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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
Application Software-RFI

Solicitation No. - N° de l'invitation	Date
G9292-211695/A	2019-02-14
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
G9292-211695	PW-$$XL-108-34622
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
108xl.G9292-211695	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2019-03-06

Time Zone
Fuseau horaire
Eastern Standard Time
EST

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

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Fenwick, Wesley	108xl
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 720-7743 ( )	( ) -

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

EMPLOYMENT AND SOCIAL DEVELOPMENT CANADA
NCR - Gatineau
140 PROMENADE DU PORTAGE
GATINEAU
Quebec
K1A0J9
Canada

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
Shared Systems Division (XL)/Division des systèmes partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Canada

APPENDIX A - DRAFT REQUEST FOR INFORMATION (RFI)

Employee Activity and Information Access Monitoring

On Enterprise Applications Software (EAIAMS) Solution

TABLE OF CONTENTS

REQUEST FOR INFORMATION REGARDING

EMPLOYEE ACTIVITY AND INFORMATION ACCESS MONITORING ON ENTERPRISE APPLICATIONS (EAIAMS)

FOR

EMPLOYMENT AND SOCIAL DEVELOPMENT CANADA

PART A:

1. Background and Purpose of this Request for Information (RFI)

a) Employment and Social Development Canada ("ESDC") is issuing this Request for Information (RFI) to solicit information from Vendors as to what solutions are available on the market to "monitor employee activity and information access on enterprise applications" (hereby called "solution") that contain sensitive information.

2. Nature of Request for Information

a) 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.

3. Nature and Format of Responses Requested

a) Respondents 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. Respondents 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.

4. Response Costs

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

5. Treatment of Responses

a) 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. 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 the client (where applicable) and Public Services and Procurement Canada (PSPC) will review the responses. Canada 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.

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) Post-Submission Review Meetings: Canada may, in its discretion, request individual Post-Submission Review Meetings with selected respondents to provide clarity on information provided, or to invite a presentation about some or all of the proposed solution. If required, these will be held at the most appropriate location, to be determined at a later date. The intent of these meetings will be to provide an opportunity for a face-to-face discussion with respondents. Although respondents may request a meeting, and their request will be considered, Canada will determine whether it requires additional information from any given respondent and will schedule meetings accordingly. All such requests, by respondents, should be forwarded to the Contracting Authority. Note that a maximum of 2 hours will be set aside for any meetings with respondents. Any costs associated the Post-Submission Review Meetings, including travel cost, will be borne by the respondent.

e) The information gathered from this RFI will be used to inform the requisite RFP to procure an Employee Activity and Information Access Monitoring solution.

f) This RFI contains an overview and summary of the associated programs to procure an Employee Activity and Information Access Monitoring solution. Interested vendors are asked to contact the Contracting Authority for supplementary details that will provide more context and the specific questions addressed to the industry.

6. Volumetric Data

The volume projections in Part B are being provided to respondents purely for information purposes. Although they represent the best information currently available to PSPC, Canada does not guarantee that the data is complete or free from error.

7. Format of Responses

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

b) **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 respondent's response and the volume number;

the name and address of the respondent;

the name, address and telephone number of the respondent's contact;

the date; and

the RFI number.

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

d) **Number of Copies**: Canada requests that respondents submit 1 electronic copy of their responses via e-mail to the Contracting Authority listed herein.

8. Enquiries

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

Contracting Authority:	Wesley Fenwick
E-mail Address:	Wesley.Fenwick@tpsgc-pwgsc.gc.ca
Telephone:	613-720-7743

9. Submission of Responses

a) Time and Place for Submission of Responses: Suppliers interested in providing a response should deliver it to the Contracting Authority identified above by the time and date indicated on page 1 of this document.

b) Responsibility for Timely Delivery: Each respondent is solely responsible for ensuring its response is delivered on time to the correct location.

c) Identification of Response: Each respondent should ensure that its name and address, the solicitation number and the closing date appear legibly on the response.

