RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Jason Knowles
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Tower C - Office 12C1 - 102-62
jason.knowles@pwgsc-tpsgc.gc.ca
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 956-1418

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
Email Transformation Initiative

Solicitation No. - N° de l'invitation	Date
2B0KB-123327/B	2012-06-21
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
20123327	PW-$TSS-002-24571
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
002tss.2B0KB-123327	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2012-07-18

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
Knowles, Jason	002tss
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(819) 956-1418 ( )	(819) 956-5165

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

SHARED SERVICES CANADA
AIRPORT PARKWAY DATA CENTRE
700 MONTREAL RD., BLDG C, 8TH FL.
OTTAWA
Ontario
K1A0P7
Canada

Comments - Commentaires
National Security Exception: The procurement related to this initiative is subject to National Security Exception and is, therrefore, excluded form all of the obligations of the trade agreements.

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
Data Centre Services/Services des centres de traitement de données
5C2, Place du Portage, Phase III
11 Laurier Street
Gatineau
Québec
K1A 0S5

Canada

The documents for this Letter of Interest are attached

Shared Services Canada

Email Transformation Initiative

Request for Information

Table of Contents

National Security Exception

National Security Exception*: The procurement related to this initiative is subject to National Security Exception and is, therefore, excluded from all of the obligations of the trade agreements.*

Purpose and Contents of this Request for Information

This is a Request for Information pertaining to the Email Transformation Initiative of Shared Services Canada. It is a document written for the purpose of eliciting feedback from industry in regards to the Email Transformation Initiative. The general contents of this Request for Information document are:

- **PART I - Request For Information Process**: Information about the intent of this Request for Information and the procedure for industry to follow for responding to this Request for Information;
- **PART II – Background of the Email Transformation Initiative**: Shared Services Canada's mandate, Email Transformation Initiative business objectives, proposed procurement approach, scope, and service delivery options;
- **PART III – Anticipated Mandatory Requirements**: Requirements that Canada expects potential bidders to comply with;
- **PART IV - Questions**: Questions asked to elicit feedback from industry that will help Canada shape the procurement approach and email transformation strategy going forward, and
- **Annex A to J** – Reference information and proposed mandatory and rated corporate evaluation criteria.

PART I: REQUEST FOR INFORMATION PROCESS

1. INTRODUCTION

This is a Request for Information (RFI) pertaining to the Email Transformation Initiative (ETI), which is an initiative of Shared Services Canada (SSC) to deliver a new Email Solution[1] for SSC and the departments and agencies that it provides information technology (IT) services for, herein, referred to as SSC's "Partners". SSC will also offer the new service to other Government of Canada (GC) organizations[2] on an optional basis.

Public Works and Government Services Canada (PWGSC) and SSC are seeking feedback from industry on the following subject matter:

(i) The ability to meet the anticipated mandatory requirements provided in Part III of this RFI;
(ii) The questions provided in Part IV of this RFI;
(iii) Industry's recommendations for a low risk approach that could be considered by SSC to deliver a consolidated email service to the GC that would meet the business, timeline, and cost reduction outcomes presented throughout this document, and
(iv) The ability to meet anticipated (draft) evaluation criteria (mandatory and rated) in Annex D.

The GC intends to use feedback from (i), (ii) and (iii) to solidify its procurement approach and help determine the "way forward" for how the new Email Solution should be acquired, delivered, and managed, and feedback from (iv) to help determine the mandatory and rated evaluation criteria for organizations to respond to at the next stage of the procurement process, in which Canada will identify a subset of successful respondents for subsequent stages in the procurement process.

1.1 Nature of this Request for Information

This is not a bid solicitation. This RFI will not result in the award of any contract. 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 Email Solution provider responds to this RFI, it will not preclude that provider 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 subject matter described in this RFI.

---

[1] An Email Solution can be composed of any combination of one or more IT systems, communication networks, servers, server applications, and client applications, etc., either implemented, operated and managed in a GC environment, or provided as a service by a commercial service provider.

[2] A complete list of GC organizations can be found at: http://www.tbs-sct.gc.ca/gov-gouv/tools-outils/org-eng.asp. Other government organizations are those listed on this web site that don't include SSC and its Partners, which are provided in Annex E.

2. INSTRUCTIONS FOR RESPONDING TO THIS REQUEST FOR INFORMATION

2.1 Terminology

Terms used throughout this RFI have been defined in Annex A – Glossary of Terms.

2.2 Response Costs

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

2.3 Treatment of Responses

Use of Responses: Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify the procurement approach, as well as any draft documentation 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.

Review Team: A review team composed of representatives of SSC and its Partners (where applicable) and PWGSC will review the responses. Canada reserves the right to hire any independent consultant, or use any GC resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

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.

2.4 Follow-up Activity

Canada may, in its discretion, contact any Respondents to follow-up with additional questions or for clarification of any aspect of a response either in writing or via RFI One-on-One meetings, as described in the ETI Industry Engagement Day notice on www.merx.com. Canada currently anticipates holding RFI One-on-One meetings with certain respondents on July 27, 28, and 30, 2012; however, these dates are subject to change.

2.5 Contents of the RFI

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

2.6 Volumetric Data

The data contained within this RFI is being provided to Respondents purely for information purposes. Although it represents the best information currently available to SSC, Canada does not guarantee that the data is complete, up-to-date, or free from error.

2.7 Format of Responses

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.

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

(i) The title of the Respondent's response and the volume number;

(ii) The name and address of the Respondent;

(iii) The name, address and telephone number of the Respondent's contact;

(iv) The date, and

(v) The RFI number.

Number of Copies: Canada requests that Respondents submit their response in unprotected PDF (e.g. no password) format by email to ConsultationSPC.SSCConsultation@tpsgc-pwgsc.gc.ca if the size of the document is less than 6MB. Alternatively, Canada requests that Respondents save a copy of their PDF (2003 or later) document onto each of 2 compact discs (CD-R) or 2 digital video discs (DVD-R) and send the discs by mail to the address specified in section 2.8. PDF format is being requested to allow Respondents to include any material (e.g. spreadsheet, white paper, brochure, etc.) with their written documentation in one file.

2.8 Enquiries

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

Contracting Authority: Jason Knowles

Department of Public Works and Government Services
Place du Portage III, 12C1
11 Laurier Street
Gatineau, Quebec
K1A 0S5

Email Address: SSCConsultation.ConsultationSPC@tpsgc-pwgsc.gc.ca

Telephone: 819-956-1418

Facsimile: 819-956-5165

2.9 Submission of Responses

Time and Place for Submission of Responses: Organizations interested in providing a response should deliver it to the Contracting Authority identified above by 2:00 p.m. EDT on July 18, 2012.

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

Identification of Response: Each Respondent should ensure that its name, return address, the solicitation number and the closing date appear legibly on the outside of the response.

PART II: BACKGROUND OF THE EMAIL TRANSFORMATION INITIATIVE

3. ORGANIZATIONAL OVERVIEW

3.1 Overview of Shared Services Canada

IT is essential to support daily federal government operations and to deliver services to Canadians. In the past, each government department and agency managed and operated its own IT infrastructure. This resulted in fragmentation, duplication and inefficiencies.

To address the situation, the Government of Canada (GC) created Shared Services Canada (SSC) on August 4, 2011, with the mandate to consolidate the organizational units of data centre, email and telecommunication services for the departments and agencies listed in Annex E[3].

SSC was given the mandate, in alignment with Budget 2011, to improve "the efficiency and effectiveness of government operations and programs to ensure value for taxpayer money."[4]

In the announcement of the creation of SSC, Public Works and Government Services' Canada Minister Rona Ambrose stated that:

> *"Shared Services Canada will have a mandate to streamline and reduce duplication in the government's IT services. Taking action will help our Government reduce duplication, and over time, our government footprint. It will also strengthen security and the safety of government data to ensure Canadians are protected."*[5]
>
> *"Shifting from costly, department-specific custom solutions to a whole-of-government standardized approach will help us improve services at a lower cost to Canadians. By creating Shared Services Canada, we are ensuring that Canadians are receiving the most efficient IT services possible, and that their money is being used responsibly."*[6]

SSC will standardize and consolidate the existing individual IT infrastructures and support organizations related to data centre, as well as the email and telecommunication services of SSC and its Partners, and transform these services to whole-of-government enterprise services, resulting in significant operational efficiencies and economies of scale.

Specific to email services, Shared Services Canada has launched the Email Transformation Initiative (ETI). The primary objective of the ETI is to replace

---

[3] http://www.pco-bcp.gc.ca/oic-ddc.asp?lang=eng&Page=&txtOICID=2011-876&txtFromDate=&txtToDate=&txtPrecis=&txtDepartment=&txtAct=&txtChapterNo=&txtChapterYear=&txtBillNo=&rdoComingIntoForce=&DoSearch=Search+%2F+List&viewattach=24553&blnDisplayFlg=1
(Privy Council Order P.C. 2011-876 to P.C. 2011-887, August 4, 2011)

[4] Budget 2011, The Next Phase of Canada's Economic Action Plan, June 6, 2011

[5] Rona Ambrose, Minister, Shared Services Canada, August 4, 2011

[6] Ibid.

existing email systems with a consolidated[7] Email Solution for the Government of Canada. The solution will be deployed to each of the departments and agencies that SSC serves. SSC will also provide this same email service on an optional basis to the remaining departments and agencies.

3.2 Overview of Email within Shared Services Canada

A key element of IT infrastructure is electronic mail, or email. Email has become a preferred communications medium for both internal use for government business and external use with Canadian citizens and industry. By nature of the tool, email has also served as an important record-keeping environment, essential to government operations.

Although the federal government has IT architectural policies and guidelines in place, there are still many disparate infrastructures currently provisioning a multitude of email systems. Each Partner department and agency has traditionally operated Email Solutions with varying versions and release levels, and with varying levels of maintenance and security. Each email system has been procured separately and has been operated and supported by individual department and agency management processes and IT support models.
The net result is that the Partner departments and agencies for which SSC provides infrastructure services operate 63 separate and distinct email systems. Many of the 63 separate email systems are implemented in a decentralized manner, with email related servers distributed in hundreds of locations. Also note that several of these systems manage Classified information up to the Secret level.

When considered at the enterprise level, this fragmented implementation represents an environment that is complex, inefficient, and expensive, as demonstrated by the following:

(i) There is no standard for email across the GC;
(ii) There are compatibility issues between the GC email systems, and
(iii) The operation of multiple email systems across the government results in departments and agencies maintaining separate licenses and having their own technical support teams.

Please refer to Annex C: Current State Summary, for more information on the current email environment for SSC's Partners.

[7] Consolidated in this context means that the chosen ETI solution will satisfy SSC and its Partners' email requirements.

4. BUSINESS DRIVERS AND OBJECTIVES

4.1 Business Drivers

4.1.1 Complexity

The GC, in its entirety, has hundreds of different email system configurations serving its employees. Within the Partner departments and agencies, there are 63 email system configurations, comprised of diverse software solutions and versions, operating on separate platforms, and managed by support organizations corresponding to each department and agency.

Of note:

- There are a number of compatibility issues between the existing email systems. Preliminary estimates show that 81% of Partner departments and agencies use Microsoft Exchange, 13% use Novell GroupWise, and 6% use IBM Lotus Notes for their email system, Partners are using different versions, and have adopted a variety of rules and practices around the use of email. This results in interoperability issues, and higher costs.
- The operation of multiple email systems across the government means that departments and agencies have traditionally negotiated and maintained separate licenses, and have had their own technical support teams in place. This duplication is costly and unnecessary[8].

4.1.2 Financial Pressures

In 2010, the GC undertook a comprehensive review of government administrative functions and overhead costs in order to identify opportunities for additional savings and improve service delivery.[9] Government organizations were asked to find cost savings and reduce expenditures in response to GC economic priorities.

IT spending in the GC is estimated to be around $5 billion[10] annually, and can yield significant opportunities for savings. However, in the current federated model, individual departments and agencies operate their own IT organizations, and acquire their own IT goods and services. Furthermore, to meet GC's expectation of high-standard safe and reliable services, the cost of information technology is continually increasing.

Email consolidation for SSC and its Partners provides the opportunity to reduce overall costs by eliminating duplication and streamlining operations. Additionally, in the specific context of email, the following are the key drivers for streamlining costs:

---

[8] Ibid.

[9] Budget 2010, Canada's Economic Action Plan, March 4, 2010

[10] Data Centre Feasibility Study, PricewaterhouseCoopers, April 25, 2011) (http://www.tpsgc-pwgsc.gc.ca/services/efcd-dcfs/index-eng.html)

(i) Individual departmental implementations have resulted in overlaps and duplications of management and support functions for administering the email systems. Currently, over 400 people are assigned to managing the current 63 emails systems used by SSC's Partners, involving approximately 1,700 email servers, all requiring power, maintenance, licensing, etc.;

(ii) Although users of emails are dispersed across Canada, foreign missions and other locations, each department has architected its email services differently, which has led to inefficient utilization and duplication of networks many of which are non-interoperable and therefore more expensive, and

(iii) The 1700 email servers are distributed across the country, and internationally as well, in data centres of varying sizes and degrees of efficiency. This adds to cost and complexity in management of email services.

4.1.3 Security Pressures

Canadian citizens and private sector organizations have become increasingly reliant on online services to conduct their affairs. This in turn requires the GC to interact with Canadians through online channels. Therefore, the use of email has become a predominant method for interacting with Canadians and businesses.

Email is a known major threat vector[11] used in compromising computer networks, and a consolidated Email Solution requires a heightened security posture against sophisticated attacks. This includes potential attacks from Advanced Persistent Threat (APT) actors as described by Public Safety Canada's Mitigation Guidelines for Advanced Persistent Threats[12].

