RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
RFI - INMATE-OWNED CANTEEN POS SOL.

Solicitation No. - N° de l'invitation	Date
21120-153706/A	2015-07-31
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
21120-15-2163706	PW-$EEM-039-29391
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
039eem.21120-153706	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2015-09-02

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

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

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Wong, Vincent	039eem
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(819) 956-3769 ( )	(819) 953-3703

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
See Herein
Précisé dans les présentes

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

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

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

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

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

Signature **Date**

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

Canada

REQUEST FOR INFORMATION

INMATE-OWNED CANTEEN POINT OF SALE SOLUTION

21120-153706/A

1. Purpose and Nature of the Request for Information (RFI)

On behalf of the Correctional Service of Canada (CSC), Public Works and Government Services Canada (PWGSC) is requesting Industry feedback regarding commercial off-the-shelf point of sale solutions for inmate-owned canteens located within CSC institutions across Canada.

The objectives of this Request for Information (RFI) are to solicit information on current marketplace availability, capabilities and interest on commercial off-the-shelf point of sale solutions that can meet CSC's business requirements, namely analysis and reporting capabilities as well as interface with CSC's inmate accounting system.

This RFI is neither a call for tender or a Request for Proposal (RFP). No agreement or contract will be entered into based on this RFI. The issuance of this RFI is not to be considered in any way a commitment by the Government of Canada, nor as authority to potential respondents to undertake any work that could be charged to Canada. This RFI is not to be considered as a commitment to issue a subsequent solicitation or award of contract(s) for the work described herein.

Although the information collected may be provided as commercial-in-confidence (and, if identified as such, will be treated accordingly by Canada), Canada may use the information to assist in drafting performance specifications (which are subject to change) and for budgetary purposes.

Respondents are encouraged to identify, in the information they share with Canada, any information that they feel is proprietary, third party or personal information. Please note that Canada may be obligated by law (e.g. in response to a request under the Access to Information and Privacy Act) to disclose proprietary or commercially-sensitive information concerning a respondent (for more information: http://laws-lois.justice.gc.ca/eng/acts/a-1/).

Respondents are asked to identify if their response, or any part of their response, is subject to the Controlled Goods Regulations.

Participation in this RFI is encouraged, but is not mandatory. There will be no short-listing of potential suppliers for the purposes of undertaking any future work as a result of this RFI. Similarly, participation in this RFI is not a condition or prerequisite for the participation in any potential subsequent solicitation.

Respondents will not be reimbursed for any cost incurred by participating in this RFI.

The RFI closing date published herein is not the deadline for comments or input. Comments and input will be accepted any time up to the time when/if a follow-on solicitation is published.

2. Background Information

CSC is in the process of modernizing its legacy systems. CSC currently utilizes a commercial off-the-shelf inventory management software for inmate canteen point of sale (POS) operations. This

software is operated in a decentralized fashion on local area networks, standardized across each CSC institution and is primarily operated by inmates.

The current POS software interfaces with CSC's Inmate Accounting System Replacement (IASR) software solution on a bi-weekly basis through a manual process (use of USB drives) to confirm availability of funds and reserve funds for individual inmates to make purchases at Inmate Owned Canteens. IASR is a trust fund management system which manages the inmate funds received from internal and external sources as well as disbursements such as food and accommodation deductions and canteen purchase.

3. Potential Work Scope and Constraints

The responses received may be used by Canada to develop or modify procurement strategies and/or any contracting documents, clauses, terms and conditions. One potential outcome of this consultation process may be the potential for a competitive RFP.

Constraints include CSC's corporate reporting and security requirements, as detailed in Annex A, "Questions to Industry".