PART B:

1. Organization Overview

a) Employee and Social Development Canada (ESDC) is a department of the Government of Canada responsible for social programs and the labour market at the federal level. ESDC's mission is to build a stronger and more inclusive Canada, to support Canadians in helping them live productive and rewarding lives and improving Canadians' quality of life.

b) ESDC delivers a range of programs and services that affect Canadians throughout their lives. The Department provides seniors with basic income security, supports unemployed workers, helps students finance their post-secondary education and assists parents who are raising young children. The Labour Program contributes to social and economic well-being by fostering safe, healthy, fair and inclusive work environments and cooperative workplace relations in the federal jurisdiction. Service Canada helps citizens access ESDC's programs, as well as other Government of Canada programs and services.

c) In particular, the Department is responsible for delivering over $120 billion in benefits directly to individuals and organizations through such Government of Canada programs and services as Employment Insurance, Old Age Security, the Canada Pension Plan and the Canada Student Loans Program. The Department also provides $1.8 billion in funding to other orders of government, educators and organizations in the voluntary and private sectors.

2. Description of the Current Environment

a) ESDC currently has approximately 24,000 employees, and over 500 enterprise applications (of which around 100 are mission critical) that are utilized to carry-out its mandate. Employees and application usage is geographically dispersed across Canada, with headquarters in Ottawa, Ontario. Many of these applications are used to deliver benefits to citizens, are custom on-premise systems, and will be modernized over the coming decade. A majority of these applications contain sensitive information, which internal staff access in order to carry out their duties. Some systems have log files that provide information on user application activity, however the quality and usability of log files varies across applications and some applications do not have log files. Enterprise applications are accessed through government-issued personal computers, laptops, and tablets. Most users are from within ESDC and some users from other Government of Canada departments and Provincial government entities. Appendix C provides additional details on the current technical environment.

b) In its 2017-2018 Departmental Plan, ESDC identified that there is a risk that ESDC's personal and sensitive information may be inadvertently or inappropriately accessed, used, disclosed and/or disposed of by employees or third parties. Risk response strategies include implementing a broader strategy for managing personal/sensitive information and to review current privacy and security practices to safeguard personal and sensitive information. The risk response approach also includes utilization of technology(ies) (in addition to controls, processes, policies, and resources) to support monitoring, detection, analysis and investigation of inappropriate internal access or misuse of information on enterprise applications.

3. Description of Desired Solution and Future Vision

a) ESDC is exploring market offerings to monitor and analyze enterprise application activity in order to detect and manage potential incidents of inappropriate internal access or use of information. Initially, the department would like to use the technology on 2-3 major in-house, custom-developed, enterprise applications, with a plan to take a risk-based approach in extending the technology and capability to additional enterprise applications. As the software solution is expected to evolve and mature over time, ESDC will expect to continue uninterrupted access, usage, and development of the product across the solution's lifespan.

b) Canada reserves the right to, at a subsequent date and at its sole discretion, identify the solution either as a multi-departmental solution, or designate the solution as a Government of Canada Enterprise-wide standard if and when determined by the GC-Enterprise Architecture Review Board (GCEARB).

c) Based on the department's requirements, ESDC is exploring **Security Information and Event Management (SIEM)** and/or **Employee Monitoring (EM)** technologies to address this risk. The department is looking for a solution that:

I. Monitors specified applications and detect incidents of inappropriate information access using (a) defined business rules, and (b) advanced analytical capabilities to flag potential incidents independent of predefined business rules for users accessing enterprise applications
II. Utilize a broad range of data sources (such as log files including O/S event logs, database records, flat files, vendor specific APIs, Cloud / SaaS sources etc.) to detect potential cases of information misuse and malfeasance as users perform transactions.
III. User-centric analysis that flags potential incidents based on user activity/behavior patterns and information across devices, applications, and information sources, so that they can be investigated.
IV. Ability to monitor and detect potential incidents independent of the use of log files to recognize patterns of user behaviour with enterprise applications.
V. Produces irrefutable evidence that is efficient to review and understand by investigators and department managers which confirm whether inappropriate information access or use has occurred.
VI. Automatically take defined actions based on triggers (e.g. auto-notifications to users of potentially inappropriate behavior) in support of operational and investigative efficiency
VII. Classifies incidents to enable triaging incidents based on level of risk to support efficiencies and workflows and workloads for investigators.
VIII. Integrates with existing case management solutions utilized within ESDC (and/or have case management capabilities that can be utilized broadly by the department). ESDC has existing case management system in place.
IX. Is accompanied with managed services will be needed to support ESDC's operational readiness, implementation, configuration, integrations, training, and application support. ESDC needs to be able to implement the solution quickly and review the operational considerations and options to support a software or service.
X. Has data residency in Canada, bilingual capabilities in English and French, and meets the accessibility requirements of the Government of Canada. Data must reside in Canada and is protected B.
XI. Has the ability to be leveraged by other Government of Canada Departments, Agencies, and Crown Corporations and/ or Provincial Crown entities.