As an additional complication, email security has traditionally been addressed on an individual departmental or agency basis. Each department and agency assessed its email risks individually, and determined how to implement security measures and controls appropriate to their business needs. Departmental security officers, in cooperation with various IT experts, determined how to implement the security measures and controls, in accordance to the Policy on Government Security[13].

However, the Policy on Government Security does not identify the manner in which email security should be implemented. This resulted in departments and agencies utilizing their own departmentally specified technical standards to meet their individual requirements, at varying degrees of protection. The use of different standards does not protect departments and agencies equally against email threats.

---

[11] A path or a tool that a hacker uses to gain access to a computer or network server in order to deliver a malicious outcome.

[12] http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

[13] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

Finally, approximately 15,000 federal civil servants have access to an Email Solution that is certified to carry Classified information, up to and including Secret (including Protected C), and/or Protected information, up to and including Protected B. There is a need for such a solution to continue to support existing users and allow for some growth over time. Increasing security requirements for some public servants should not reduce the ability for SSC to realize cost savings, on delivering a more cost effective solution, for most public servants. SSC hopes to engage the industry on these questions to achieve the most optimum answer with respect to user segmentation, information and overall system security, and delivery options.

4.1.4 Privacy Pressures

Canadians are extremely concerned about their privacy, particularly in the context of electronic service delivery. The GC is committed to protecting the privacy of Canadians' personal information used in the provision of programs and services to the public, in every delivery channel, including in-person, mail, telephone, and on-line.

The GC department and agency operations are driven by policies derived from the Privacy Act[14]. The Privacy Act entrenches in law, the right of Canadians to control the collection use and disclosure of information about themselves.

4.1.5 Consistent Service Delivery

There is no single email standard within the GC. Canadians and businesses are often perplexed by the complex and confusing government email structure, with different departmental naming conventions.

SSC plans to implement a new Email Solution that:

(i) Is simple, effective and useful for communications with citizens and businesses, and

(ii) Utilizes a single standard email name convention for all GC employees, e.g. jane.doe@canada.gc.ca[15].

Internally, the ETI will improve operational challenges, such as:

(i) Facilitate interoperability by improving email and calendar functions among SSC and its Partners;

(ii) Increase self-service capabilities to allow users of the email system to better manage their mailboxes, retrieve archived emails, etc., and

(iii) Standardize service levels to ensure a consistent delivery of email services to SSC and its Partners.

[14] http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html

[15] The naming convention used here is just an example, and has not been finalized yet by Canada.

4.1.6 Data Sovereignty

It is incumbent for SSC to secure and protect all information and data repositories used by its Partner departments and agencies. The protection of this information from a privacy and security perspective is core to the integrity of government programs, which underpins confidence in the GC.

Furthermore, privacy and security to ensure the protection of personal and confidential information are imperative requirements for the ETI. Canadians expect the GC to take all appropriate measures to protect confidential and personal information.

Most importantly, the information managed by the prospective Email Solution provider, including all emails, email attachments, and email user information, is the exclusive intellectual property of the GC and shall be deemed to remain under the ownership and control of the GC for the purposes of the Access to Information Act and all other legislation requirements.

The email services and infrastructure of the ETI will be established on Canadian soil. Stringent contractual and technical measures will be put in place to ensure that government information is secured at all times, at rest and in motion, and is only accessed by Canadians authorized to access the email infrastructure for those purposes approved by the ETI. Therefore, any potential future contractual arrangement between Canada and a prospective Email Solution provider would require recognition of:

(i) Canada's right to order the destruction or deletion of data;

(ii) Solution provider compliance with the GC privacy and security policy instruments and practices, and recognition of the GC notification regarding privacy and security breaches, and

(iii) Proof of privacy and security training and awareness of Email Solution provider employees that will have access to relevant components of the Email Solution.

4.2 Business Objective and Benefits

The SSC Business Objective, as outlined in the 2012-2013 Report on Plans and Priorities[16], is:

> *"Mandated services are delivered in a consolidated and standardized manner to support the delivery of Government of Canada programs and services for Canadians."*[17]

The ETI will consolidate and modernize SSC mandated email services for SSC and its Partners to reduce costs, increase security, and enhance program delivery to Canadian citizens and businesses. SSC will offer the new service to other GC organizations on an optional basis.

[16] http://www.tbs-sct.gc.ca/rpp/2012-2013/index-eng.asp?acr=2024

[17] SSC Report on Plans and Priorities, February 2012

The ETI will provide the following benefits:

(i) Reduction in costs to deliver email services;

(ii) Continuous improvement to the security posture of email services so that programs and services can continue to be delivered securely and reliably to Canadians;

(iii) Improved interoperability among SSC Partners;

(iv) Consistent email naming standards;

(v) Common service levels for all users, and

(vi) Secure and reliable Email Solution that can process emails – A Secret system (which includes Classified information up to Secret and Protected information, up to Protected C) and/or a Protected system, up to and including Protected B.

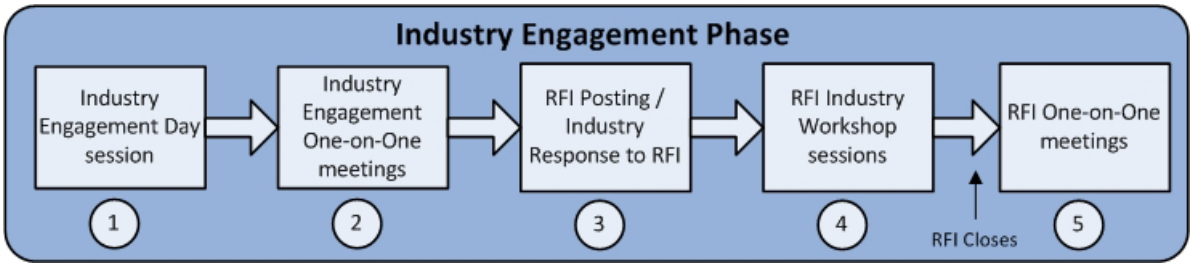
5. PROPOSED PROCUREMENT APPROACH

Depending on the feedback from the Industry Engagement Phase, the procurement strategy may include multiple parallel or sequential procurement activities. For complex requirements, such as those for a transformational ETI solution, the Collaborative Procurement Solution (CPS) is the proposed procurement approach. A description of each phase of CPS is described in the following subsections.

Figure 1: Collaborative Procurement Solution (CPS)

5.1 Industry Engagement Phase

The first phase of the CPS is the "Industry Engagement Phase". In this phase, Canada will set out its expectations for organizations interested in delivering an Email Solution for the GC. The Industry Engagement Phase is designed to solicit feedback from industry on the requirements and the procurement approach. It is composed of 5 main sub-components:



1. Industry Day Session (completed);
2. Industry Engagement One-on-One meetings (completed);
3. This RFI and its response;
4. RFI Industry Workshop: Canada will host a full-day session to familiarize the Respondents with the current state of SSC's email systems, as well as the scope, requirements and technical challenges for the new Email Solution, so that Respondents can provide more detail in their responses to the RFI that will allow Canada to make more educated decisions in its email transformation strategy and requirements going forward. The session is tentatively scheduled to take place on July 5, 2012 in the National Capital Region, with videoconferencing to regional locations. A panel of several Government of

Canada representatives will present information and answer questions from industry. The registration form and logistic information for the session is provided in Annex J. Please fill out the form and submit it via email to the attention of the PWGSC Contracting Authority, identified in section 2.8, by no later than 4:00 p.m. EDT on June 27th, 2012. Canada does not intend to place a limit on the number of representatives that can attend per Respondent, but Respondents are requested to fill in the approximate number of people that will be attending from their organization so that Canada can determine the address/room location for the RFI workshop. Canada will determine, and notify all parties that submitted the form in Annex J, the address/room location for these meetings, by no later than 4:00 p.m. EDT on July 3, 2012.

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

5.2 Request for Responses for Evaluation Phase

As part of this phase, Canada will issue a Request for Responses for Evaluation (RFRE). The purpose of the RFRE is to identify a subset of Successful Respondents with the demonstrated and proven necessary skills and experience in email technologies and email services to implement and operate the new consolidated Email Solution. These Successful Respondents will then proceed to the "Review and Refine Requirements Phase" and will subsequently be asked to provide individual proposals in response to these requirements, as part of the Bid Solicitation Phase.

The proposed RFRE evaluation criteria will focus on Respondent's capabilities and experience to deliver email services in a secure and timely manner, taking into consideration parameters for size, scope, and complexity. As well, financial stability and security clearance are important corporate criteria. Respondents must retain these criteria throughout the process. Canada may, at its sole discretion, reject the Respondents from continuing in the process, if they fail to maintain these criteria. At a high level, Part III includes anticipated mandatory requirements, and Annex D includes the proposed evaluation criteria for the RFRE Phase. Canada may consider that any point-rating assigned to the RFRE Phase be carried forward to the final RFP evaluation.

5.3 Review and Refine Requirements Phase

In this phase, the Successful Respondents from the preceding phase (e.g. RFRE) will work jointly with Canada to review and finalize the technical and solicitation requirements, such as, but not limited to:

(i) Business, functional, architectural, security, and technical requirements of the Email Solution, and its interfaces to desktop and business applications;

(ii) Application conversion requirements, such as standard application program interfaces;

(iii) Data conversion requirements, such as active email storage, archived email storage, and directory interfaces;

(iv) Transition planning requirements, to ensure that SSC and its Partners can seamlessly convert to the new Email Solution, without service interruption or loss of data;

(v) Security Assessment and Authorization requirements applicable to the design, implementation and operations of the solution, in accordance with government standards and guidelines;

(vi) Systems and lifecycle management requirements for the ongoing operation of the Email Solution, and

(vii) Resulting terms and conditions, evaluation, pricing structure, etc.

During this phase, the Successful Respondents may be asked to demonstrate how their solution will meet specific requirements. Each Successful Respondent may be required to build a Proof of Concept (PoC) environment for up to 50 test users at their cost that is accessible via the Internet. The data used in the PoC will be unclassified test data. Each PoC environment should also have support staff from the respective Successful Respondents available to resolve any identified issues in a timely manner. The PoC environment has several purposes including but not limited to:

(i) Review, verify and discuss ETI service requirements;

(ii) Validate risks and assumptions;

(iii) Test migrations from Microsoft Exchange;

(iv) Test migrations from IBM Lotus Notes / Domino;

(v) Test migrations from Novell GroupWise, and

(vi) Test application integration with selected key applications.

The results of this phase will be used by Canada to finalize the requirements for the Request for Proposal (RFP) in the Bid Solicitation Phase. They will not be used to evaluate Successful Respondents/Bidders.

5.4 Bid Solicitation Phase

In the Bid Solicitation Phase, Canada will issue the formal RFP to the Successful Respondents who have completed the Review and Refine Requirements Phase.

The RFP will then permit each Successful Respondent to formally respond to the full set of requirements. Canada may consider that any point-rating assigned in the Request for Responses for Evaluation Phase be carried forward as part of the final RFP evaluation. The process for carrying forward of any RFRE scoring will be clearly set out in the RFRE document.

Upon receipt of the proposals, Canada will conduct a comprehensive evaluation of each proposal, and select the proposal which provides the best value to Canada.

5.5 Award Contract and Implementation Phase

Canada estimates the period of implementation/migration for the Email Solution to take 18 to 24 months for SSC and its Partners, and Canada expects the implementation and migration to the new Email Solution to be completed by March, 2015. Canada is considering a 5-year contract plus 3 one-year optional periods. This contract period includes the implementation and migration period. Canada will officially determine the length of the contract and optional extensions in a subsequent phase of the procurement.

5.6 Anticipated CPS Schedule

Phase	Estimated Duration
Industry Engagement	May to July 2012
Request for Responses for Evaluation	August to September 2012
Review and Refine Requirements	October to December 2012
Bid Solicitation	January to March 2013
Contract Award	April to May 2013

6. SCOPE

6.1 Email Transformation Scope

6.1.1 Functional Scope

The high level functional scope is defined below. Specific scope elements and supporting requirements (e.g. alignment to vision and strategy, use of standards, and integration with existing SSC services) will be refined and documented in more detail during the Review and Refine Requirements Phase.

A more detailed summary of the current scope of the ETI has been attached in Annex B: ETI Scope Matrix.

In Scope

(i) Email;
(ii) Instant Messaging;
(iii) Calendar;
(iv) Personal Contacts;
(v) Personal and Shared Email Folders;
(vi) Email Fax Service Integration;
(vii) Historical Email Access (Email Archiving);
(viii) Email Directory;
(ix) Email Anti-Virus / Anti-Spam, and
(x) Mobile Device Management (smartphone, tablet).

Out of Scope

(i) Integrated Inbox (e.g. Voicemail Integration);
(ii) Collaborative Workspaces;
(iii) Wikis, Blogs and Forums, and
(iv) Office Productivity Suites (except for the email client).

6.1.2 Other Scope

Additional scope is defined below. A more detailed summary of the current scope of the ETI has been attached to Annex B: ETI Scope Matrix.

In Scope

(i) Secret system (which includes Classified information up to Secret and/or Protected information up to Protected C) and/or a Protected system, up to and including Protected B);

(ii) All SSC Partner Locations in Canada, as well as all Embassies and Missions internationally;

(iii) Data Migration and Transition;

(iv) Implementation and Training Support;

(v) On-going Email and User Support, and

(vi) Integration Support for GC "Corporate" and "Program" applications (via standard interface toolkits).

Out of Scope

(i) Top Secret Email Systems;

(ii) Email Services for Mobile Physical Platforms (e.g. Department of National Defence (DND) Naval Ships), and

(iii) Desktop Management (excluding email client).

6.1.3 Application Interfaces

The replacement of application integrations with Partner department and agency business and corporate applications is in scope.

The current strategy is that ETI will be responsible to develop an email integration framework, guidance, and toolkit. Partner departments and agencies will be responsible to modify their applications to integrate into the new Email Solution.

