 Treatment of Responses

2.6.1 Use of Responses

Responses received by the RFI closing date will be reviewed and may be used by CSC to develop or modify procurement strategies or any draft documents contained in this RFI. CSC may, at its discretion, review responses received after the RFI closing date.

2.6.2 Review Team

A review team composed of representatives of CSC will review the responses. CSC 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.

2.6.3 Confidentiality

Respondents should mark any portions of their response that they consider proprietary or confidential. CSC will handle the responses in accordance with the *Access to Information Act*.

2.6.4 Follow-up Activity

CSC may, at its sole discretion, contact any respondents to follow-up with additional questions or for clarification of any aspect of a response. CSC reserves the right to invite any or all respondents to present their submissions to this RFI and/or perform a product demonstration (herein referred to as a “Vendor Session”).

Respondents that have expressed such interest can expect to be contacted approximately four (4) weeks after the RFI closing date to schedule the Vendor Session. An Invite Agenda along with specific questions or areas of interest to be covered during the session will be provided to the invited respondents.

The Vendor Session will be located in the National Capital Region (NCR). The exact location and timeframe will be detailed in the Invite Agenda. Vendors will also be asked to provide an electronic version of their presentation.

The Vendor Session will cover specific functional and technical aspects of the Solution. As such, vendor representatives attending the session must include Subject Matter Expert(s) in these areas in order to meaningfully respond to questions at the session. CSC personnel with extensive experience in IT technology will attend the presentation.

2.7 Response Format

2.7.1 Response Preparation Instructions

CSC requests that the Vendor provide their responses in separately bound sections as follows:

a. One hard copy and one soft copy on CD in a Microsoft Word Format. CSC requests that Vendors follow the instructions described below in the preparation of their response:

   i. use 8.5 x 11 inch (216 mm x 279 mm) paper; and
   ii. use a numbering system that corresponds to the RFI.

b. In accordance with the *Policy on Green Procurement*. In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process *Policy on Green Procurement* (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, Vendors should:

   i. use 8.5 x 11 inch (216 mm x 279 mm) paper containing fibre certified as originating from a sustainably-managed forest and containing minimum 30% recycled content; and
   ii. use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

2.7.2 Volume Cover Page

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

2.7.3 Title Page

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

- Title of the respondent's response;
- Volume number and the total number of volumes;
- Name and address of the respondent;
- Name, address and telephone number of the respondent's contact;
- Date; and
- RFI number.

2.7.4 Numbering System

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

2.7.5 Language of Response

Responses may be in English or French at the preference of the Vendor.

2.8 Enquiries

Because this is not a bid solicitation, CSC 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:

Steve Perron
Senior Procurement Officer
National Headquarters
Correctional Service Canada
T. 613-992-6509
E. steve.perron@csc-scc.gc.ca

2.9 Submission of Responses

Vendors interested in providing a response **must** deliver it to the Contracting Authority identified above by 14:00 EST on March 6, 2019.

Each Vendor is solely responsible for ensuring that its response is delivered on time to the correct location.

The review of responses will begin after the date and time specified above. Responses received after this date may not be reviewed.

In the event that a response is not sufficiently clear, the CSC reserves the right to seek additional information at their sole discretion.

2.10 Procurement Strategy

This RFI is for the sole purpose of gathering information as described herein.

ANNEX A – Response Requirements

The purpose of this RFI is to obtain detailed information from the Vendor community. CSC has outlined below a list of questions to which the Vendor should respond with sufficient detail as to allow CSC to determine solutions available in the current marketplace.

This RFI is not a commitment with respect to future purchases or contracts. In preparing their responses, the Vendor community should refer to *ANNEX B – CSC Technical Environment Information*.

CSC is requesting that the Vendor community provide the following:

1. Corporate Profile

Each Vendor should provide:

a. Company name, address, telephone & fax numbers and e-mail address;
b. Company contact name and telephone number; and
c. Company background information including location of parent company, contact information for company representative and/or distributor in Canada (if any), types of products sold, and website address.

CSC may request additional contact information at any point in time.