4. Anticipated Volume

Metric	Initial Roll-Out	Potential Future State
Number of Enterprise Applications to Monitor	4	130
Number of Enterprise Application Users to Monitor	13,100	25,000
Number of Concurrent Users	5,600	TBD
Transaction volume / Year	107,010,000	TBD

ANNEX A: INDUSTRY QUESTIONS

Respondents are requested to provide a detailed response, addressing each of the following questions:

	Company Profile
A1	**Presence in Canada**: Do you have offices in Canada?
A2	**Relevant Experience – Information Access:** What is the number of current active and completed implementations at a similar scale and complexity as our organization? Please provide closest match to requirements that are comparable in terms of industry, scale, geography/localization, complexity, and regulatory compliance needs. What are some best practices that can be leveraged from these experiences?
A3	**Relevant Experience and Knowledge – Government of Canada:** Does your company have current or past relevant experience with other federal departments within the Government of Canada, Canadian Provincial Governments, or any large federal government departments in other jurisdictions. Please provide some examples.
A4	**Financial Viability**: Provide information that summarizes your recent performance in new software license revenues, client retention rate, profitability performance, R&D spending and priorities, and other information that you feel would help ESDC understand your financial health and viability
A5	**Company Security**: Demonstrate how you comply with the current Government of Canada standards referenced in Annex B. Indicate if you have been subject to the security requirement contained in Annex B by providing references of Departments or Agencies using your solution.
A6	**Product Roadmap**: Describe your company vision and product roadmap as it relates to Monitoring Employee Information Use and Access on Enterprise Applications offerings with a clarity on what differentiates your proposed solution from the competition?
A7	**Services Strategy:** Describe what services you offer supporting your clients as it relates to Monitoring Employee Information Use and Access on Enterprise Applications offerings with specific details on partnerships or other market approach.
A8	**Client References:** Please provide three reference for comparable clients for whom you have implemented an information misuse solution of similar nature. At least one Canada Public Sector client is preferred.

Product Questions – Functional

B1	**Monitoring Employee Information Use and Access on Enterprise Applications –** Please describe your product's capabilities to monitor and detect inappropriate internal access and use of information on custom, in-house enterprise applications. What type of technology is it (Security and Information Event Management (SIEM), Employee Monitoring (EM), etc.)?
B2	**Method of Monitoring Application Activity** – How is application information use and access monitored by the product? At what level is the product monitoring (end-point device, server, network) and exactly what does it monitor (application screen activity on end-point device, application log files, etc.) Does it depend on any integration(s) with the application or to the database? Does it generate a record of user activity on the application or depend on another source of information for that (e.g. Application log file). If it requires a record of application user activity (e.g. Application log file), what information is required within those files?
B3	**Detection Sensitivity and False Positives –** Please describe average increase in number of verified cases of inappropriate access, inappropriate information usage, or internal fraud after your solution is implemented on sites similar to ESDC. What type of false positive rate, on average, is observed with your product initially, and after a "tuning" period? What capabilities does the product have to reduce the rate of false positives?
B4	**Additional Data sources** – What type of data sources can, or are typically, ingested by the product to enrich the detection capability? As an example can it utilize data from HR platforms (e.g. PeopleSoft), building access data, and information security software files and information? Describe what sources it can collect data from (e.g. log files, O/S event logs, database records, flat files, vendor specific APIs, Cloud / SaaS sources etc.) and how data collection is achieved
B5	**Detection Based on Business Rules –** Does the product allow detection of potential incidents based on business rules? Describe how these rules are defined and "coded", and what skill sets are required to define and implement them? Can you describe the nature of and provide an estimate of how much support do you need from the ESDC to define these business rules?
B6	**Advanced detection independent of business rules** – Does your solution have advanced analytics (machine learning, etc.) capabilities to monitor and flag incidents based on patterns of user behavior, independent of defined business rules? Describe in detail how these capabilities work, what information is needed, how the system needs to be trained for this, how long does this training take, and the skill sets required to train the system
B7	**Advanced detection of user behavior across devices / applications:** – Does your solution have "user entity and behavior analytics" (UEBA) capabilities / advanced analytics (machine learning, etc.) to monitor and flag incidents based on patterns of user behavior across devices, applications, and time periods? Please describe these