6.2 Email Current State Summary

A summary of the current email systems of SSC's Partners, with estimated volumetric information, has been included in Annex C: Current State Summary.

6.3 Anticipated Mandatory Requirements

An overview of some anticipated mandatory requirements that are considered important by Canada for the Bid Solicitation Phase is included in Part III - Anticipated Mandatory Requirements.

7. EMAIL SERVICE DELIVERY OPTIONS

Canada has considered a number of service delivery options for the management and delivery of an Email Solution. Before making any final service delivery decisions, more information is required from industry on two of the options: Managed Services and Outsourcing. These options are defined below.

SSC is eliciting industry feedback on these two options and/or any other service delivery option that industry believes should be considered by SSC as the most viable and cost-effective email service delivery option for the GC. Final service delivery strategy decisions will be made in subsequent phases of the project.

It should also be noted that Canada has made significant investments in hardware, software, training, and application integration in our existing Email Solutions. It is SSC's intent to make these investments available to industry as Government Furnished Equipment (GFE). SSC is interested in understanding if and how industry would recommend leveraging this investment to deliver the most value to Canada. More specifically, what are industry's recommendations on how Canada should assess prospective proposals based on a Total Cost of Ownership which includes all migration, integration and training costs. It is important to note that at this time Canada has not made any decisions with respect to how existing investment in Government Furnished Equipment (hardware and software) will be leveraged. We are seeking industry feedback on possible options.

7.1 Managed Service Option Description

The construction and commissioning of the new Email Solution would be performed by a private sector Email Solutions provider, located in a data centre managed by SSC. Once built, SSC and its Partners would transition to the new solution with the assistance of a private sector Email Solutions provider. The solution would be managed and operated by a private sector Email Solutions provider.

Canada is open to a range of scenarios for this service delivery option in regards to ownership of assets, support of applications and interfaces, and the provisioning of data centre and security infrastructure. Provision of network connectivity to end user devices will be provided by SSC.

7.2 Outsourced Service Option Description

SSC would outsource the email service to a private sector Email Solutions provider. The service provider would own the hardware and software assets as well as be responsible for the provision of all professional services required to provide the email service. Canada would contract for the service provider to plan, build, and operate the proposed Email Solution. The location of the service would be in data centres located in Canada, and managed by the private sector Email Solutions

provider. Provision of network connectivity to end user devices will be provided by SSC.

Please refer to Part IV for specific questions related to these two options.

8. IT SECURITY RISK MANAGEMENT

With today's dynamic threat environment and GC fiscal constraints, IT security can no longer be an afterthought; it needs to be a vital component of any major project. Therefore, security is one of the corner stones in the ETI initiation and planning phases.

A life cycle approach publication, called the Information Technology Security Guidance-33 (ITSG-33), is being developed by Communications Security Establishment Canada (CSEC). It includes processes recommended by CSEC to help government departments and agencies ensure security is considered right from the start in their IT implementations and that their systems and organizations undergo continuous improvement to evolve with environmental threats.

ITSG-33 contains a catalogue of Security Controls structured into three classes of control families: Technical, Operational, and Management. These three classes of Security Controls together represent a holistic collection of standardized security requirements, which cover all aspects of systems and organizations.

A draft of available security controls is available as an attachment to this RFI and must be downloaded by Respondents, as denoted in Attachment #2 to this RFI. Please note that ITSG-33 is not final and is subject to change by CSEC. Canada will contextualize and select required security controls as part of its planning phase in order to form a baseline of security requirements that properly address evaluated threats and vulnerabilities, and reduce security risks for SSC and its Partners.

PART III: ANTICIPATED MANDATORY REQUIREMENTS

9. BUSINESS AND FUNCTIONAL REQUIREMENTS

9.1 Consolidated Email

The Email Solution must consolidate and modernize SSC mandated email services for SSC and its Partners within the contract period specified in Part II – Background of the ETI – Section 5.5. Once the implementation and migration is completed for SSC and its Partners, the Email Solution must be made available for use by other GC organizations with the same services and at the same service levels. The other GC organizations may elect to onboard to this Email Solution at any time that SSC determines that it is feasible to do so. There is no commitment on the number of mailboxes or the timing of activation of the Email Solution for the rest of the GC organizations.

9.2 User Friendly

The Email Solution must be user-friendly and intuitive, requiring no formal training. Training through documentation or online tutorials of less than 60 minutes, would be considered the maximum.

9.3 Accessible

The Email Solution must be available to all SSC partner locations in Canada, as well as in all Embassies and Missions abroad through access over the GC network infrastructure. The Email Solution must be available in both official languages, and provide users with the ability to switch their language preference dynamically without recourse to an administrator. The Email Solution must meet the standards on accessibility, as defined under the TBS Accessibility Standard[18], and accommodate those with special needs, e.g. interoperability with applications to support visually and hearing impaired employees.

9.4 Mobility Support

The Email Solution must provide Mobile Device Management capabilities for platforms such as Research in Motion (RIM) BlackBerry® smartphones, Apple iPhone® smartphones and iPad® and tablets, and Android™/Windows® smartphones and tablets.

9.5 Available and Reliable

The Email Solution has a target of 100% uptime for users, on a 24/7/365 basis.

9.6 Broad Intelligent Search

The Email Solution must support end-user email message and content search.

[18] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12044&section=text

9.7 Local Email Administration Support

The Email Solution must allow for SSC and partner personnel to perform email administrative functions such as adding and removing accounts, and resetting passwords.

9.8 Legislative and Policy Alignment

The Email Solution must adhere to existing Legislation and Treasury Board Secretariat (TBS) instruments (e.g. policies, standards, guidelines). Note: TBS is addressing any policy gaps resulting from the implementation of a “cross government” email service. Refer to Annex G: Legislative TBS and Policy Instruments for an initial list of instruments that possibly impact this project. This list is subject to change.

9.9 Time Sensitive

The end date for the implementation (including migration) is targeted at March 31, 2015 for SSC and its Partners.

9.10 Cost Effective

This initiative must enable the GC to deliver email services at costs that are at par with industry.

10. TECHNOLOGY PLATFORM REQUIREMENTS

10.1 Open Standards Support

The Email Solution must be compliant with industry standards using open, non-proprietary standard interfaces. Examples of interfaces are included in Annex B: ETI Scope Matrix.

10.2 Legacy System Integration Toolkit

The Email Solution must provide an integration toolkit for SSC and its Partners to leverage in order to integrate their applications into the new Email Solution.

10.3 Access Management

The Email Solution must manage user profiles, credentials, authentication, and authorization.

11. IMPLEMENTATION AND MIGRATION REQUIREMENTS

11.1 Email Migration

Existing email content/data must be migrated to the new service, including file attachments.

The Contractor must:

a) Deliver training and data migration solutions that will reduce transition cost, complexity, and risk to Canada;

b) Provide application integration tools and industry standard interfaces, as identified in Annex B – ETI Scope Matrix, to departments and agencies to facilitate the integration of the Email Solution with their existing applications;

c) Provide migration guidance that will minimize the transition effort, the impact on operations, and risk of loss of data and email performance to departments and agencies in the integration of the Email Solution with their existing applications, and

d) Assume the complete training and migration costs, as estimated by the vendor and as validated and agreed to by SSC, associated with transitioning to a new email technology if different from the existing email platforms used by SSC and its Partners.

The Contractor will only be responsible for providing the standard interfaces, and will not be responsible for integrating the legacy applications into the Email Solution.

11.2 Smooth Transition

Existing functionality must be in place during the transition in order to allow users to retain access to email services, at all times, during the transition.

12. INFORMATION TECHNOLOGY SERVICE MANAGEMENT REQUIREMENTS

12.1 Information Technology Service Management Integration

The Contractor must integrate with the Information Technology Service Management (ITSM) processes and tools of SSC and its Partners. Note that the level of integration is expected to vary depending on the email service delivery option selected.

13. SECURITY REQUIREMENTS

13.1 Multiple Levels of Security

The new email service will be certified to accommodate emails: A Secret system (which includes Classified information up to Secret and Protected information, up to Protected C) and/or a Protected system, up to and including Protected B.

13.2 Layered Security

The service must support layered security controls, such as:

- Perimeter security services (e.g. firewall, anti-virus, anti-spam);
- Protection from threats to the data at rest (e.g. access control), and
- Protection for data in motion (e.g. encryption).

13.3 Public Key Infrastructure Support

The Email Solution must support Secure Multipurpose Internet Mail Extensions (S/MIME). The GC is evolving its requirements in the area of public key infrastructure (PKI) support and the Email Solution is expected to support these evolving standards as they are developed.

13.4 Canadian Citizenship for Support Personnel

All engineering and technical support personnel must be Canadian citizens.

13.5 Data Sovereignty

All data infrastructure components for the email system must reside in Canada:

a) All email servers and data repositories must be housed in Canada;

b) The storage of media, for purposes of backup and recovery, or historical archiving, or any other purpose, must be housed within secure approved location(s) in Canada;

c) The Email Solution must contain access controls and monitors on data repositories and other computer systems, such that Canada may, at its discretion, monitor, audit and restrict access to Canada's data. These activities must include a logging, audit trails and reporting mechanism that identifies all individuals that have accessed all email system components for purposes of operation and maintenance;

d) All GC internal emails sent from government users located in Canada or abroad, to other government users located in Canada or abroad, must travel through appropriately secured networks. Any redirections of emails by vendors, not expressly following these two circumstances, will not be accepted. Data in transit must not be saved or stored between their starting and end points, and

e) In the event of unauthorised access to Canada's data (e.g. access that has not been expressly permitted by Canada) within the Email Solution (e.g. to comply with a foreign government's production order), there will be no limit to the Email Solution provider's liability to Canada for such unauthorised access.

13.6 Supply Threats to the Government of Canada

In addition to the threat of cyber attack, there is a growing awareness of the risks posed by potentially vulnerable or shaped technologies that may be entering the GC communications networks and IT infrastructure through the supply chain.

The Contractor must provide the GC with a list of all hardware and software manufacturers and vendors proposed to be used in the IT Infrastructure and Services of the ETI in advance of contracting with them. Canada reserves the right to reject a hardware or software manufacturer and/or vendor for security and/or business stability reasons.

The Contractor must abide by the Technology Supply Chain Guidelines (TSCG), accessible at:

HTML http://www.cse-cst.gc.ca/its-sti/services/tscg-ccat/tscg-ccat01g-eng.html

PDF: http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01g-eng.pdf

http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01l-eng.pdf

French:
HTML: http://www.cse-cst.gc.ca/its-sti/services/tscg-ccat/tscg-ccat01g-fra.html

PDF: http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01g-fra.pdf

http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01l-fra.pdf

Communications Security Establishment Canada (CSEC), as part of Industry Day held on June 12, 2012, presented an unclassified cyber-security and supply threats briefing to companies who were in attendance.

CSEC has offered to provide organizations interested in participating in subsequent phases of the ETI procurement with a more sensitive supply threats briefing. One or more briefings will be carried out as part of the June to July 2012 Industry Engagement phase, as outlined in section 5.6. Organizations will be required to register directly with PWGSC. In terms of attendance for the briefing, there should be at least one company officer present that has decision-making authority in security, technology and/or procurement (e.g. VP/CTO, CSO, etc). All individuals, from each Organization, that plan to attend the supply threats briefings, must sign the Non-Disclosure Agreement (NDA) in Annex H, and send it in with their registration form (as described below and available in Annex I) in order to receive the supply threats briefing. Industry is advised that the subject

NDA is not negotiable and must be signed by an executive company representative that has the authority to agree to the terms and conditions of the NDA. Once signed, the NDA is to be submitted via email to the attention of the PWGSC Contracting Authority, identified in section 2.8, no later than 4:00 p.m. on June 27th, 2012. Subject to PWGSC's and CSEC's acceptance of the NDA, organizations will be scheduled for a sensitive supply threats briefing by PWGSC.

At Canada's discretion, these sensitive briefing(s) may be conducted on a one-on-one basis or in group session(s) where a number of organizations attend the same briefing. Please fill out the form in Annex I and submit the form via email to the attention of the PWGSC Contracting Authority, identified in section 2.8, by no later than 4:00 p.m. EDT on June 27th, 2012, which will help PWGSC determine date(s) for the supply threats briefing(s). Canada will determine the date(s)/time(s) when this/these briefing(s) will take place, and notify all parties that submitted the form in Annex I of the logistics via email.

13.7 Security Clearance

A security clearance is a certification that is granted by the Canadian Industrial Security Directorate (CISD) of PWGSC. Security requirements will be set out in the Request for Responses for Evaluation (RFRE) and the Request for Proposal (RFP).

Canada currently anticipates that Successful Respondents and/or Bidders will require the following:

a) **Secret Clearance** from Canada for any Successful Respondent and/or Bidder who will have access to any Sensitive Information;

b) **Facility Security Clearance (FSC) and Document Safeguarding Capability** (DSC) from the Canadian Industrial Security Directorate (CISD) for the facility at which the Successful Respondent and/or Bidder intends to use and store Sensitive Information, and

c) **Information Technology Security** capability vetted by CISD for the facility at which the Successful Respondent and/or Bidder intends to use and store Sensitive Information, in order for the Successful Respondent and/or Bidder to be able to process, store or transmit Sensitive Information electronically.

Companies should expect that personnel assigned after the industry engagement phase will be required to be security cleared to Secret. Companies can expect that at the RFP stage, all bidders must satisfy all security requirements. Please refer to Annex F – Draft Security Requirements Checklist (SRCL).

Respondents are advised that works and services, to be carried out for the ETI, shall be accompanied by special security measures and be subject to national security constraints. Consequently, Successful Respondents and Bidders must accept the conditions set out in the RFRE and RFP relating to national security and national interest, which requires vetting and security checks for designated

individuals involved in the ETI. Respondents should anticipate that there will be stringent requirements and the absolute need to comply with them, including requirements applying to the processing of Secret information.