4. Legislation, Trade Agreements, and Government Policies

The following is indicative of some of the legislation, trade agreements and government policies that could impact any follow-on solicitation(s):

a) Agreement on Internal Trade (AIT)
b) North American Free Trade Agreement (NAFTA)
c) World Trade Organization – Agreements on Government Procurement (WTO-AGP)
d) Federal Contractors Program for Employment Equity (FCP-EE)

5. Nature and Format of Responses Requested

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

6. Treatment of Responses

a) Use of Responses: The responses received may be used by Canada to develop or modify procurement strategies and/or any contracting documents, clauses, terms and conditions. Canada will review all responses received by the RFI closing date. Canada may, in its discretion, review responses received after the RFI closing date.

b) Review Team: A review team composed of representatives of Canada will review the responses received. Canada reserves the right to hire independent consultants, if Canada considers it necessary, to review any response received. Not all members of the review team will necessarily review all responses.

c) Confidentiality: Respondents should mark any portions of their response that they consider proprietary or confidential. Canada will handle the responses in accordance with the Access to Information Act.

d) Follow-up Activity: Canada may, in its sole discretion, contact any respondents to follow-up with additional questions or for clarification of any aspects of a response.

7. Contents of this RFI

This RFI contains specific questions addressed to Industry regarding the requirement. This document remains a work in progress and respondents should not assume that new clauses or requirements will not be added to any bid solicitation that is ultimately published by Canada. Nor should respondents assume that none of the clauses or requirements will be deleted or revised. Comments regarding any aspect of the RFI are welcome.

8. Enquiries

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

Vincent Wong
Contracting Authority
Software and Shared Systems Procurement Directorate
Public Works and Government Services Canada

Email: Vincent.Wong@tpsgc-pwgsc.gc.ca

9. Submission of Responses

a) RFI Closing Date and Preferred Method of Submission: Interested Respondents should submit their responses via email to the PWGSC Contracting Authority, identified in section 8 “Enquiries”, by 14:00 EDT on September 2, 2015. Respondents who wish to submit their responses other than by email should contact that PWGSC Contracting Authority.

b) Responsibility for Timely Delivery: Respondents are solely responsible for ensuring their responses are submitted on time to the correct email address.

c) Identification of Response: Respondents should ensure that their responses include a point of contact for the Respondent, identifying the contact’s name, title, contact phone number, and email address.

10. Changes to RFI

Changes to this RFI may occur and will be advertised on the Government Electronic Tendering Service. Canada asks Respondents to visit Buyandsell.gc.ca regularly to check for changes, if any.

REQUEST FOR INFORMATION

INMATE-OWNED CANTEEN POINT OF SALE SOLUTION

21120-153706/A

ANNEX A – QUESTIONS TO INDSUTRY

1. Background on Current Point of Sale System and Processes

The Correctional Service of Canada's (CSC) current point of sale (POS) system is a standalone system on a closed LAN in each institution where it is implemented. It consists of a desktop computer which serves as the database and application server for POS application, one or more admin workstations in other locations, and two to four desktop computers used by offenders in Inmate Managed Canteen(s) behind Security. All desktop computers currently have Windows XP as the operating system. The desktops are linked to each other but are kept physically separate from the CSC network.

CSC Finance staff use one admin desktop (usually the server) to transfer financial information from CSC's Inmate Accounting System on the CSC network to the POS server via USB key, and transfer information back the same way. Inmate financial information is then pushed to the canteen workstations, and record of inmate purchases are pulled from the canteen workstations to the server.

Another admin workstation is usually located in CSC Materiel Management and is used to enter inventory into the system and complete key mapping on the KB3000 input keyboard to correspond with the inventory items. These updates are pushed to the canteen workstations.

CSC IT staff at the institutions manually install updates to the application on the server via CD or USB key. Updates are then pushed to the canteen workstations and other admin workstations. A backup and archive of the database is done every night, and then the backup file is manually transferred to a CD.

The workstations in the canteens (the Front End Wickets) are set so that on start up they go directly to the POS application. The desktop is locked down so that the canteen user cannot access anything but the POS application, and when the canteen user logs off, the workstation automatically restarts. The peripherals attached to these workstations include:

- A monitor;
- A KB3000 input keyboard;
- An HHP IT3800 Linear Bar Code Scanner or a 2200VS or 2300HS Magellan Bar Code Scanner;
- An IBM 4610 Receipt Printer; and
- A Handscanner

The canteen workstations do not have a standard keyboard or mouse as peripherals. The desktop is encased in a metal box with a padlock. The canteen workstations use a custom built utility to interface the hand scanners with the POS application.