	capabilities in detail. How does the product attribute incidents to specific people (users vs. devices)?
B8	**Product "Tuning"** – Please describe whether and how the product needs to be configured / tuned / trained to develop an optimal level of detection accuracy and effectiveness. How long would this "refinement" period typically take? What type of information is needed? What is required by the customer?
B9	**Collusion** – Can the product detect collusion across multiple internal users? Describe how the product does this?
B10	**Automation –** Describe any automation capabilities in executing customized actions in response to triggers and risk of potential incident (e.g. Email first-time offenders of potential inappropriate behavior)? How are these automated actions defined and configured? Please describe the depth and breadth of these capabilities.
B11	**Classifying and Ranking Incidents by Risk Level –** Does the product have capabilities to classify and/or rank incidents by risk level (e.g. criticality, volume, etc.). Is it a configured automated or a manual assignment capability? Please describe how this works.
B12	**Triage and Workflow Management by Risk** – Describe any capabilities to triage and manage the volume of potential incidents according to risk? Is this manual or automated? Please describe how this works.
B13	**Evidence –** Please describe in detail what type of evidence the product produces for investigators and business unit managers to assess and confirm incidents of information misuse and malfeasance. Is it a video, screen-shot play-back of user actions on applications based on detection triggers? Is it a report? Please describe this in detail.
B14	**Selective Monitoring –** Can the customer define what is being monitored (e.g. monitor application x and y, and not email, web activity, etc.)?
B15	**Analytics –** Beyond analytical capabilities utilized for detection, please describe any additional analytical capabilities the product has
B16	**Reporting –** What type of information can be reported from the system? Are reports configurable? What file format are the reports? Does your product have plug-ins for common business intelligence platforms and applications?
B17	**Timeliness –** What is the lag between when an incident occurs and when an alert is generated? Does your solution offer real-time detection? Batch-processing during off hours?
B18	**Case Management** – Can this system support case management? Can it integrate with other systems that support case management and workflows?

Product Questions – Technical	
C1	**Number of Applications**: What is the total number of enterprise applications that the product can monitor? Describe how you provide scalability of the solution. What is the largest number of applications for a single organization that has been implemented?
C2	**Number of Users**: How many total application users can be monitored by the system? How many concurrent users? What is the largest number of users for a single organization that has been implemented?
C3	**Transaction Volume:** What is the range (minimum, maximum) of transaction volume that your solution is designed to accommodate? At what level of transaction volume does product performance become negatively impacted?
C4	**Deployment**: Is the product deployed on end-point devices, or does it operate on a central server? Where is information generated (end-point?), and where is information stored?
C5	**Internal Network bandwidth:** Based on the user and application volume metrics, what would be the internal network bandwidth requirements? How much load/strain would the solution place on the internal network?
C6	**Storage**: Based on the user and application volume metrics, provided, how much storage would be required?
C7	**Devices –** On what devices can the product monitor enterprise application activity by internal users (personal computers, tablets, smart-phones, etc.)
C8	**User Configuration:** Describe what level of configuration is available – what can be configured and how? Can it be configured by the customer independently from your company? What level of expertise is required to configure the system? What parts of the solution need to be configured jointly with, or solely by your company?
C9	**Customization:** What parts of the solution can, or would need to be customized, to meet customer requirements? Can any components of the solution be customized by the customer beyond built-in configuration options?
C10	**Cloud / On-Premise:** Is your solution offered on premise, Cloud-based, Software as a Service (SaaS) or a managed service? Is any of the data associated with your solution stored in the cloud? If so, specify the name and location of the cloud service provider? Is any of the data associated with your solution stored outside of Canada? If so, where?
C11	**Connectors / Integration to Information Security Applications:** Please describe what types and vendors of information security software your product can connect with? How

	does it work with those products (File transfers? Plug-ins? Hard-coded integrations?). Examples include access control software, authenticators, endpoint monitoring software, DLP monitoring software, etc.
C12	**Accessibility**: Does your solution support and adhere to Government of Canada accessibility requirements, including the GC's Web Accessibility Toolkit (WET), and Web Content Accessibility Guidelines (WCAG 2.0AA (Reference: WET and WCAG 2.0AA)?
C13	**Bilingual**: Does your solution support the GC's bilingualism standard under the Official Languages Act (English/French)?
C14	**CATS**: Is your solution compliant with the Cyber-Authentication Technology Solution (CATS) specifications version 2.0? Does it have the required flexibility to adapt to future versions of the CATS specifications?