SSC currently expects that the ETI contract may require some or all of the following contractual obligations and restrictions:

a) Individuals employed by the Contractor, who are required to work with the ETI drawings/documents or visit some of the government sites, must have a Secret clearance;

b) All Persons performing contractor duties under the ETI must have a security clearance at the appropriate level. Accordingly, the contractor must ensure that appropriate personnel have the required security clearance levels, and the contractor must ensure that security clearances of its personnel are processed in advance to ensure that they are in place when required;

c) Pertaining to the Managed Service sourcing option, the movement of all security cleared personnel will be limited to their required areas of work and they will not be permitted to enter areas designated as restricted;

d) Pertaining to the Managed Service sourcing option, the Contractor personnel will not be allowed access to certain sites without either an authorized escort or the required security clearance;

e) Pertaining to the Managed Service sourcing option, Canada will reserve the right to designate security screening requirements for the contractor personnel who need access to the site during the term of the ETI contract;

f) Pertaining to the Managed Service sourcing option, Contractor personnel who need regular access to a site will require Secret clearance. Personnel not situated on site full-time, who are required by the Contractor to perform activities on an “as-needed basis”, may be required to be accompanied by an authorized escort or to first obtain a security clearance at a designated level, and

g) Security requirements and protocols will exist to ensure that sensitive information and ownership in the control of the Contractor, the Facility, and the ETI are not acquired by any person who does not have appropriate security clearances as a result of any assignment, transfer, or disposition by the Contractor, change in control of the Contractor, exercise of remedies by lenders, or otherwise.

13.8 Canadian Industrial Security Directorate Security Process

Security clearances (issued by CISD) will allow Respondents to work on GC premises and have access to confidential or sensitive information if/as required. GC Security Policy requires that individuals undergo a personnel-screening process if their duties or tasks necessitate access to Classified/Protected information and assets. Respondents must be sponsored by a representative from SSC in order to start the process of obtaining or upgrading a security clearance

Claude Bazinet
Project Coordinator
Shared Services Canada
Email Transformation Initiative
255 Albert Street, Room 1201-19
Ottawa, Ontario K1P 6A9
Canada

Email Address: claude.bazinet@ssc-spc.gc.ca

Telephone: 613-960-9253
Facsimile: 613-941-2783

Early submission of all applications for security clearances is strongly encouraged. Respondents are strongly encouraged to submit applications for security clearances for all Key Individuals and any other persons who may be required during the Review and Refine Requirements Phase to have access to sensitive information and/or access to secured sites. Procurements will not be delayed in order to provide time for suppliers to obtain required security clearances.

13.9 Privacy

The Email Solution must ensure that information is accessible only to those authorized. The Email Solution must comply with the statutory obligations under the Privacy Act[19] and the Access to Information Act[20].

[19] http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html
[20] http://laws-lois.justice.gc.ca/eng/acts/A-1/index.html

PART IV: QUESTIONS

14. QUESTIONS

Industry is requested to provide feedback and comments to the following questions by category for Canada's consideration as it moves forward with the ETI. Please provide any rationale for your responses in order to give Canada basis for further consideration on the way forward.

Please feel free to comment on any aspect of this RFI document as well as provide any general comments or recommendations for this initiative.

The following questions have been grouped under ten general themes. Details relating to each of these themes may be presented and discussed during the RFI Workshop. Respondents are asked to answer these questions in the context of the material presented.

1. Email Service Delivery Options;
2. Business, Policy, Information Management, and Functional Requirements;
3. Security Requirements;
4. Privacy Requirements;
5. Technology Platform Considerations;
6. Implementation and Migration;
7. Service Management and Operations;
8. Small and Medium Enterprise Socio-Economic Considerations;
9. Greening Considerations, and
10. Proposed Procurement Approach.

14.1 Email Service Delivery Options

Two email service delivery options have been identified under Part II – Background of the ETI - Section 7 regarding SSC's sourcing of email products and services. Canada is looking for industry feedback on the viability of any and all perspectives with regards to these service delivery options.

At this time, Canada has an understanding of the requirements associated with the email technologies – product functions, server and storage infrastructure, and thick/thin client components. However, any additional information in regards to email technologies, focussed on innovative thinking in these areas, would help complement Canada's knowledge in this domain.

Of special interest, Canada is seeking to obtain a greater understanding of services and opportunities that can be provided by private sector organizations related to the design, conversion, transition and on-going system management requirements of an email service.

Q01: Can you provide any case studies and/or business rationale that could assist SSC in its decision process in determining the optimal service delivery model for delivering the GC Email Solution?

Q02:

(i) Do you have a service delivery model preference for providing an Email Solution within the project timeframe for the ETI for Protected email, up to and including Protected B, for SSC and its Partners? (Please reference the service delivery options described in Part II – Background of the ETI – Section 7):

a) A Managed Service;

b) An Outsourced Service; or

c) Any other option the GC should consider.

(ii) Would this preference change for Classified email up to and including Secret (including Protected C)? If so how? Please provide rationale in your response, including, at a minimum, the pros and cons you would consider for the options the GC should consider.

(iii) Would this recommendation change if SSC were to separate the provision of the Email Solution for a Secret system (which includes Classified information up to Secret and Protected information, up to Protected C) and/or a Protected system, up to and including Protected B?

Q03: Do you have the capability to provide an Email Solution within the project timeframe for the ETI for Protected email, up to and including Protected B, for SSC and its Partners? Do you have the capability to provide an Email Solution within the project timeframe for the ETI for Classified email, up to and including Secret (including Protected C)? Please provide rationale in your response.

Q04: If Canada was to restrict the provisioning of the Email Solution to a Canadian company, or a Canadian foreign subsidiary (e.g. a Canadian company, operating in Canada, which is a subsidiary of a foreign parent company), and further restrict the use of subcontractors to Canadian companies and Canadian foreign subsidiaries, how would this affect your service offering in still meeting ETI's service requirements?

Q05: What would you consider to be the largest risks for this kind of an email consolidation project and what steps would you recommend to Canada to mitigate those risks? Please list your risks from the perspectives of Planning, Migration, Implementation, and Support.

14.2 Business, Policy, Information Management, and Functional Requirements

SSC is seeking industry's feedback on the Bidder's ability to meet anticipated mandatory requirements in Part III.

Q06: Are there any requirements in Part III - Anticipated Mandatory Requirements, or in Attachment #2 – ITSG-33: Information Technology Security Guidance - Security Control Catalogue that your organization would deem as a concern to the overall implementation of the Email Solution? Please comment on any of the complexity, cost and delivery risks to the ETI objectives, business requirements, assumptions and the conceptual model.

14.3 Security Requirements

SSC has requirements for a Secret system (which includes Classified information up to Secret and Protected information, up to Protected C) and/or a Protected system, up to and including Protected B. A decision on whether a single service provider and/or solution will be able to meet both of these requirements has not been determined at this time. In order to assist with this important decision-making, SSC wants to understand more of the capabilities and experience of industry to deliver and support a Secret email system. As such, this section contains detailed questions related to security. Responses to this section will serve as valuable input to the service delivery sourcing strategy.

Q07: Describe the risk management methodology you currently employ. Include the following in your response:

a) Organization's security governance structure;

b) Asset categorization process;

c) Threat and risk assessment process, and

d) Continuous monitoring and improvement process.

Q08: Describe the information system security engineering process you currently employ (e.g. Secure System Delivery Life Cycle). Include the following in your response:

a) Project governance structure;

b) Key security activities and deliverables of the process;

c) How security would be incorporated into system development, implementation, and design decision coordination with the GC throughout the Email Solution contract, and

d) Secure coding methodology (if applicable).

Q09: Describe your proposed conceptual (high level) security architecture for the consolidated GC Email Solution. Where possible include the following in your response:

a) How this conceptual architecture addresses the threats from Part II – Background of the ETI - Section 4.1.3;

b) Identity and account management approach;

c) Access control approach, including user and email authentication, authorization, remote clients and email classification handling;

d) Use of encryption, including any use of Public Key Infrastructure (PKI) technologies;

e) Email integrity approach, including any use of digital signature;

f) Boundary protection approach;

g) Email and document classification marking software capabilities;

h) Any other security labelling and management rights approach, including secure handling of information at rest and in-transit and integration to access control;

i) Web security approach;

j) Denial of service protection approach;

k) Domain Name System (DNS) protection approach;

l) Malicious code protection approach; (e.g. email attachments), and

n) How you propose to protect the GC against the issue of users opening emails with embedded threat agents, e.g. Virus, worm, spam protection.

Q10: Describe your proposed operational processes for the consolidated GC Email Solution. Include the following in your response:

a) Audit approach, including logging, monitoring, Intrusion Prevention System (IPS), Intrusion Detection System (IDS) incident management, and response approach;

b) Secure configuration, and change management approach;

c) Secure migration approaches for migration of current and archived email content from legacy systems (e.g., malware detection and removal);

d) Media access, storage, transport and sanitization protection approach;

e) Backup, redundancy, and contingency safeguards;

f) Physical, and environmental protection approach;

g) Personnel security approach;

h) Supply chain protection approach, and

i) For all previous items, any standards used.

Q11: Describe your ability to conform to third party (GC) security monitoring and audit requirements. Include the following in your response:

a) Sharing of security audit related information, including:

(i) Copies of all unmodified message transactions, and

(ii) Sharing and receiving of threat information;

b) External auditor's assessment of your IT infrastructure and operational processes. (e.g. operational procedures document review, key operational personnel interviews, vulnerability assessment testing);

c) Integration of GFE and software for the purposes of network data aggregation and monitoring;

d) Ability to conform to GC requirements regarding handling security incidents in collaboration with the GC-designated Information Protection Centre, and

e) Ability to apply GC-provided inputs to perimeter defence safeguards (e.g., malware and intrusion signatures, IP and URL black and white lists).

Q12: At a high level, briefly describe the different protection strategies for Protected information versus Secret information in an Email Solution.

Q13: SSC currently supports multiple segregated networks for Protected B and Secret processing, including email capability. It is estimated that there are approximately 15,000 users utilizing Secret email and 377,000 users utilizing email systems that can handle information up to and including Protected B.

a) Using the existing GC infrastructure, can you provide access to the Protected B and Secret emails from a common user environment (e.g. single desktop)? If not, what solution do you propose (e.g. thin clients)?

If yes, then:

b) Please identify advantages and disadvantages of implementing a consolidated Email Solution supporting both Protected B and Secret email, versus two separate Email Solutions, from a cost, procurement complexity, requirement complexity, implementation complexity and security perspective. Are you capable of delivering a consolidated Email Solution?

c) If SSC was to consider acquiring two separate Email Solutions, a Secret and a Protected B Email Solution, would you recommend Canada use a single Contractor approach or two Contractors providing each solution separately? Please provide pros and cons, and comment on this from procurement complexity, requirement complexity, implementation complexity and security perspective.

Q14: Canada wishes to ensure that the Email Solution contains stringent privacy and security controls on all repositories of Canada's data (as described in Part III - Anticipated Mandatory Requirements - Section 13.5). These controls should also provide detailed logging, monitoring, auditing, and reporting of all individuals who have accessed or attempted to access Canada's email data.

a) What control measures (solutions, functionality, tools, processes, etc.) can you propose which would meet these requirements?

b) How would you address sites outside of Canada (e.g. Missions)? Are there any technical limitations, service delivery and cost implications that should be considered by Canada?

c) Do you have other thoughts or views on how Canada can safeguard its data sovereignty, and simultaneously meet the objectives as stated in Part II – Background of the ETI - Section 4.1.5?

Q15: Have you successfully deployed a:

a) Secret Email Solution (e.g. more than 500 mailboxes)? and

b) Protected B Email Solution

that have been certified to standards that could meet GC standards? Are you able to provide the certification evidence and/or a reference? Please elaborate.

14.4 Privacy Requirements

This section solicits information on the privacy aspects of the Email Solution.

Q16: Describe the process and procedures your organization would employ to protect personal information. Please indicate, at a high level, the roles and responsibilities, tools, resources, policies, procedures and best practices you would use to protect the personal information.

Q17: Email services relay, collect and retain vast amounts of personal information. An undertaking to consolidate the Email Solutions across Partner organizations will present unique and significant privacy risks. Describe mitigation strategies your organization would propose to address current trends in privacy threats in an Email Solution.

14.5 Technology Platform Considerations

This section solicits information on the technology platform considerations of the Email Solution.

Q18: For which email components (including infrastructure) and/or processes do you believe the GC should retain service delivery accountability?

Q19: Would your Email Solution be able to leverage Canada's existing investment in email hardware, software, and/or tools (e.g. GFE), where applicable, in order to provide the best value to Canada? More specifically, what are industry's recommendations on how Canada should assess prospective proposals based on a Total Cost of Ownership which includes all migration, integration and training costs?

Q20: Today, departments and agencies have multiple directories, including email-specific directories that are not integrated. How do you envision meeting the requirement for the consolidated Email Solution to manage user profiles, authentication, and

authorization? What do you suggest Canada do to prepare to integrate with your email service directory solution as it pertains to account and directory management?

Q21: The creation of an Enterprise Identity, Credential and Access Management (ICAM) solution is not in the scope of the ETI project. However, if you have a strong understanding of the ICAM market and existing ICAM solutions in place in the GC today, please suggest strategies that could be considered to meet the basic ICAM needs of ETI in a cost effective and timely manner.

Q22: Today, each Partner department and agency manages their own desktop environment. Most Partners typically have a secure remote access solution. Users are often provided with mobile access to a fully functional email application via different methods, such as thin client and/or VPN. Are there technical considerations or business requirements that Canada should identify in order to deliver this mobile access capability to users?

Q23: The GC would like to evolve to a Single Sign-On model in the future. Do you have any suggestions on how the ETI can further this objective?

Q24: How can the new Email Solution utilize social media technology in terms of citizen engagement and enablement?