2. Solution Description

Each Vendor should provide:

a. A Solution identifier such as a model number, version number and a description of all components required for the Solution;
b. Brochures including photos outlining full Solution specifications;
c. Details of the infrastructure components required to deploy the Solution;
d. Pricing model(s);
e. Licensing model(s); and
f. Support and maintenance model(s).

3. Questions to Industry

CSC is requesting the Vendor community to respond to the questions below.

TABLE 1 – LEARNER MANAGEMENT

1	Does the proposed Solution allow the capture of learner information (e.g., job information, leave information, medical exemptions, learner's manager or direct report)?
2	Does the proposed Solution provide **learner, delegated manager, and instructor** self-service functionalities, such as: a. Viewing/customizing the learner profile and/or dashboard (e.g., course history, learning plan progress, course marks, course registration)? b. Viewing the catalogue of courses? c. Viewing the status of electronic training requests? d. Allowing registration to training or events once approved? e. Assessing and completing online learning events? f. Tracking progress and completion (learner & delegated manager)? g. Accessing online help within the LMS? h. Allowing for discussion capacity between users (read, reply, post comments, including communicating with co-learners from the specific course or instructors communicating with learners)? i. Managing attendance, marks, email, withdrawal, and availability (instructor)? j. Capturing instructor information and qualifications, including non-employee instructors? k. Managing their own training delivery schedule (instructor)?
5	Does the proposed Solution allow for the management of learning plans, such as: a. Creating, viewing, updating, and deleting learning plans? b. Setting the duration of a learning plan? c. Requests for specific courses by learners and approval/rejection of requests by managers? d. Allow browsing of the Canada School of Public Service (CSPS) catalogue and adding CSPS courses to the learning plan? e. Allow data extractions to identify CSPS and internal training requirements to plan training delivery?

6	Does the proposed Solution allow any of the following role management functionalities: a. Grant access to functionality based on roles (e.g., administrator, learner, manager, instructor); b. Manage full or partial access for administrators; c. Manage delegation of roles to other users; d. Manage a variety of learner audiences (e.g., employees, recruits); and e. Log and monitor user and administrator activity.
7	Does the proposed Solution allow for the management of target audiences, such as: a. Restricting access to specific groups of learners (e.g., students, correctional officers)? b. Ability to assign/remove learning events, opportunities, information to specific groups of learners? c. Promoting learning events to various groups? d. Reporting on groups of learners?

TABLE 2 – COURSE OFFERING MANAGEMENT – CATALOGUE MANAGEMENT

8	Does the proposed Solution allow for the creation and maintenance of a course catalogue?
9	Does the proposed Solution allow self-service access to the catalogue? a. Does it provide select and register functionality through self-service? b. Does it allow items to be added to the learning plan from the catalogue?
10	Does the proposed Solution allow for the creation and management of all types of sessions (in-class, online, webinar, self-directed, instructor led)?
11	Does the proposed Solution provide functionality to enforce course restrictions and prerequisites, including obtaining required approval from a manager or instructor?

TABLE 3 – COURSE OFFERING MANAGEMENT – RESOURCE MANAGEMENT

13	Does the proposed Solution allow for the capture and maintenance of: a. Training equipment information and inventory? b. Training infrastructure (e.g., classroom, gym, firing range)? c. Printed course material inventories?
14	Does the proposed Solution allow for the assignment/booking of resources to course offerings? (e.g., instructor, room, equipment, learning material)?

TABLE 4 – COURSE OFFERING MANAGEMENT – REGISTRATION MANAGEMENT

15	Does the proposed Solution allow bulk/group registrations for online and self-paced learning events?
16	Does the proposed Solution allow the management of waitlists?

TABLE 5 – COURSE OFFERING MANAGEMENT – CALENDAR, TRACKING & MONITORING MANAGEMENT

17	Does the proposed Solution allow: a. Functionality to create, view, and maintain a learning event calendar? b. Calendar events to be linked to registration pages? c. The monitoring of changes to registrations (e.g., per training, program, group of learners)?

TABLE 6 – COURSE CONTENT MANAGEMENT

18	Does the proposed Solution allow the importing and management of training content?
19	Does the proposed Solution allow the importing of SCORM (https://scorm.com/) compliant training content?
20	Does the proposed Solution allow the use of multimedia objects (e.g., audio, video) and media rich objects (e.g., 3D animations)? If so, which formats are supported?
21	Does the proposed Solution support multiple compression standards? How does the Solution maximize bandwidth to ensure high-quality content streaming and optimal performance? Please describe the network architecture required to maintain quality.
22	Does the proposed Solution allow searching of content using parameters (e.g., course info, location, timeframes, competencies, instructors, type of training, learning provider)?