2. CSC Technical Architecture and Requirements

The targeted technical specifications for desktops and servers at CSC:

Component	Standard
Desktop OS	Windows 7 or Windows 10
Office Suite	MS Office 2013
Web Browser	IE11
Desktop JRE	1.8u33
Server OS	Windows Server 2012 R2
	Red Hat Enterprise Linux 6
Database Management	SQL Server 2013 Enterprise
	Oracle 12c

Web Server Software	Apache HTTP Server 2.6
	MS IIS 8 with NET 4.5.2

The majority of servers at CSC are virtual machines managed by VMware vSphere 5.5. In some cases, exceptions can be made in order to host a physical server.

Network centric solution: servers will be hosted at data centres managed by Shared Services Canada (SSC) and CSC will not be able to access servers directly. Application must be available through network links (i.e. through Internet Explorer).

SSC will not support a distributed architecture. Servers are required to be centralized at a single data centre, and to provide services to sites across Canada, including remote locations with slow internet. As well, many sites lose contact with the NHQ data centre for hours to days at a time. Any solution will have to be fully operable on site without connection to the central server. For example, data must be able to be cached on administration and materiel management desktops, for use during downtime, and changes uploaded to central database when network connections are re-established.

2.1 CSC Technical Architecture and Requests Questions

Q-1 Are there any elements outlined above, which raise challenges? If so, what are they?

Q-2 What key hardware and software elements does your POS solution include / require?

Q-3 Does your POS solution require implementation on a physical server? If yes, please explain requirements.

Q-4 Will your POS solution be able to provide reliable access to remote institutions across Canada using a centralized data centre model?

Q-5 Please provide a high-level description of the proposed physical and logical architecture of your POS solution.

3. CSC Security Requirements

The *CSC Standards for Inmate Access to IT Systems* must be complied with as per the following excerpt from CSC's Commissioner's Directive (CD) 225 on Information Technology Security:

Access by Offenders

Offenders will not be given access to CSC's IT systems, services or electronic information, unless approved under specific CSC programs. All such programs will be reviewed and approved by the Director, IT Security.

Offender access to CSC's IT systems, services or electronic information will be granted only after IT Security has completed an assessment and all recommendations have been implemented by the operational unit or the Program or Service Delivery Manager.

Offenders will be denied access to CSC's IT systems and services that are:

- *capable of retrieving personal information on members of the public, government employees or other offenders;*

- *capable of communicating with another computing device inside or outside the institution (other than approved printers or networks); or*
- *required to support the IT infrastructure of any facilities of the serviced agencies;*
- *Offender accessible devices, such as computers, game consoles or other electronic devices, are only permissible if they abide by the conditions outlined in this directive and;*
- *only if they are authorized by a CSC policy, an educational program, a work program or for legal discovery purposes; and*
- *after IT Security has completed an assessment and all recommendations have been implemented by the institution or the Program or Service Delivery Manager*

The following are notes to clarify how these requirements might be translated into technical considerations:

- Traffic between the inmate-accessed systems and back-office components need to be restricted by technical means, e.g. firewall and IDS, to the minimum required to support system operation – all other traffic must be blocked. The required traffic must be identified by source address; destination address; UDP/TCP protocol required and purpose.

- Transfers are to be initiated by a pull from the back-office components and not a push from the POS components on the Inmate network which is not connected to the CSC secure network.

- The aspect of physical security of the equipment in inmate accessible areas must be addressed to ensure that an inmate cannot tamper with the hardware and bypass the technical safeguards.

- Inmate-accessible IT systems to have current security patches and anti-virus and functionality restricted to the minimum required for the system to function.

3.1 CSC Security Questions

Q-6 How do you propose meeting the IT security requirements defined herein related to inmates being denied access to IT systems, services or electronic information that are:

- capable of retrieving personal information on members of the public, government employees or other inmates;
- capable of communicating with another computing device inside or outside the institution (other than approved printers or networks); or
- required to support the IT infrastructure of any facilities of the serviced agencies

Q-7 Are you aware of technology that would allow the implementation of a POS solution on CSC's wide area network while respecting the above defined security requirements? Please explain how the suggested solution would allow for off-line use at institutions.