14.6 Implementation and Migration

The consolidation of email systems used into a consolidated GC-wide email service is a significant component of this project. The three main components of migration under consideration at this time are: data migration, application migration (migration of program and other applications that are currently integrated with various departmental email systems), and user migration.

Q25: Please describe your recommended considerations for implementation and migration based on lessons learned. Provide examples of lessons learned that Canada should consider with respect to application and data migration for a requirement of this size, scope, and complexity.

Q26: With respect to transition services, how do you transition your customers from their current state to your fully-deployed Email Solution? What do you see as the main challenges with migrating a minimum of 377,000 users from their existing email to the new Email Solution? Would you suggest Canada do any preparation prior to the migration?

Q27: What best-practices would you recommend for migrating a large number of users from one email service implementation to another such that:

a) The user's experience during the migration is as seamless as possible;
b) The business impact on the GC is minimized, and
c) The compatibility issues with the implementation of the Email Solution with existing legacy applications are minimized?

Q28: What information would you require at the Review and Refine Requirements and the Bid Solicitation phases, in order to accurately estimate the costs for the migration effort?

Q29: What are your views on the Contractor assuming the training and migration costs associated with transitioning SSC and its Partners to a new email technology from their existing platforms?

Q30: What are your views on the application integration and industry standard interface migration tools currently available in the market?

Q31: The current application integration strategy, is that SSC's Partners will be accountable for integrating their applications into standard interfaces with an integration toolkit provided by the Email Solution Provider.

(i) To avoid the risks associated with dependencies with SSC's Partners, what are the pros and cons of adjusting this strategy to make the Email Solution Provider responsible for application integration?

(ii) Do you have alternate strategies that the GC should consider to reduce the cost and timeline risks of application integration with the Email Solution?

Q32: SSC is interested in lessons learned from similar email service implementations. Please provide lessons learned on email projects of similar size, scope and complexity that your organization has implemented in the past (where your organization consolidated different vendors' email software products, e.g. Microsoft Exchange, IBM Lotus, Novell GroupWise).

14.7 Service Management and Operations

For a requirement of this nature, the GC typically specifies service levels. The GC will likely include a requirement so that it can satisfy itself that it is contracting with a service provider that regularly meets or exceeds the service level commitments it has made to its customers.

Q33: Do you have different service tiers? If so, please describe them. What are the key attributes that drive costs for each tier?

Q34: How would you recommend the GC segment the user population in order to minimize costs for implementation, migration, and on-going support?

Q35: Can you provide service delivery and service level metrics for a similar large engagement where you acted as the email service provider? Please provide examples of specific service delivery performance statistics that you think are relevant to measuring a service provider's ability to provide high-quality services.

Q36: The Contractor will be expected to integrate with the ITSM processes and tools of SSC and its Partners. Do you have any suggestions on how the service model would be organized?

Q37: Depending on the final service delivery model selected, there could be a number of different Email Solution providers delivering the overall Email Solution (e.g. email application service provider, storage provider, Level-1 service desk, etc.). Do you have recommendations on how the GC should define and manage the overall Service Model

to ensure multi-supplier service accountabilities are clear and well understood (e.g. for triage, problem resolution, performance reporting) and can be monitored by the GC?

14.8 Greening Considerations

The Office of Greening Government Operations (OGGO) encompasses a wide range of activities: It establishes government-wide priorities, accountabilities, targets, timelines and reporting requirements to assist the GC in its commitment to become a model of environmental excellence in its own operations.

Q38: Do you have a corporate environmental policy? If so, would you provide a copy?

Q39: Respondents are requested to provide input regarding the applicability and standards already in place or envisioned for the managed email services that would align with and support Canada's Sustainable Development (Green Procurement) strategy.

14.9 Small to Medium Enterprise Socio-Economic Considerations

The Government is interested in supporting the development of innovative Canadian Small and Medium Enterprises (SMEs).

Q40: What are your views on leveraging the ETI to support the development of innovative Canadian SMEs? How can SSC assist in this regard? What can be done to leverage PWGSC's Canadian Innovation Commercialization Program (CICP)[21]?

Q41: If you are a large IT service provider, does your business model involve subcontracting portions of the work to smaller or regional businesses? If so, what portions of the work would you suggest subcontracting to third parties in this context? If not, is there a reason you choose not to subcontract?

Q42: If you are a smaller or a regional or specialized business, do you often work with larger organizations as a subcontractor?

Q43: What other services do you think can be provided by private sector organizations outside the scope of the ETI, but relating to design, conversion, transition, facilitation and on-going system management requirements of the email service?

14.10 Proposed Procurement Approach

14.10.1 The CPS process is described in Part II – Background of the ETI - Section 5. This is the proposed procurement approach for the ETI.

Q44: Are you familiar with this innovative procurement process? If so, please provide opinions and comments on this procurement approach.

---

21 https://buyandsell.gc.ca/initiatives-and-programs/canadian-innovation-commercialization-program

Q45: The Jenkins report[22] recommended that RFPs should, where appropriate, define the needs to be met or the problems to be solved, rather than being overly prescriptive of the solution. Canada intends to implement the Jenkins approach. Would you agree with this recommendation? Do you have suggestions as to how this could be implemented with respect to the CPS approach?

14.10.2 Please refer to Annex D - Evaluation Procedures and Identification of Successful Respondents.

Q46: Please provide any feedback you have on the mandatory and rated evaluation criteria contained in Annex D, including which criteria you find most and least relevant, and please provide an explanation.

(i) Do you have suggestions for other criteria?

(ii) Do you think these can best be measured through mandatory and/or rated requirements (as described in Annex D)?

14.10.3 High quality managed email services depend heavily on the skills of the core team individuals involved in the design, architecture, construct, and implementation of the Email Solution.

Q.47: SSC will be expecting that the Successful Respondents provide the following Core Team of resources for the implementation of the Email Solution:

a) Senior Project Executive;

b) Senior Project Manager;

c) Business Analyst;

d) Technical Email Architect;

e) Senior IT Security Design Specialist, and

f) Implementation Manager.

Do you believe that the resource competencies defined for the Core Team in Annex A – Glossary adequately covers the resource skills set necessary for the ETI?

14.10.4 Canada is interested in soliciting feedback on ETI service costing and pricing with specific references to cost and price determinants and how they would influence SSC's final price model.

Q48: Please provide comments on which pricing models have been successful in your email service contracts with large corporate customers. Do you offer more than one pricing model when supplying managed or outsourced email services to your customer

[22] http://rd-review.ca/eic/site/033.nsf/vwapj/R-D_InnovationCanada_Final-eng.pdf/$FILE/R-D_InnovationCanada_Final-eng.pdf

base? Can you please describe the basis on which you charge (e.g. mailbox, user, etc.)?

Q49: Based on the anticipated mandatory business requirements (as described in Part III - Anticipated Mandatory Requirements) and the information in this RFI, please provide pricing information for your email service. The information provided here will be used as an input for project planning purposes.

Q50: How would your price structure be affected if SSC was to consider splitting the email requirements into a Secret system (which includes Classified information up to Secret and Protected information, up to Protected C) and a Protected system, up to and including Protected B?

Q51: Canada is currently considering a 5-year contract with 3 one-year optional periods. This includes the implementation and migration period. In your view, what length of contract (including fixed years and option years) would provide best service pricing to Canada and make it beneficial to both parties? Please provide feedback (e.g. magnitude of price discounts for longer term). If there is a range, please provide rationale for the minimum and maximum contract term.

Q52: Based on your experience with an email project of this magnitude, can you provide an approximate percentage breakdown of the major cost elements over a 5 year total cost of ownership period (e.g. implementation, software licenses, servers, storage, operations, etc.)?

Q53: What are your standard terms and conditions for outsourced, managed and other types of email service products and offerings that you provide?

Q54: What is your standard limitation of liability for a project of this scope and magnitude?

Q55: The GC has an objective to minimize the risk of a security or privacy breach due to vendor negligence and due to a vendor being compelled by a foreign nation to hand over email information owned by the Government of Canada. What are your thoughts on unlimited liability to achieve this objective?

ANNEXES

ANNEX A: GLOSSARY OF TERMS

1. Acronyms

Acronym	Description
API	Application Programming Interface
ATIP	Access to Information and Privacy
CAL	Client Access License
CalDAV	Calendaring Extensions to Distributed Authoring and Versioning
COTS	Commercial Off-the-Shelf
CPS	Collaborative Procurement Solutions
DCS	Data Centre Services
EA	Enterprise Architecture
EDRMS	Electronic Document Records Management System
ETI	Email Transformation Initiative
GC	Government of Canada
HTTPS	Hypertext Transfer Protocol Secure
IM	Information Management
IMAP4	Internet Message Access Protocol (version 4)
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
LDAP	Lightweight Directory Access Protocol
MAN	Municipal Area Network
MIME	Multipurpose Internet Mail Extensions
MS	Microsoft
OGD	Other Government Department
OL	Official Languages
PKI	Public Key Infrastructure
POP3	Post Office Protocol (version 3)
PWGSC	Public Works and Government Services Canada
RDIMS	Records Documents and Information Management System
RFI	Request for Information
RFP	Request for Proposal
RFRE	Request for Responses for Evaluation
RPP	Reports on Plans and Priorities
RSS	Rich Site Summary

RTM	Requirements Traceability Matrix
S/MIME	Secure Multipurpose Internet Mail Extensions
SLA	Service Level Agreement
SME	Small and Medium Enterprise
SMS	Shared Municipal Area Network
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SoR	Statement of Requirements
SSC	Shared Services Canada
TBIPS	Task-Based Informatics Professional Services
TSPS	Task and Solutions Professional Services
TSSD	Transformation Service Strategy and Design
VMO	Vendor Management Office
WAN	Wide Area Network
WBS	Work Breakdown Structure
WSDL	Web Services Description Language
XMPP	Extensible Messaging and Presence Protocol

2. Definitions

Term	Definition
Bidder	Person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both. It does not include the parent, subsidiaries or other affiliates of the bidder, or its subcontractors.
Certification	Please refer to definition for Security Assessment (below).
Classified information	This relates to the national interest. It concerns the defence and maintenance of the social, political, and economic stability of Canada. There are three levels of Classified information: Top Secret: A very limited amount of compromised information could cause exceptionally grave injury to the national interest. Secret: Compromise could cause serious injury to the national interest. Confidential: Compromise could cause limited injury to the national interest.
Collaborative Procurement Solutions	Collaborative procurement approach consisting of the following Phases: (i) Industry Engagement Phase – to seek industry feedback on the project and procurement approach; (ii) RFRE Phase – to identify Successful Respondents; (iii) Review and Refine Requirements Phase – Successful Respondents collaborate with SSC to review and refine the business and technical email requirements; (iv) Bid Solicitation Phase – Successful Respondents are invited to submit technical and price proposals; (v) Contract Award Phase – issue contract to winning Bidder(s), and (vi) Implementation Phase – design architecture, build and implementation of the Email Solution and service delivery.
Complex Email Transformation Project	Implementation of an Email Solution in a multi-stakeholder enterprise organization, comprised of a minimum of 10,000 users, where an Email Solution has been integrated with multiple business applications.
Consolidated Solution	A term meaning that the chosen ETI solution will satisfy all of the email requirements of SSC and its Partners.

Core Team	Senior Project Executive: The proposed resource should have at least 5 years of experience, within the last 15 years, as the Lead member of an integrated project team, in the delivery of email transformation projects for an enterprise, in a Complex Email Transformation Project. Senior Project Manager: The proposed resource should have at least 5 years of experience, within the last 15 years, as a Senior Project Manager working within a Project Management Office, in the delivery of email transformation projects for an enterprise, in a Complex Email Transformation Project. Senior IT Security Design Specialist[23]: The proposed resource should have at least 10 years of experience, within the last 15 years, and have worked, at a minimum, on 2 email business transformation projects, conducting the following activities tailored to the Bidder's technical proposal (e.g., Protected B Email Solution, Secret Email Solution, combination of Email Solutions): (i) Produced security requirements and traceability matrices for Email Solutions in a Complex Email Transformation Project; (ii) Preparation of technical reports such as requirement analysis, options analysis, technical architecture documents including security, etc.; (iii) Design complex, secure Email Solutions, including the designing the security related to email and supporting applications, web and database servers, directories, and networking components, and (iv) Produced operational security requirements used during the operational and disposal phases of an Email Solution. Implementation Manager: The proposed resource should have at least 5 years of experience, within the last 15 years, as an Implementation Manager, in the delivery of email transformation projects for an enterprise, in a Complex Email Transformation Project.

[23] More details can be found about this resource category on the CPSA web site: http://www.tpsgc-pwgsc.gc.ca/app-acq/amac-cpsa/ws3-eng.html

	Technical Email Architect: The proposed resource should have at least 5 years of experience, within the last 15 years, as a Technical Email Architect, in the delivery of email transformation projects for an enterprise, in a Complex Email Transformation Project. Business Analyst: The proposed resource should have at least 3 years of experience, within the last 10 years, as a Business Analyst, in the delivery of IT projects for an enterprise, in a Complex Email Transformation Project.
Corporate Customer	An entity with a minimum of 5,000 users, from either the private sector or from a public sector organization, of an Email Solution designed, architected, built and implemented by the Respondent.
Email Solution	An Email Solution can be composed of one or more IT systems/data centres, one or more communication networks, and servers, server applications, client applications, etc. either implemented, operated and managed in a GC environment, or as a service offered by a commercial service provider.
In-House Service	An Email Solution designed and deployed by SSC government in-house technical resources.
IMAP Email Protocol	Please refer to RFC 3501 - http://tools.ietf.org/html/rfc3501.
Interested Party	An organization who wishes to participate in the Industry Engagement Phase activities associated with the ETI
Joint Venture	Association of two or more parties who combine their money, property, knowledge, expertise or other resources in a single joint business enterprise, sometimes referred as a consortium, to bid together on a requirement.
Managed Service	The provision of a service to the Corporate Customer where the Email Solution provider has the responsibility for delivery of the service and where the service must meet the Client's pre-defined service levels.
Outsourced Service	The definition, construction, migration, and operation of the new Email Solution would be exclusively managed by a private sector Email Solution provider. The infrastructure would be owned and operated by the private sector Email Solution provider. The location of the service would be in data centres managed by the Email Solution provider.
Partners	Departments and agencies for which SSC provides information technology (IT) services. Please refer to Annex E for the complete list.