23	Does the proposed Solution allow the creation and use of: a. Surveys and questionnaires? b. Self-assessments, quizzes, and formal tests? c. Any other assessment/learning evaluation tool? If so, please specify the possible question types (e.g., multiple choice, short answer, long answer, true or false).

TABLE 7 – LEARNING DELIVERY

24	Does the proposed Solution allow access to training via mobile devices? If so, please outline any devices and operating systems that are supported.

TABLE 8 – LEARNING PROGRAM MANAGEMENT

26	Does the proposed Solution allow the creation and management of competencies, including competency structures linked to job codes and/or positions?

TABLE 9 – LEARNING PROVIDER MANAGEMENT

27	Does the proposed Solution provide functionality to grant automatically competencies, compliance and/or certification upon completion?

TABLE 10 – TALENT MANAGEMENT

28	Does the proposed Solution allow the creation and management of talent management plans? Please describe any talent management features the proposed Solution can offer.
29	Does the proposed Solution allow the creation and management of succession plans? Please describe any succession plan features the proposed Solution can offer.
30	Does the proposed Solution allow the creation and management of career plans? Please describe any career plan features the proposed Solution can offer.

TABLE 11 – RECRUITMENT PLANNING

31	Does the proposed Solution provide the ability to plan recruiting requirements based on identified needs or gaps (e.g. staffing planning based on language abilities, qualifications etc.)?

TABLE 12 – REPORTING

32	Does the proposed Solution allow reporting on various themes, such as: a. Seat utilization by course? b. Asset inventory? c. Recertification requirements? d. Compliance? e. Completion? f. Mandatory training? g. Certification? h. Number of active courses? i. Number of programs? j. Number of certified learners? k. Outstanding courses? l. Test and assessment results? Please provide any additional details on other reportable themes.
33	Does the proposed Solution allow scheduling of report generation?
34	Does the proposed Solution allow exporting of reports in various formats? Which formats?

TABLE 13 – NOTIFICATIONS AND COMMUNICATIONS

35	Does the proposed Solution provide notification functionality for users? If so, can the notifications be customized (e.g., frequency, thresholds)?
36	Does the proposed Solution allow auto-generated notifications for the following: a. Actions required? b. Confirmations? c. Reminders? d. Information? e. Compliance/recertification requirements?

TABLE 14 – INVOICING, COSTING AND FINANCIALS

37	Does the proposed Solution allow for the capture of training financial codes?
38	Does the proposed Solution allow for the capture of training and/or travel costs?

TABLE 15 – GENERAL AND SYSTEM REQUIREMENTS

39	Please describe the technical architecture (e.g., logical, physical, functional, security) of the Solution by providing documents and diagrams required to describe the full deployment of the Solution.
40	Please provide a pricing model. Does the proposed Solution have ongoing licensing or maintenance costs?
41	Does the Vendor guarantee minimum service levels though service level agreements (SLAs)?
42	Does the proposed Solution allow the management of data storage, archiving, retention and recall?
43	Does the proposed Solution provide encryption for data at rest, in transit and in process? Please describe protocols, standards and techniques used at each stage in detail. (Refer to Data Encryption Requirements in Annex B 3.2 and Communication Encryption Requirements in Annex B 3.3)
44	Does the proposed Solution comply with all federal government security/privacy standards? (Refer to CSE ITSG-33, data privacy and information security in Annex B 3 and B 3.1)
45	If the Solution is Cloud based, does it offer Multi Factor Authentication (MFA)?
46	If the Solution operates from a GC Data Centre, can it use Government of Canada authentication protocol (e.g., single sign-on) or other federated authentication (e.g., Security Assertion Markup Language, Active Directory, Federated Active Directory)?
47	Does the proposed Solution allow the capture of: a. Personal Record Identifier (PRI) for a learner as an identifier? b. Other identification information for learners who do not have a PRI?
48	Is the proposed Solution certified by the international certification to allow the storage of data/courseware content up to Government of Canada Protected B? (Examples are, but are not limited to ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, FedRAMP, Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR), AICPA Service Organization Controls (SOC) audit reports or certification.)
49	Does the proposed Solution ensure that data in process, transit, storage, backup, or remotely managed resides within Canada at all times? The Solution is expected to comply with apply the Direction for Electronic Data Residency (ITPIN No: 2017-02) (Refer to Cloud Based Solution in Annex B 3.4)