Q-8 CSC currently has small standalone POS networks in each institution, resulting in a lack of centralized analysis and reporting. If you are unable to recommend a solution that will allow the institutional POS systems to be part of a centralized

network, can you recommend a solution that will allow for centralized analysis and reporting?

Q-9 Is your POS solution accredited/authorized in accordance with a recognized certification and Accreditation (C&A) process or Security Assessment and Authorization (SA&A) process?

Note: *CSC's C&A process is under review. Consideration is currently being given to the Guide to Certification and Accreditation for Information Technology Systems (MG-4) with Security Assessment and Authorization (SA&A) based on IT Security Risk Management: Lifecycle Approach (ITSG-33). Both MG-4 and ITSG-33 are available online. US vendors may be familiar with Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800-53) (rev.4), parts of which are incorporated into ITSG-33.*

Q-10 Would you participate in CSC's Certification and Accreditation (C&A) process?

Note: CSC's Certification and Accreditation (C&A) process is set out in the attached C&A Process Flowchart (Appendix 2).

Q-11 Are portable POS systems available? Can they work offline? If so, how are they synced with the main system while respecting CSC security requirements?

4. Questions on Peripheral Equipment

4.1 Biometric Identification

For security purposes, CSC requires biometric recognition devices to grant POS access to inmates, both clerks and clients. CSC currently uses Schlage ID3D and Schlage Handkey 2 hand scanners.

Q-12 Does your POS solution support the model of hand scanners currently used by CSC?

Q-13 What other models of hand scanners are supported in common canteen POS solutions? Where is the biometric information stored within the system?

Q-14 What other biometric identification technologies are supported, i.e., fingerprint identification?

Q-15 Are POS solutions modular enough to easily switch biometric identification methods in the future?

4.2 Keyboard

CSC currently uses Logic Controls KB3000 POS keyboards for inputting non-UPC purchases in the POS system.

Q-16 Does your POS solution support the model of keyboards currently used by CSC?

Q-17 What other technologies does your POS solution support for inputting non-UPC purchases into a POS system? How do these technologies hold up within a correctional or simliar environment?

4.3 Receipt printer

CSC currently uses Star 300, Star 312 and IBM 4610 Receipt Printers (RS-232 versions).

Q-18 Does your POS solution support the models of receipt printers currently used by CSC?

Q-19 What other models of receipt printers are supported in common canteen POS solutions?

4.4 Universal Product Code (UPC) Scanner

Wireless technologies are not permitted within federal institutions. CSC currently uses several models of non-wirless barcode scanners, including the Honeywell Hyperion 1300g barcode scanner (hand-held unit), Magellan 2300HS Horizontal Scanner (table top barcode scanner), and Unitech PC Wan 110 (pen style).

Q-20 Does your POS solution support any of the models of barcode scanners currently used by CSC?

Q-21 What other models of non-wireless barcode scanners are supported in common canteen POS solutions?

Q-22 Are there any emerging technologies that may make barcode scanners obsolete? What are the current industry best practices in this area?

4.5 Opportunities to consolidate peripherals

Q-23 Are there integrated POS peripheral devices that may make canteen setups more efficient and cost effective than what is presently configured at CSC?

4.6 POS trends in other Correctional Environments

Q-24 What biometric or other (i.e. ID cards) identification technologies are commonly used in POS systems within other correctional services and in other similar environments?

4.7 Other

Q-25 In centralized environments, how are the differences in barcode numbering for similar products addressed (i.e. a particular softdrink may have a different barcode in Vancouver than in Toronto)?

Q-26 Has your POS solution ever been integrated with biometric identity devices? If yes, please describe.

5. Other Proposed CSC POS Requirements

5.1 Interface with CSC Inmate Accounting System

As a minimum, the following three automated interfaces will be required between a POS solution and CSC's Inmate Accounting System (IASR) as USB drives are no longer deemed acceptable. The existing interface files are slash delimited text file.

- At the beginning of the canteen period (which is a recurring two week interval with a maximum spending limit of $90), the POS system will interface with IASR a file

containing the amount of canteen funds in inmate is requesting to be available in the upcoming canteen period;

- IASR will verify the requested amount against an inmate's available funds and place a hold on those funds. The approved requested funds will be interfaced to the POS system.
- At the end of the canteen period, the POS system will send an interface file to IASR containing the amount the offender actually spent in the canteen this period. NOTE: Upon completion of this transaction all canteen account balances in the POS system must be reset to $0 and no sales transactions can occur until the new period's information has been uploaded from the IASR.