Product Questions – Information Security and Architecture	
E1	**Connectors / Integration to Information Security Applications:** Please describe what types and vendors of information security software your product can connect with? How does it work with those products (File transfers? Plug-ins? Hard-coded integrations?). Examples include access control software, authenticators, endpoint monitoring software, DLP monitoring software, etc.
E2	**Supported Platforms**: What computing platforms does your solution support? Please specify server OS and supported browsers (across all device types).
E3	**Access:** Describe the level of access customers have to the vendor's development and collaboration tools (e.g. source code repository, continuous integration and automated testing tools, plug-ins, etc.).
E4	**Programming Language:** What programming language was used to develop your application? Is the software written in a commercially available development language that is still being enhanced and supported by the supplier?
E5	**Architecture overview:** Please provide an overview of your solutions architecture
E6	**Safeguarding Information**: How does your solution safeguard confidential information that it collects, stores or transmits (e.g. Protected B, investigation details, etc.) to ensure a high degree of information integrity?
E7	**Administration**: Describe your solution's administrative functions (e.g. account management, access control, logging, intrusion, alerts, etc.)
E8	**Security certifications**: Does your solution have any security certifications or assessments?

E9	**Disaster Recovery:** Describe your disaster recovery (DR) and business continuity approach for the following: • Your own product/service platform if offered as an external cloud solution • Client specific data/ IP assets that are in scope of services provided?

Implementation, Training, Support, and Managed Services	
F1	**Readiness Assessment**: Describe what steps are taken to assess and assist a customer on their readiness to adopt your solution? What are the components of the assessment? What does the customer need (technically and operationally) in-place prior to implementation
F2	**Implementation Steps**: Describe the steps to implement your solution. Presuming the IT infrastructure was in place, how long would it take your staff to install your system, configure and make it ready for production? Typically, how long would it take for a client to complete this work themselves, with and without technical support?
F3	**Implementation Methodology**: Describe your methodology, including tools and processes to use for a successful implementation. Describe the processes to support acceptance testing, UX, interoperability/integration testing, performance testing, security and migration testing and subject matter expertise that would be available to support implementation.
F4	**Implementation Risks**: What are the typical implementation risks encountered with other projects of similar size and scope? What actions have you put in place to minimize these risks?
F5	**Testing:** What is your typical role in testing, release management and maintenance phases?
F6	**Transition to Acceptance:** How would the vendor support ESDC during the transition from 'go live' to 'final acceptance'?
F7	**Third Party Services**: Describe whether any third-party services are required for implementation and support. Are these resources typically the responsibility of the client (ESDC) or the vendor?
F8	**Implementation Services**: What services does your company provide to support implementation of the product?

F9	**Configuration and Solution "training" Services**: What services does your company provide in configuring the solution including initial configuration, business rule coding, business rule development, "training" / tuning the solution, reporting, etc.?
F10	**Integration Services**: What services does your company provide in supporting any required integrations / connections to other software platforms?
F11	**Training**: What product training is available pre and post installation? Do you provide training, user manuals and support in both English and French? How is training tailored and delivered to different user types: administrative (IT and information security), super-user, investigator end-user, business unit manager end-user, analysis staff, etc.
F12	**Client Resources and Activities**: What activities and type/level of ESDC resources would be required to implement your standard solution?
F13	**Support Model:** Describe your maintenance and support model and what is included. (e.g. on-site vs remote support, hours of operation, language support**,** response time by level of incident/issue, etc.). How do you share your performance (daily, weekly, or monthly) in handling support requests?
F14	**ESDC Support Resources**: What are the activities and the type/level of resource expertise ESDC would require to maintain your solution on an on-going basis?
F15	**Release Management:** How often do you issue a new release/version? What is your release/version strategy? How long does it take, on average, to implement a new release/version? How many versions do you support? (e.g. is the current version the only one supported, or are previous versions also supported?) For how long is a version supported, after a newer version is released? (e.g. does support on the current version expire as soon as the next one is released?) How much in advance do you normally announce a version will be End of Life (EOL)?
F16	**Patch Management**: What is your patch management strategy? How long does it take, on average, to implement patches? What is the effort involved in resources and cost?
F17	**Communication**: How do you inform your clients of new releases and critical upgrades? How do you share your performance (daily, weekly, or monthly) in handling support requests?
F18	**Relationship Management**: How would support for an organization of ESDC's size and complexity be typically managed (e.g. dedicated support personnel, call center, etc.)