50	Does the proposed Solution support high throughput to allow video streaming, virtual classrooms and online training?
51	Does the proposed Solution support learning activities and profiles of up to 20,000 users?
52	Does the proposed Solution provide high availability and/or failover functionality?
53	Does the proposed Solution provide multiple environments (e.g., development, quality assurance, pre-production, production)?
54	Does the proposed Solution allow compatibility and/or inter-operability with: a. PeopleSoft HR Management System? (importing HR data to the LMS; importing learning data to HRMS) b. SAP Oracle Financial Systems/Microsoft Power BI? (linking financial codes to learning events and travel expenses) c. CSPS? (importing training data to the LMS) d. Government of Canada Departmental Electronic Mailing Solution? (interfacing with the LMS) e. Corporate reporting tools? (exporting LMS data for corporate reporting)
55	Does the proposed Solution provide a Graphical User Interface (GUI) platform, and/or is it Configuration File Loader (CFL) compatible?
56	What are the highest foreseeable risks for this CSC project? What steps does the Vendor recommend to mitigate those risks? Please provide a list of risks from the perspectives of planning, migration, implementation, and support.

4. Alternative Suggestions

Does the Vendor have any suggestions and/or concerns with respect to the questions listed in *Annex A* or the technical environment in *Annex B*? Are there any foreseeable issues that would prevent the Vendor from being able to respond to a future proposed bid solicitation? If so, please outline your suggestion(s), concern(s) and any recommendations to resolve them.

5. Demonstrations

Would your company be interested in attending a RFI follow-up session with the opportunity to demonstrate your Solution? These sessions will take place on-site at CSC or remotely utilizing web/video conferencing. See the section entitled *Follow-up Activity* for more details.

ANNEX B – CSC Technical Environnent Information

1. Background

CSC is a distributed organization segmented into five geographical regions and the National Headquarters. The Human Resource Management (HRM) sector oversees the Learning and Development (L&D) Branch which is responsible for training over 19,000 employees and the operation of six learning centres and the CSC Training Academy.

CSC is seeking to promote L&D business operations by securing an organisational Learning Management System (LMS) solution that supports the department's comprehensive and evolving training needs and adheres to Organizational Priorities and the Blueprint 2020 Vision.

The current Learning Content Management System (LCMS) in use by CSC is IBM ForceTen. To accommodate different audiences, two instances of ForceTen have been deployed, specifically an internal instance for employees and an external instance for recruits. With ForceTen being dependent on Adobe Flash and support to end by 2020, approximately 85% of CSC's online content will be inoperable at that time. The remaining 15% of the online content is already facing challenges with current web browsers.

To accommodate the needs of the CSC, the Vendor must be capable of providing a system that allows the management of all aspects of training including online/in-class delivery, e-learning/coaching, virtual classrooms, enterprise analytics, evaluations, automated functions, program management, and career/learning plans. Furthermore, the system architecture should be capable of hosting learning material on premises to avoid excessive network traffic and consumption based on trainee location.

2. Data Sovereignty

The protection of information, from a privacy and security perspective, is core to the integrity of government programs, which underpins confidence in Canada. All information managed by Canada requires protection, including information published publicly in order to appropriately protect the confidentiality, integrity and availability of the information. The information up to and including "Protected B" may be shared while using the network, and it is incumbent that the work incorporates the appropriate controls in order to safeguard the interests of Canada and those of its partners to this level of security.

Furthermore, security controls, which ensure the confidentiality, integrity and availability of the work, are imperative requirements for the work alone monitoring system, as Canadians expect Canada to take all appropriate measures to protect personal and sensitive information. Therefore, the anticipated solution must be within the political and graphic boundaries of Canada (see *Annex C - Certification of Data Centres Located in Canada*). Stringent contractual and technical measures must be put in place to ensure that information is secured at all times, at rest and in motion, through encryption protection and is only accessed by those authorized to access the infrastructure for those purposes approved by Canada.