Platform	General purpose information systems components used to process and store electronic data, such as desktop computers, servers, network devices, and mobile devices. Platforms usually contain software, such as operating systems, device drivers, and applications.
Protected Information	This refers to specific provisions of the Access to Information Act and the Privacy Act and applies to sensitive personal, private, and business information. Protected A (low-sensitive): Applies to information that, if compromised, could reasonably be expected to cause injury outside the national interest, for example, disclosure of exact salary figures. Protected B (particularly sensitive): applies to information that, if compromised, could reasonably be expected to cause serious injury outside the national interest, for example, loss of reputation or competitive advantage. Protected C (extremely sensitive): applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the national interest, for example, loss of life.
Request for Responses for Evaluation (RFRE).	Procurement instrument used to identify Successful Respondents for the Review and Refine Requirements and Bid Solicitation Phases of the CPS procurement approach.
Respondent	An organization that provides a written response (via electronic documentation) to the RFI and/or RFRE.
Security Assessment	The on-going process of evaluating the performance of IT security controls throughout the lifecycle of information systems to establish the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the departmental business needs for security. Security assessment supports authorization by providing the grounds for confidence in information system security.
Security Authorization	The on-going process of obtaining and maintaining official management decision by a senior organizational official to authorize operation of an information system and to explicitly accept the risk of relying on the information system to support a set of business activities based on the implementation of an agreed-upon set of security controls, and the results of continuous security assessment.

Security posture	A characteristic of an information system that represents the ability of implemented security controls to satisfy the business needs for security and counter a selected threat environment. Note: A security posture that satisfies the business needs for security and counters a selected threat environment is deemed *adequate*. The security posture may vary over time, as threats and business needs for security evolve, and vulnerabilities are discovered. To maintain an adequate security posture requires the review and update of implemented security controls to adapt to changes. Note: The security posture of an information system is assessed using the same methodology as security risks assessment, and is thus a closely related concept. The adequacy of a security posture implies that the residual risks are low.
Service	A Service provided to one or more customers by an IT service provider. An IT Service is based on the use of information technology and supports the customer's business processes. An IT Service is made up from a combination of people, processes and technology and should be defined in a Service Level Agreement. (ITIL v3 Glossary) Note: A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific cost and risks.
SMTP email protocol	Please refer to RFC 5321 - http://tools.ietf.org/html/rfc5321.
Successful Respondent	A Respondent who is identified by Canada to participate in the Review and Refine Requirements and Bid Solicitation phases of the procurement.
Supply Threat	A product can be easily tampered with in the supply chain to later facilitate a cyber-attack against that product in order to exploit a network and the information the network carries. Security requirements for cyber-protection, cyber-defence and supply threats risk mitigation must be met by Email Solution providers in order to successfully bid on GC shared IT services initiatives.
System	A generic term used to mean network and other devices, operating systems, computing platforms, virtualization software and applications or any combination thereof. Its use is context specific.

ANNEX B: ETI SCOPE MATRIX

The high level functional scope is defined below. Specific scope elements and detailed requirements (e.g. alignment to vision and strategy, use of standards, and integration with existing SSC services) will be refined and documented in more detail during the Review and Refine Requirements Phase.

Ref #	Scope	In Scope	Out of Scope	Interface Only	Comments
1.	Email				
	Standard Email Messaging Functionality	X			Support Standard Email functionality that is common in all major Commercial Off-the-Shelf (COTS) products.
	Historical Email Access	X			Provide users with access to their historical emails (active and archived) using the new Email Solution. The access will be limited based on the established retention period for SSC and its Partners.
	Fax Integration			X	Support interface to Central Fax Services and functionality.
	Mobile physical platforms		X		Email capability for physically mobile environments are out of scope (e.g. military deployments, naval ships)
2.	Calendaring/Scheduling				
	Standard Calendaring Functionality	X			Support typical Calendaring/Scheduling functionality that is common in all major COTS products.
	Free/Busy Look-up for users of the Common Email System	X			Allow users to view schedules (free/busy availability) and plan meetings with other users on the Common Email system.
	Free/Busy Look-up for users NOT on Common Email System.		X		
3.	Contact Management				
	Standard Contact Management Functionality	X			Support Standard Contact Tracking functionality that is common in all major COTS products.
4.	Mobile Device Management				
	Mobile Device Support (includes RIM BlackBerry® smartphones and Playbooks, Apple iPad® tablets and iPhone® smartphones, Android™ smartphones and tablets, etc.)	X			Allow users to access standard email and calendaring functionality using these devices. Breadth of support by device can vary based on device capabilities and constraints.

Ref #	Scope	In Scope	Out of Scope	Interface Only	Comments
5.	Directory				
	Email Directory	X			Users are able to find any other GC user(s) in the Common Email's directory via the address book services of the solution.
	Distribution List Management	X			The ability to create and manage distribution lists to facilitate communications with groups of recipients.
6.	Collaboration Tools				
	Instant Messaging	X			An Instant Messaging Solution will be implemented and available to all users of the Common Email Solution.
	Support other Collaboration features such as: Collaborative Workspaces; Web Conferencing; Application Sharing; Voicemail integration with email, and Discussion Forums, Wikis and Blogs.		X	X	Collaboration and Unified Communications technology and services are out of scope. However, future capacity to integrate to these technologies and services is in scope.
7.	Security Requirements				
	Anti-Spam / Anti-Virus	X			Support standard Anti-Spam and Anti-Virus functionality for messaging that is common in all major COTS products.
	GC Identify Credential Management Interface			X	The consolidated email service will have Encryption / Public Key Infrastructure functionality, however, the work to be completed will be handled outside of the requirements for this initiative.
	Secret Email Capability	X			Provide a Secret email capability for a subset of SSC users.
8.	Application Integration				
	Provide Standard Application Programming Interfaces (APIs) for email	X			Provide an industry standard interface to allow applications to send and receive emails (see Ref #10 - Open Standards Support for more information).
	Provide Standard APIs for calendaring	X			Provide an industry standard interface to allow applications to send and receive calendar events (see Ref #10 - Open Standards Support for more information).
	Provide Standard APIs for contacts	X			Provide an industry standard interface to allow applications to send and receive contact information (see Ref #10 - Open Standards Support for more information).

Ref #	Scope	In Scope	Out of Scope	Interface Only	Comments
	Integrate all legacy applications into the new Common Email system			X	This is the department's responsibility. SSC will provide an interface, and support itself and its Partners in their integration efforts.
	Deliver technical support and documentation to SSC and its Partners for Application integration	X			SSC will provide an interface, and support itself and its Partners in their integration efforts.
9.	Back-up and Archiving				
	Contingency planning (e.g., disaster/failure recovery)	X			The ability to gracefully recover email capabilities under disaster or various failure scenarios.
	Dedicated Email Archiving	X			Support Email Archiving and provide the ability for a user to easily recover archived email in an automated manner.
	Back-up/Restore mailbox	X			The capability to backup and restore email content globally, by group, and by mailbox.
	Integration with Information Management tools, such as Electronic Document and Records Management System (EDRMS), Records Documents and Information Management System (RDIMS), and GC-DOCS.			X	The email service will integrate with an EDRMS solution however the ETI is not responsible for determining or developing the solution.
10.	Other Technical Requirements / Constraints				
	Open Standards Support	X			Support open standards that allow for interoperability of various messaging components. Specific standards to be supported including, but not limited to, HTTPS, POP3 over TLS, IMAP, IMAP over TLS, SMTP, SMTP over TLS, LDAP, CalDAV, CalDAV over TLS, XMPP, RSS, OMA-DS, P-IMAP, WebDAV, WebDAV over TLS, LDAP over TLS, VoiceXML, SOAP, MIME, S/MIME, and delegated support for external authentication frameworks.
	End User Training	X			Online training / tutorial material will be available. Also, the Email Solution will prepare user training material and will train the trainers during transition.
	Single Sign-On / Simplified Sign-On	TBD	TBD	TBD	SSC would like to evolve to a Single Sign-On model in the future. During Industry Engagement, SSC will determine if the ETI can further this objective.

Ref #	Scope	In Scope	Out of Scope	Interface Only	Comments
11.	Migration Requirements				
	Migrate email and contacts	X			Migrate all legacy email content and contacts to the new environment.
	Migrate calendar events	X			Migrate all time-bound calendar events to the new environment.
12.	Service Establishment				
	Engage a private sector email service provider	X			
	Ensure the delivery of an on-going service management framework	X			As a reference model for defining a Service Management Framework, please refer to ITIL Version 3.

ANNEX C: CURRENT STATE SUMMARY

1. Overview of the Current Government of Canada Email Services

1.1 Architecture Issues

The GC hosts numerous email systems comprising a variety of architectures, designs, products and management processes. These represent a significant portion of the GC's larger information technology (IT) infrastructure footprint and are critical to GC's business operations.

There are many disparate IT infrastructures currently provisioning a multitude of email systems in the GC. Each department and agency operates with varying versions and release levels, and with varying levels of maintenance and security. Each email system is procured separately and operated and supported by individual department/agency management processes and IT support models.

At a high level, the following articulates some of the major areas of difference among SSC's Partners:

- Primarily highly de-centralized implementations present varying architectures, which creates differences in functionality, performance, and interoperability. It also creates unnecessary duplications of equipment/software purchases and implementations, as well as maintenance, support, and security protection. Examples of these discrepancies in architecture are:
    - Hardware: There are hundreds of servers of different makes and models located across the country in data centres, server farms and local offices
    - Software: There are multiple email software solutions across and within Partner departments and agencies. The various email systems are not fully compatible. While the majority of Partner departments and agencies use Microsoft Exchange/Outlook, there are a smaller number of implementations of IBM Lotus Notes and Novell GroupWise for email delivery services. Departments and agencies have different versions of software, and have adopted a variety of non-compatible processes and practices.
    - Versions: Both legacy and leading-edge products, with multiple versions, exist.
    - License Agreements: PWGSC, on behalf of each Partner department/agency, negotiates and maintains separate license agreements.
- Independent management of foundation infrastructures (including network and data centre resources) and IT support provided locally, with different Partner departmental and agency support models (1st, 2nd and 3rd levels), contribute to varying service levels. Examples of these service levels are:

- Availability;
- Disaster recovery procedures;
- Backup procedures and recovery capabilities;
- Storage/archiving policies (e.g. capacity, retention period);
- Incident and change management;
- Response time objectives, and
- Support services.

- Varying application of security products (e.g. anti-virus, anti-spam, intrusion detection, etc.), which results in inconsistent approaches to security and data privacy;
- Individual determination and application of email policies (e.g. mailbox size, attachment size, data retention periods, etc.), and
- Various methods and technologies used for integrating Business Applications with email systems.

1.2 Functionality and Capabilities

With regard to currently available email services within the GC, it is understood that the following functionality is generally provided:

- Mail;
- Contacts;
- Calendaring;
- Public and Shared Folders;
- Tasks, and
- Notes.

While most email systems are quite capable of providing the following services, it has yet to be determined if and how they are provisioned and consistently available for SSC's Partners:

- Bilingual user interfaces;
- Instant messaging;
- Anti-virus;
- Spam protection;
- Encryption;
- BlackBerry® Enterprise Server (BES) integration;
- Archiving, and
- Mobile support.

1.3 Email Inter-dependencies

While email systems are comprised of a number of specific messaging infrastructure components, they are also totally dependent on or are integrated

with a variety of other components to be able to provide an end-to-end email delivery service. These include:

- Desktop Client Presentation Layer;
- Business Applications;
- Security Platform;
- Directory Services;
- Data Centre Processing;
- Storage Capacity, and
- Network Capacity.

2. Current Email Components of SSC's Partners

The information and data presented in this Annex was collected via surveys conducted by SSC in November and December of 2011 for SSC's Partners (43 departments and agencies).

2.1 Summary of Quantitative Data

Table 1 (below) shows a summary of some of the most significant quantitative data that was collected. Due to the fact that the surveys were collected in the fall of 2011, the data may not be entirely current.

Type of Data	Sub-Total	Total
Total Number of Email Platforms		3
Total Number of Email Servers (Lotus 677; Novell - 159; MS Exchange – 867)		1,703
Total Number of Employees		377,804
Total volume of Email Storage (actual usage)		950 TB
Organizations that currently use Unified Communications		18
Total Departmental Applications integrated via Email (estimate)		2,250
Number of Outlook Licenses		369,480
Number of Networks		144
Number of MS Exchange Standard Licenses with SA	354	
Number of MS Exchange Standard Licenses without SA	125	
Number of MS Exchange Enterprise Licenses with SA	518	
Number of MS Exchange Enterprise Licenses without SA	324	
Total Number of MS Server Licenses		1,321
Number of MS Exchange CALs with SA	254,909	
Number of MS Exchange CALs without SA	68,965	
Total MS Exchange CALs		323,874
Number of Lotus Notes / Domino Licenses	23,535	
Number of Novell GroupWise Licenses	52,392	
Total number of Licenses (Exchange, Notes and GroupWise)		399,801

Number of User Mailboxes *	562,270	
Number of Generic Mailboxes	75,050	
Total Mailboxes		637,320
Number of BlackBerry® smartphones	70,167	
Other Mobile Devices	347	
Total Number of Mobile devices		70,514

Table 1: Summary of Quantitative Data

*The Number of User Mailboxes contains both active and inactive mailboxes for employees, consultants, students, ameritus scientists, etc. A mailbox can be made inactive when an employee has retired, transferred or accepted a secondment.