5.2 Manage Account Balances

The application must maintain control over multiple inmate accounts and account balances. Currently, each customer has two account types: a Canteen Account and a Health and Hygine Account.

5.2.1 Canteen Account

- The POS system will automatically generate requests for the maximum canteen spending limit per inmate for active inmates to spend in their canteen account at the beginning of each canteen period (two weeks).
- The canteen operator can override the $90 maximum amount with a lesser amount upon the request of the offender with proper identification. This override amount will automatically be the requested amount going forward until the offender requests another change.
- Reduce the amount available in the canteen account as the offender makes purchases against this account
- The automatic and override requests will be interfaced to IASR to ensure funds are available.
- At the end of the canteen period, all unused balances in the canteen account revert back to the offender's 'bank' account in the Inmate Accounting System and resetting the offender's canteen account balance to zero.
- Provides the analysis and reporting capability at the individual inmate level and aggregate levels e.g. institution, region and national on account activity.

5.2.2 Health and Hygiene (H&H) Account

The POS system will:

- Automatically update an inmate's H&H Account each period with a set dollar value until the maximum dollar value is reached.
- Reduce the amount available in the H&H Account as an inmate makes purchases against this account
- Provides the analysis and reporting capability at the individual inmate level, and aggregate levels e.g. institution, region and national on account activity
- When an inmate is released, the health & hygiene account is reset to zero and the account is closed.
- An inmate's health & hygiene account is also reset to zero when the inmate is transferred to another institution.
- The administrator sends the health & hygiene balance to the receiving institution and it is entered as the inmate's opening balance in the account.

The last two bullets above represent the current process; CSC seeks this transfer to be automated.

Note:
(1) The POS system must be able to recognize products that are designated as H&H products. Inmates have the option of purchasing H&H products either from their regular canteen account or H&H account. For this reason, whenever an H&H product is selected, the system should ask the canteen operator if the product is to be purchased from the inmate's canteen or H&H account.

(2) The finance administrator requires the ability to manually adjust account balances at any time. An audit trail must exist for all changes to account information.

5.3 CSC Reporting Requirements

As a minimum, CSC requires the following reports on account balances, profit and loss report and period purchases by Account type (Canteen and Health and Hygiene); all reporting is required at the institution, region and national levels.

5.4 Other Proposed CSC POS Requirements Questions

Q-27 Does your POS solution address the other proposed CSC POS requirements identified above e.g. interfaces and management of accounts balances?

Q-28 What are the capabilities of your POS solution for generating custom reports?

6. Other Questions

6.1 Other Proposed CSC POS Requirements Questions

Q-29 Have you had any previous experience in delivering a POS solution within a correctional environment? If so, where and how did those requirements differ from ones identified herein?

6.2 Project Implementaiton

CSC anticipates that the provision and configuration of the POS software, testing, train the trainer training session and supplier oversight of 2 pilot installations (English and French for a 2 week cycle) will be complete within 150 business days of contract award and the complete implementation (48 sites) to be completed within 100 business days after the pilot implementation.

Q-30 Based on your experience in implementing your POS solution, is this reasonable? If not, what is a reasonable timeframe?

6.3 Licensing

Q-31 How do you license your POS solution? What is your licensing model for testint/development environments versus full production roll-out? Do you provide enterprise licenses?

Q-32 Are there other factors and/or functionality that should be considered?

Appendix 1 – Glossary of Acronyms

Acronym	Full Length
C&A	Certification and Accreditation
CD	Commissioner's Directive
CSC	Correctional Service Canada
IASR	Inmate Accounting System Replacement
ITSG-33	IT Security Risk Management: A Lifecycle Approach (ITSG-33) (https://www.cse-cst.gc.ca/en/publication/itsg-33)
MG	A Guide to Certification and Accreditation for Information Technology Systems
NHQ	National Headquarters
NIST 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
POS	Point of Sale
RFP	Request for Proposal
SA&A	Security Assessment and Authorization
UPC	Universal Product Code