3. Data Privacy and Information Security

All CSC data must be managed in accordance with Canadian Security Establishment *IT Security Risk Management Life Cycle Approach (CSE ITSG-33).* It is anticipated that PB-M-M Security Control Profile will be applicable for this requirement.

Canada will require the Vendor to establish and maintain a data privacy and information security program, including physical, technical, administrative, and organizational safeguards designed to:

a. Ensure the security and confidentiality of Canada's Data;

b. Protect against any anticipated threats or hazards to the security or integrity of Canada's Data;

c. Protect against unauthorized disclosure, access to, or use of Canada's Data;

d. Ensure the proper disposal of Canada's Data; and

e. Ensure that all employees, agents, and subcontractors of the Contractor, if any, comply with all of the foregoing.

3.1 Privacy – Protection of Personal Information

Canada has an obligation to ensure that Canadian statutes, regulations, and policies on privacy protection are respected. Where applicable, federal institutions must ensure that personal information is protected in accordance with the *Personal Information Protection and Electronic Document Act* **(**http://laws-lois.justice.gc.ca/eng/acts/P-8.6/**)** and the *PRIVACY ACT* (https://laws-lois.justice.gc.ca/eng/acts/p-21/).

3.2 Data Encryption Requirements

The information system implements in accordance with applicable GC legislation and TBS policies, directives and standards:

- ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information, August 2016: https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111

- CSE ITSD-01A IT Security Directive for the Application of Communications Security Using CSE-Approved Solutions, January 2014: https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsd01a-eng_0.pdf

The integrity and confidentiality of sensitive application data shall be protected when in storage and in transit between application components using approved cryptography.

3.3 Communication Encryption Requirements

The SOLUTION must use a Communication Security Establishment (CSE) approved encryption mechanism, namely a minimum 128-bit Transport Layer Security (TLS) 1.2 or later encryption, using approved Cryptographic Primitives for TLS.

CSE ITSP.40.062 - Guidance on Securely Configuring Network Protocols, August 2016: https://www.cse-cst.gc.ca/en/node/1830/html/26507

3.4 Cloud Base Solution

Any cloud based solutions must be compliant with TBS directives on cloud based computing/solutions (https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) and available via SSC as the GC Cloud Services Broker.

- The solution must meet the security management requirements as defined in Annex B Section 2. Data Sovereignty – Canadian Control at all times.

- The Solution is expected to comply with the TBS Direction for Electronic Data Residency (ITPIN No: 2017-02), March 2018: https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/direction-electronic-data-residency.html

4. Supply Chain Security

In addition to the threat of cyber-attack, there is a growing awareness of the risks posed by potentially vulnerable or shared technologies that may be entering the GC communications networks and IT infrastructure through the supply chain. The Vendor will be required to provide the GC with a list of all proposed hardware and software manufacturers and suppliers in the delivery of IT Infrastructure and services in advance of contracting with them. Canada will reserve the right to reject a hardware or software manufacturer and/or supplier for security and/or business stability reasons.

The Vendor will also be required to abide by the *Technology Supply Chain Guidelines (https://www.cse-cst.gc.ca/en/page/technology-supply-chain-guidance)*.

5. Service-Delivery Models

Shared Services Canada (SSC) currently provides infrastructure services to CSC.

CSC will accept Vendor feedback using any of the following service-delivery methods:

a. *Vendor-Managed Solution in a GC Owned Facility*

The solution will be constructed and hosted by the Vendor at a facility owned by the GC. The solution itself, including the server hardware, application software, security patches, network and all licences required, would be provided, managed and operated by the Vendor as a service.

b. *Fully Managed Solution Hosted Outside of GC Facilities*

The Vendor would be responsible for provisioning hardware and software assets that are required to deliver the solution to the GC. The location of the service would be in facilities within the boundaries of Canada and would be managed by the Vendor (see *Annex D - Certification of Data Centres Located in Canada*).

c. *Alternative Solution Delivery*

The Vendor may propose any other delivery mechanism for the solution that it would like the CSC to consider.