Pricing and Licensing	
G1	**Distribution**: Do you distribute your software solution in Canada directly or via an authorized third party?
G2	**Modules**: Describe what functional modules (components) are included in the base solution and what additional functional modules (components) are available.
G3	**Costs**: Describe the basic solution costs and identify incremental costs for solution options that are complementary add-ons to enhance the basic solution, include standard streams and category descriptions for professional services.
G4	Describe the pricing models for the solution and which option you would recommend. For example, is your preferred model one of the following: • purchase product and implementation services from the solution vendor • purchase licenses and contract with an implementation partner • purchase software and complete the implementation using in-house ESDC personnel or is there another option you would present, please explain.
G5	Enhancements: Describe the pricing model for enhancements, such as adapting or modifying the solution post-implementation based on client feedback.
G6	Licensing Model: Describe your solution's licensing model. If your solution is available in an enterprise-license configuration, please describe the conditions necessary to qualify for an enterprise license, including any minimum investment in terms of money or other licenses.
G7	Expansion: Does your licensing model allow for expanding the proposed solution to other Government of Canada departments and/or agencies?
G8	Please provide an order of magnitude annual price range for solution and services you have provided to a comparable organization such as ESDC. Feel free to make reasonable assumptions about scale and scope and state the major price impacting assumptions in your response.

ANNEX B: VENDOR SECURITY REQUIREMENTS

A detailed security review will be required to determine the security requirements for vendors selected to work on this project. The following security requirements are provided as a guide and may be subject to change:

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 Canadian Industrial Security Directorate, Public Services and Procurement Canada.

The Contractor/Offeror personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the Canadian Industrial Security Directorate (CISD), Public Services and Procurement Canada (PSPC).

The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CISD/PSPC has issued written approval. After approval has been granted or approved, these tasks may be performed up to the level of PROTECTED B, including an IT Link up to the level of PROTECTED B.

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

The Contractor/Offeror must comply with the provisions of the:

Security Requirements Check List and security guide (if applicable)

Industrial Security Manual (Latest Edition).

Vendors will not be required to adhere to these requirements for the purposes of the RFI.

ANNEX C: TREASURY BOARD POLICIES

The Service Provider must comply directly with all relevant federal policies, directives and guidelines including namely:

Policy Framework for Information and Technology
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12452&section=text

Policy on Information Management
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742

Policy on Management of Information Technology
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12755

Operational Security Standard: Management of Information Technology Security (MITS)
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text

Guideline on Defining Authentication Requirements
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262&section=text#sec1.2

Policy on Acceptable Network and Device Use
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=27122

Policies, Standards and Directives governing on-line service delivery, including but not limited to: (These Web Standards replace Common Look and Feel 2.0 (CLF 2.0)

Web Standards for the Government of Canada
http://www.tbs-sct.gc.ca/ws-nw/index-eng.asp

Standard on Web Accessibility
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601

Standard on Web Usability
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=24227

Standard on Web Interoperability
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25875

Common Look and Feel Standards for the Internet, Part 4: Standard on E-mail
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25439

Policy on Internal Audit

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16484

Communications Policy of the Government of Canada
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12316

Federal Identity Program Policy
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12314

Directive on Identity Management
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577

Standard on Identity and Credential Assurance
www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776

Policy on Privacy Protection
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510

Policy on Access to Information
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453

Directive on the Administration of the *Access to Information Act*
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18310

Policy on Government Security
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

Operational Security Standard on Physical Security
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329&section=text

Policy on Financial Management Governance
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14005

Standard on Social Media Account Management
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27033

Additional policies, standards, guidelines and directives can be found in their entirety on the Treasury Board Secretariat of Canada website: www.tbs-sct.gc.ca.

ANNEX D: ENTERPRISE ARCHITECTURE PRINCIPLES

The Service Provider's solution should demonstrate alignment with the following Government of Canada Enterprise Architecture Principles:

Scope: GC Enterprise First, GC Enterprise Clusters Second, Department Uniqueness Last

Reusability: Reuse First, Buy Second, Build Last

Business and Users First

Client and Service Oriented

Information, including data, is an Asset

Interoperability

Open by Default, Proprietary only by Necessity

Mobility Preferred

Secure by Design

Privacy Aware

Cloud First

Technology Debt Managed