Note: The GC also has an Enterprise Agreement for Oracle Beehive software licenses. These licenses include messaging within a collaborative environment.

2.2 Email Systems

There are 63 individual email systems across the Partner departments and agencies. The total number of mailboxes across SSC is approximately 637,320, which includes 562,270 user mailboxes and 75,050 resource mailboxes. The five largest SSC entities represent 59% of all mailboxes.

Of the 63 email systems within the Partner departments and agencies, the individual systems are divided among three types of software applications and supporting hardware systems:

- Microsoft Exchange (server) and Microsoft Outlook (client);
- Novell GroupWise, and
- IBM Lotus Notes.

Each of these email systems is procured, implemented, supported, and operated individually, and has a dedicated BlackBerry® server environment.

The following statistics define the current overall size of the SSC email service: Approximately 59% of the SSC mandated organizations' population (168,102) is regional, while 41% (114,898) are situated in the National Capital Region (NCR).

2.3 Mobile Devices

BlackBerry® Services are an integral part of the GC's existing email infrastructure. Generally, this provides BlackBerry® users with mobile access to the organization's resources including messaging, calendar, contact information, and wireless Internet and Intranet access. Some departments and agencies provide access to online business and/or corporate administrative applications via a BlackBerry® smartphone or other mobile device.

Currently, there are approximately 70,514 mobile devices (70,167 BlackBerry® smartphones and 367 other smartphone devices) deployed for SSC's Partners. The

top five departments and agencies (DND, Royal Canadian Mounted Police (RCMP), Department of Foreign Affairs and International Trade (DFAIT), Canada Revenue Agency (CRA), and Human Resources and Skills Development Canada (HRSDC)) represent almost 50% (49.8%) of all mobile devices currently deployed.

2.4 Mobile Applications

Currently, there are very few departmental business applications that are installed on mobile devices across the Partner departments and agencies. In fact, only seven SSC organizations (Agriculture and Agri-Food Canada (AAFC), Health Canada, HRSDC, Parks, Privy Council Office (PCO), Transport Canada and Treasury Board Secretariat (TBS)) have business applications installed on mobile devices. Among these seven organizations, there are a total of eleven different email-enabled applications deployed on the mobile devices.

2.5 Directory Services

A directory domain service is an infrastructure component that email systems cannot exist without. However, it is not considered to be a specific email system component, as it facilitates most, if not all, distributed services, including user authentication or user access control. It is the directory service that provides email users a directory of all departmental employees, as well as access to the GC Global Address List (GAL) for a listing of employees from other government organizations that have decided to share their directories.

In addition to the many variations in the GC email systems, each of them is reliant on its own department-based mail directory service. Across the entire GC, there are approximately 700 directory implementations (the majority are Microsoft (MS) Active Directories) associated with the distribution of email systems. Many departments and agencies integrate the desktop sign-on and authentication with email access to effectively manage infrastructure costs, while most, but not all, offer direct access to email via desktop sign-on.

Email directories are implemented as follows for SSC's Partners:

- 32 MS Active Directory services
- 5 Lotus directory services
- 8 Novell directory services

Note: The total number of directories above equals 45 (instead of 43) because two of the Partners (HC and Industry Canada (IC)) that use two directories. As noted previously, many of these directory services are implemented in a decentralized environment.

2.6 Network

All GC email systems are dependent on and supported by 144 underlying telecommunications networks. Each of these is a separate network supporting a variety of departmental services, including but not limited to email.

With the exception of some large departments and agencies (including: Canada Border Services Agency (CBSA), CRA, DND, and RCMP), most of these networks are procured by leveraging shared common contracts under the GC Converged Network Services. Also, SSC's Partners have connectivity to the GC Secure Channel Network (SCNet) and a large number of them (26) are already connected to the GC Shared Metropolitan Area Network (MAN) Service (SMS). It should also be noted that there are networking agreements in place (for some of SSC's Partners) for international connectivity requirements.

SSC can leverage the GC's SMS infrastructure and current departmental connectivity to facilitate the deployment of a consolidated email system for all SSC employees across the country. Currently, SMS is local to the NCR only, whereas GC's SCNet has national scope.

Email services are provisioned in centralized, decentralized or mixed fashions depending on the capability of each department's and agency's network design, including Wide Area Network (WAN) optimization, network topology, bandwidth management, etc.

2.7 Storage

Centralized email systems rely on enterprise storage solutions referred to as SANs (Storage Area Networks) which have the ability to store a considerable amount of mail centrally and provide various tiers of client and business services from online storage to archiving. While most of SSC's Partners have central storage implementations, they are used quite differently in terms of data retention periods for unstructured data and archiving (e.g. choice of tier for primary versus archived storage), self-service retrieval and other storage services. Therefore, statistics gathered via a survey in the fall of 2011 of all 43 Partner departments and agencies cannot clearly represent the utilization of storage media.

Distributed email systems, on the other hand, tend to store client content on less expensive local storage, typically the disk drives of local file and print servers. Regardless of the storage medium, different approaches are taken to store emails locally (e.g. Microsoft users use Personal Storage Tables [PSTs]). Some departments and agencies permit local file storage to be managed via email mailboxes, which influences the amount of storage departments and agencies are reporting as email-related, while others treat them as personal file storage. Current backup and storage practices are very different across SSC's Partners. Storage practices vary between three and five years of data, or in many situations organizations retain email records until users actually leave the organization.

According to Fall 2011 survey results, the total email storage currently being used across the 43 SSC organizations is approximately 950 Terabytes (TB), and approximately 60% (~573TB) of storage is managed in a centralized manner in

the NCR, while 40% (~377TB) remains locally managed in the regions. Of the 950TB of storage, CRA manages 385TB, which represents 40.5% of the total data stored by SSC's Partners. The top five organizations with the most storage (CRA, DFAIT, HC, Statistics Canada (StatCan), and HRSDC) make up 58.0% of the total storage of SSC departments and agencies. However, Canada estimates that the total email storage currently being used by SSC's Partners is as high as 1,600TB (1.6 Petabytes) because some of the Partners were not able to report on personal file storage (e.g. PSTs) amounts in their reporting.

2.8 Archiving

Approximately 44% of the Partners have implemented an archive solution that services email. However the departmental policies, guidelines, processes, and tools vary greatly, and a standard archiving solution does not exist.

2.9 Data Retention

No single email characteristic demonstrates the noticeable differences between the Partner departments and agencies as much as data retention guidelines. While some organizations keep their data for 30 days, others keep it for up to seven years, and one Partner indicated that they retain the information indefinitely.

2.10 Security Protection

Today, the GC's dependence on technology has increased Canada's risk of data loss or manipulation to accidental and/or malicious behaviour, and has elevated the need for a wide variety of security solutions for prevention and/or remediation.

All email is subject to security measures designed to protect the integrity of the GC data and the computing environment, including: firewalls, filters for viruses, intrusion detection, SPAM protection, inappropriate content and attachment screening, etc. Each Partner's email system currently permits Protected A, Protected B and/or Secret data and applies its interpretation of the required level of security protection potentially including, but not limited to, a variety of security products and versions of software and hardware solutions.

In addition, most, if not all, departments and agencies have developed strict policies for the implementation of PKI solutions, requiring a unique user certificate for email messaging encryption and digital signature capabilities.

In the survey, all of SSC's Partners identified that they had multiple security defences for their respective email systems, such as anti-spam, anti-virus, intrusion detection and/or firewall. Multiple programs and software versions are used for email security defence.

2.11 Email Enabled Applications

Today's email systems allow for the integration of business/administrative applications. The number of applications is significant with varying levels of integration to email.

An initial consultation with SSC's Partners has revealed that there are approximately 2,250 applications, both internally developed and COTS, which may be integrated into the consolidated Email Solution. Integration of these applications into a new email service varies in complexity.

3. Email Usage

3.1 Examples of Email Usage

Examples of common "internal" email use include functions, such as:

- Mail / calendaring / scheduling;
- Notification (news/broadcast information);
- Collaboration (exchanging information);
- Approvals (leave/financial/work flow etc.), and
- Mobile communications (e.g. BlackBerry®).

Specific "internal" departmental use of email includes functions such as:

- Health Canada – Internal product safety information dissemination;
- Canadian Food Inspection Agency (CFIA) notifies all inspectors immediately concerning food recalls, and
- DFAIT uses email for consular and diplomatic communications.

Examples of external email use include the following functions:

- Communication with citizens – canadasite@canada.ca. This is an HRSDC program along with 1-800-OCanada to answer any citizen questions;
- HRSDC also communicates with provinces for Labour Market Agreements;
- PWGSC's Acquisition Branch communicates with Canadian businesses to send out RFPs (TBIPS, TSPS), send out contracts to bidders, and answer questions from organizations;
- Industrial Security Sector (ISS) communicates with company business officers with regards to personnel security clearances;
- CRA communicates with Canadian businesses and citizens to confirm state of transactions;
- CBSA issues Amber alerts, also some post border operations such as transmitting refugee information between OGDs;
- DND uses "anonymous" email addresses for security reasons;
- RCMP communicates with external policing agencies (e.g. Interpol);
- Health Canada communicates public health issues and responses;

- DFAIT communicates with diplomatic community and foreign governments, and
- CFIA uses SMTP email for alerts.

3.2 User Locations

Another significant factor related to the SSC email system is the locations from which users access the SSC email systems. There are over 1,000 client locations across Canada and abroad with hundreds of locations with email servers.

ANNEX D: ANTICIPATED (DRAFT) REQUEST FOR RESPONSES FOR EVALUATION - PROCESS FOR IDENTIFICATION OF SUCCESSFUL RESPONDENTS

1. Introduction

In accordance with the Request for Responses for Evaluation (RFRE) Phase of the CPS procurement approach, Canada will issue an RFRE document in the future. Based on the evaluation scores of the Respondents to the RFRE, a subset of Respondents will be identified by Canada to participate in the subsequent “Review & Refine Requirements” and “Bid Solicitation” phases.

This Annex contains mandatory and point-rated technical criteria for the RFRE Phase to identify the Successful Respondents. These evaluation criteria are considered essential to deliver an enterprise Email Solution of the size, scope, and complexity of the ETI.

These mandatory and point-rated technical requirements may change depending on industry feedback.

Please refer to Part IV - Questions, for specific industry questions related to the proposed evaluation procedures and identification of Successful Respondents.

2. Evaluation Procedures

An evaluation team composed of representatives of SSC and PWGSC will evaluate the Respondent’s response to the RFRE. PWGSC and/or SSC may hire any independent consultant, or use any GC resources, to evaluate the responses. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

Respondents must meet the Mandatory Technical Requirements to be considered as a Successful Respondent, eligible to participate in the Review & Refine Requirements Phase.

PWGSC has engaged a Fairness Monitor for this procurement. The Fairness Monitor will not be part of the evaluation team, but will observe the evaluation with respect to Canada's adherence to the evaluation process described in this RFRE.

3. Conditions for the RFRE and/or RFP

3.1 Security

The Respondent must meet the security requirements detailed in this RFI

3.2 Financial Viability

The Respondent must have the financial capability to undertake this requirement. In order to demonstrate its financial capability, PWGSC may require the submission of financial information.

4. Mandatory Corporate Technical Experience Requirements

Canada seeks to identify Respondents with a proven track record for designing, building and deploying an enterprise Email Solution, as described in Part III of this Request for Information - Anticipated Mandatory Requirements.

Respondents will be required to demonstrate compliance with all of the following Mandatory Corporate Technical Experience Requirements and will be required to provide the necessary documentation to support compliance.

The Mandatory Corporate Technical Experience Requirements listed below will be evaluated on a simple pass/fail (e.g. compliant / non-compliant) basis. Respondents that fail to meet any of the following Mandatory Corporate Technical Experience Requirements will be discarded without further consideration.

4.1. Corporate Experience

In order to address the Mandatory Corporate Technical Experience Requirements of M02, the Respondent must provide a list containing a minimum of 10 corporate customer email transformation projects over the last 5 years, as of the issue date of this document, including the:

(i) Name of the Corporate Customer;
(ii) Name and a brief description of the project;
(iii) Date and duration of the project, and
(iv) Corporate Customer contact name, phone number and/or email address.

In order to address the Mandatory Corporate Technical Experience Requirements of M01, M03, M04, M05 and M06, the Respondent must provide detailed information about the work your organization performed, including information related to the email platform used, for 3 of the 10 projects in the list above. One of these projects must have involved the implementation of a secure Email Solution, including the capability to process Secret emails.

The mandatory requirements of M01 through M06 can be demonstrated using 1 or more of the 3 projects, but do not have to be the same for each mandatory requirement (M01 to M06).

For this purpose, a Respondent may use their own corporate email system as a reference. Canada may conduct reference validation checks in writing by email, to validate that the information provided by the Respondents is true and accurate.

M01: The Respondent must have designed, architected, built and implemented an Email Solution as a Managed and/or Outsourced service provider, for a minimum of 10 Corporate Customers over the last 5 years, as of the issue date of this document.

M02: The Respondent must currently be provisioning and operating email services for a minimum of 10 Corporate Customers with:

(i) A minimum of 100,000 combined users for the combined Corporate Customers;
(ii) At least one Corporate Customer consisting of a minimum of 50,000 users, and
(iii) At least one Corporate Customer in Canada consisting of a minimum of 25,000 users.

M03: The Respondent must have designed, architected, built, implemented and operated at least one secure Email Solution, consisting of a minimum of 500 users, including the capability to process Secret emails, over the last 5 years, as of the issue date of this document.

M04: The Respondent must have been providing email services operating 24 hours per day, 7 days per week, and 365 days per year over at least the last 2 years, as of the issue date of this document, for a minimum of 3 Corporate Customers, consisting of a combined minimum of 50,000 users, and a bilingual (French and English) email service desk is provided for a minimum of 1 Corporate Customer. The email service desk must be in Canada.