6. Current Service Offering

6.1 Geographical Distribution

CSC's current LCMS is accessed across Canada consisting of five geographical regions and the National Headquarters.

6.2 Number of Users

As of September 30, 2018, CSC had 19,634 employees including recruits, full-time indeterminate, part-time and term staff. In addition, approximately 500 staff at the Parole Board of Canada currently use CSC's LCMS.

6.3 Content

6.3.1 Number of Courses

In total, CSC has 212 courses developed in ForceTen (i.e., 60 courses) and StoryLine (i.e., 152 courses).

6.3.2 Amount of Content

CSC has 13,906 windows in ForceTen and between 53,000 - 71,000 windows in StoryLine. In total, CSC has 66,906 - 83,906 windows of content.

6.3.3 Security Level of Content

CSC's training content contains both Government of Canada Protected A and Protected B information.

6.4 Environments

CSC has 4 instances of ForceTen including internal, back-up (DEV), external, and sandbox. Communication between the external user and LMS is encrypted.

7. Networks

The proposed solution must work with the CSC and GC networks. All software and websites must be certified through CSC and Shared Services Canada (SSC) governance processes before being accessed through the corporate firewall.

Solutions using SSC infrastructure will be hosted on virtual servers, which will allow for better stability and growth in terms of hardware resource procurement, and disaster recovery services.

Bandwidth availability may be limited to connection to the portal. Examples include, but are not limited to:

- Internal WAN: 1.5 Mbps to regional offices;
- Internet (SMS): 100 Mbps connection; and
- National Headquarters (NHQ) Local LAN: 100 Mbps backbone for workstations/1 Gbps backbone for servers.

There are also varying levels of network traffic within and between networks producing latencies between 1 ms (e.g., within NHQ) and 83 ms (e.g., between NHQ and select prairie regional sites).

The proposed solution must operate without performance degradation.

7.1 Public Access Zone

Users may access the solution from a desktop or remote computer. Connectivity to the network and the solution will comply with SSC standards and must protect the security and integrity of the connections and data.

7.1.1 Operations Zone

Enterprise-wide services are supported by a distributed server-based back end infrastructure. The infrastructure provides:

- Directory services (e.g., Active Directory, Forefront Identity Manager);
- File services (e.g., Distributed File System

- Print services (e.g., Windows, direct IP Printing);
- Electronic distribution (e.g., System Centre Configuration Manager 2007); and
- Secure remote access (e.g., Citrix, Cisco AnyConnect).

7.1.2 Other Client System Integration

The solution may need to integrate with other current and future systems deployed by the clients including, but not limited to:

- PeopleSoft Human Resource Management System (HRMS)
- Public Service Performance Management (PSPM)
- Canada School of Public Service (CSPS)
- SAP Oracle Financials

8. GoC/Departmental Electronic Mailing Solution General Architecture

With regards to network security, the proposed Solution must use an approved GC data encryption algorithm. GC operational security standards, including *Management of Information Security* (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328), and department specific security standards and procedures must be followed. Access will comply with the architecture and zones in accordance with ITSG-38 and ITSG-22 guidelines.

The proposed Solution must offer a minimum of two-factor authentication through a portal (e.g., Web interface) or application. Should the solution connect to the SSC infrastructure, two-factor authentication is required including the GC myKEY authentication (https://eajl-orca.securise-secure.gc.ca/O/vw/bienvenue-welcome-eng.pub) and conforming to ITSG-31 and ITSG-33 guidelines.

ANNEX C – Certification of Data Centres Located in Canada

By submitting a response, the Vendor acknowledges that the proposed Solution must be an internet-based solution that is located within the geographical boundaries of a Canadian province or territory. The Vendor must also ensure that:

1. Data transmitted and/or stored by and for Correctional Service Canada (CSC) shall be segregated from all trans-border dataflow between Canada and the United States of America (USA);
2. Under no circumstance will the data be transmitted, stored or shared other than between the Vendor and CSC;
3. Data transmitted and/or stored by and for CSC shall be segregated from other company records and information holdings and shall be delivered to the Government of Canada upon request; and
4. Electronic audit trails for information are stored in an immutable database in order to easily determine the history of access for any individual at any time.