M05: The Respondent must have conducted the migration of email systems, in the last 5 years, as of the issue date of this document, where the transformation involved at least 10,000 mailboxes, on one of the following email platforms:

(i) Microsoft Exchange;
(ii) Novell GroupWise, or
(iii) IBM Lotus Notes Email.

M06: The Respondent must have conducted the conversion of business applications integrated with email systems, in the last 5 years, as of the issue date of this document, where the transformation consisted of at least 10,000 mailboxes, on one of the following email platforms:

(i) Microsoft Exchange;
(ii) Novell GroupWise, or
(iii) IBM Lotus Notes Email.

5. Point-Rated Technical Requirements

Respondents that meet all of the Mandatory Technical Requirements will then be evaluated and scored in accordance with Point-Rated Technical Requirements (R1 to R3 described below), based on the Respondent's experience of designing, constructing, deploying and operating an enterprise Email Solution, as described in this RFI.

In this regard, Canada will rate Respondents on the following Point-Rated Technical Requirements:

(i) Corporate Experience;

(ii) Service Obligation, and
(iii)Email Transformation Experience.

Each Respondent's submission will be rated in accordance with the Point-Rated Criteria, identified in RFRE by the word "rated" or by reference to a score. Respondents who fail to submit complete information as requested in the RFRE will be rated accordingly.

Ref ID	Rated Requirement	Maximum Value	Weight
R1	Corporate Experience	600	40.0
R2	Service Obligation	100	10.0
R3	Email Transformation Experience	700	50.0
	Total	1,400	100.0

Point-Rated Technical Requirements

Reference ID	Rated Requirement	Value	Weight
R1	**Corporate Experience**		**40%**
R1.1	The Respondent should provide the number of Corporate Customers for which it provided and operated email services, 24 hours per day, 7 days per week, and 365 days per year. Point Scale 4 - 5 Corporate customers – 25 6 - 9 Corporate customers – 50 10 or more Corporate Customers – 100	100	
R1.2	The Respondent should demonstrate a proven track record, covering the last 5 years, as of the issue date of this document, for designing, building, deploying, and operating an Email Solution for a Complex Email Transformation Project. Point Scale 1 project – 100 2 or 3 projects – 150 More than 3 projects – 200	200	
R1.3	The Respondent should demonstrate a proven track record, covering the last 5 years, as of the issue date of this document, for designing,	100	

	building, deploying, and operating an Email Solution that had to conform with GC policies and legislative processes. Point Scale 1 project – 50 2 or 3 projects – 75 More than 3 projects – 100		
R1.4	The Respondent should demonstrate a proven track record, covering the last 5 years, as of the issue date of this document, for designing, building, deploying, and operating a secure enterprise Email Solution for a minimum of 500 users, including the capability to process Secret emails. Point Scale 2 or 3 projects – 150 More than 3 projects – 200	200	
R2	**Service Obligation**		**10%**
R2.1	The Respondent should provide the number of Corporate Customers for which it provides a bilingual (French and English) Email Solution service desk(s). Point Scale 2 or 3 customers – 50 points More than 3 customers – 100 points	100	
R3	**Email Transformation Experience**		**50%**
R3.1	The Respondent should identify the number of Corporate Customer mailboxes that the Respondent has migrated. Point Scale 10,000 – 99,999 mailboxes: 50 points 100,000 – 199,999 mailboxes: 75 points 200,000 or more mailboxes: 100 points	100	
R3.2	The Respondent should demonstrate a proven track record, covering the last 5 years, as of the issue date of this document, for managing and conducting the migration of email systems involving at least 10,000 mailboxes, on one of the following email platforms:	200	

	i) Microsoft Exchange; ii) Novell GroupWise, or iii) IBM Lotus Notes Email. Point Scale: 2 or 3 projects – 100 More than 3 projects – 200		
R3.3	The Respondent should demonstrate a proven track record, covering the last 5 years, as of the issue date of this document, for managing and conducting the conversions of business applications involving at least 10,000 mailboxes, on one of the following email platforms: i) Microsoft Exchange; ii) Novell GroupWise, or iii)IBM Lotus Notes Email. Point Scale: 2 or 3 projects – 100 More than 3 projects - 200	200	
R3.4	The Respondent should demonstrate a proven track record, covering the last 5 years, as of the issue date of this document, for successfully migrating **all email data**, without loss of data or service level degradation. Point Scale: 1 project – 75 2 - 3 projects – 150 4 projects or more - 200	200	

5. Corporate Customer Reference Check

As part of the reference verification process for the RFRE, Corporate Customers may be contacted by email, to confirm that the information provided by Respondents in a Reference Project Verification Form (to be designed) is true and accurate.

6. Identification of Successful Respondents

Canada may consider inviting only top ranked Successful Respondents to participate in the subsequent Review and Refine Requirements and/or Bid Solicitation phases of the CPS procurement process.

The identification of top ranked Successful Respondents will be based on a selection methodology to be determined and included in the RFRE.

ANNEX E: SSC PARTNER DEPARTMENTS AND AGENCIES

Aboriginal Affairs and Northern Development Canada (AANDC)
Agriculture and Agri-Food Canada (AAFC)
Atlantic Canada Opportunities Agency (ACOA)
Canada Border Services Agency (CBSA)
Canada Economic Development for Quebec Regions (CED)
Canada Revenue Agency (CRA)
Canada School of Public Service (CSPS)
Canadian Food Inspection Agency (CFIA)
Canadian Heritage (PCH)
Canadian International Development Agency (CIDA)
Canadian Northern Economic Development Agency (CanNor)
Canadian Nuclear Safety Commission (CNSC)
Canadian Space Agency (CSA)
Citizenship and Immigration Canada (CIC)
Correctional Service of Canada (CSC)
Department of Finance (FIN)
Department of Justice (JS)
Department of National Defence (DND)
Environment Canada (EC)
Federal Economic Development Agency for Southern Ontario (FedDev Ontario)
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
Fisheries and Oceans Canada (DFO)
Foreign Affairs and International Trade Canada (DFAIT)
Health Canada (HC)
Human Resources and Skills Development Canada (HRSDC)
Immigration and Refugee Board of Canada (IRB)
Industry Canada (IC)
Infrastructure Canada (INFC)
Library and Archives Canada (LAC)
National Research Council Canada (NRC)
Natural Resources Canada (NRCAN)
Parks Canada (PC)
Privy Council Office (PCO)
Public Health Agency of Canada (PHAC)
Public Safety Canada (PS)
Public Service Commission of Canada (PSC)
Public Works and Government Services Canada (PWGSC)
Royal Canadian Mounted Police (RCMP)
Statistics Canada (StatCan)
Transport Canada (TC)
Treasury Board of Canada Secretariat (TBS)

Veterans Affairs Canada (VAC)
Western Economic Diversification Canada (WD)

ANNEX F: DRAFT SECURITY REQUIREMENTS CHECKLIST (SRCL)

The following is the SRCL. To view the form, you must double-click on the object below.

"SRCL draft.pdf"

Object 1 Draft SRCL

ANNEX G: LEGISLATION AND TREASURY BOARD SECRETARIAT POLICY INSTRUMENTS

The policy instruments below may impact the Email Transformation Initiative. This list is currently under review, and is subject to change.

1. Policies

Policy on Government Security
Common Services Policy
Access to Information Policy
Policy on Privacy Protection
Communications Policy
Contracting Policy
Policy Framework for the Management of Assets and Acquired Services
Policy on the Management of IT
Official Languages Policy Framework
Policy on the Duty to Accommodate persons with disabilities in the federal public service
Policy on the Management of Projects
Policy on the Use of Electronic Networks
Policy on Information Management

These policies are accessible at: http://www.tbs-sct.gc.ca/pol/index-eng.aspx?tree=a2z.

2. Directives

Directive on Identity Management
Directive on the Management of IT
Directive on Record Keeping

These are directives accessible at: http://www.tbs-sct.gc.ca/pol/index-eng.aspx?tree=directive.

3. Standards / Guidelines

Management of Information Technology Security (MITS)
Standard on Electronic Documents and Records Management Solutions
Standard on Metadata
Standard on Web Accessibility/Usability
TBITS 26: Software Product Evaluation, Quality Characteristics and Guidelines for their User
TBITS 3: Coded Character Sort for Information Interchange
TBITS 36: All Numeric Representation of Dates and Times
TBITS 6.9: Canadian open systems application criteria (COSAC), telecommunication wiring system in GC owned and leased buildings

These standards and guidelines are accessible at: http://www.tbs-sct.gc.ca/pol/index-eng.aspx?tree=standard and http://www.tbs-sct.gc.ca/pol/index-eng.aspx?tree=guideline.

Legislation information can be found at: http://laws-lois.justice.gc.ca/eng/index.html.

ANNEX H: NON-DISCLOSURE AGREEMENT

MUTUAL
NON-DISCLOSURE AGREEMENT
between

_____

and
HER MAJESTY THE QUEEN IN RIGHT OF CANADA,
as represented by
THE MINISTER OF NATIONAL DEFENCE
on behalf of
THE COMMUNICATIONS SECURITY ESTABLISHMENT

Nature of Agreement

1. This is a non-disclosure agreement between_____ (the "Company"), a body corporate incorporated under the laws of_____ and having principal offices at _____: and the Communications Security Establishment ("CSE"), having offices at 719 Heron Rd., Ottawa K1G 3Z4.

Purpose of Agreement

2. The purpose of this agreement is to enable the CSE to provide sensitive supply threats information which leads to risk mitigation strategies for potential Email Solution providers of the Email Transformation Initiative, (ETI solution for the Government of Canada (GC) and for CSE to receive company proprietary and/or competition sensitive information.

Definition

Sensitive Information when used in relation to information means information identified or classified by the Crown as TOP SECRET, SECRET, CONFIDENTIAL OR PROTECTED.

Terms and Conditions of Agreement

3. In consideration of the mutual exchange of information, and the mutual covenants contained in this Agreement, the Company and CSE hereby agree as follows:

Company Proprietary Information

4.

(a) Whenever the Company discloses to CSE information which the Company deems proprietary and/or competition sensitive, the Company shall then and there clearly identify such information, in writing, as "Proprietary Information", and

(b) If such disclosure is made orally or visually, such oral or visual information shall be identified as Proprietary Information at the time of its disclosure, and the fact that it is Proprietary Information shall be reduced to writing promptly by the Company.

5. CSE shall hold identified Proprietary Information in confidence between itself and other government agencies and shall use such Proprietary Information only for the Purpose stated above.

6. The parties acknowledge that this non-disclosure agreement is subject to the *Access to Information Act* (R.S.C. 1985, c. A-1, as amended) and that requests for any information that is subject to this non-disclosure agreement will be governed by the provisions of that *Act.*

7. Proprietary Information shall not be afforded the protection of this Agreement if such Proprietary Information:

(a) has been developed by CSE independently or is already known by CSE at the time of disclosure;

(b) is known or available to CSE from a source other than the Company, without breach of this Agreement by CSE;

(c) has been made a part of the public domain; or

(d) has been released without restrictions by the Company to anyone.

8. All Proprietary Information shall remain the property of the Company and shall be returned to it or destroyed, at the option of the Company, upon request by the Company, within 30 days following such request.

CSE Sensitive Information

9.

(a) Whenever CSE discloses information to the Company which CSE deems

(b) Sensitive, CSE shall clearly identify such information, in writing, as "Sensitive

(c) Information", and

(d) If such disclosure is made orally or visually, such oral or visual information shall be identified as Sensitive Information at the time of its disclosure and the fact that it is Sensitive Information shall be reduced to writing promptly by CSE.

10. The Company shall hold identified Sensitive Information in confidence. The Company shall not permit any person to have access to any Sensitive information unless

the person is a Company employee, who has a security clearance commensurate with the level of sensitive information being accessed, without the prior written consent of CSE. The Company shall immediately notify CSE if any person accesses sensitive information without the appropriate security clearance.

11. All Sensitive Information shall remain the property of CSE and shall be returned to CSE or destroyed, at the option of CSE, upon request by CSE, within 30 days following such request.

General

12. This Agreement shall be governed, construed and interpreted in accordance with the laws of the Province of Ontario, Canada.

13. This Agreement shall come into force when signed by both parties and remain in force for_____ years, unless earlier terminated in writing signed by both parties.

14. This Agreement may only be amended in writing signed by both parties.

_____	Communications Security
Company Name	Establishment
_____	_____
Signature	Signature
_____	_____
Title	Title
_____	_____
Date	Date

ANNEX I: REGISTRATION FORM FOR A SUPPLY THREATS BRIEFING BY CSEC

Supply Threats Briefing Registration Form

Note: Canada will determine the date(s)/time(s) when this/these briefing(s) will take place, and notify all parties that submitted this form of the logistics via email at a later date.

What is the name of your firm/association?

Name: _____

Please indicate the location(s) from which your representatives will attend the session as well as the representatives' names who will be attending at each location:

Location	Representative Names	Location	Representative Names
Calgary		National Capital Region	
Edmonton		Toronto	
Halifax		Vancouver	

Montreal		Winnipeg	

Please provide an email address that PWGSC can use to reply to you for confirmation of the date(s)/time(s) and address/room location(s):

Email Address: _____

The duly signed NDA must be signed and submitted with this registration form.

ANNEX J: REGISTRATION FORM FOR RFI WORKSHOP

RFI Workshop Registration Form

Note: Canada will determine, and notify all parties that submitted this form, the address/room location for these meetings, by no later than 4:00 p.m. EDT on July 3, 2012.

What is the name of your firm/association?

Name: _____

Please indicate the location(s) from which your representatives will attend the session as well as the representatives' names who will be attending at each location:

Location	Representative Names	Location	Representative Names
Calgary		National Capital Region	
Edmonton		Toronto	
Halifax		Vancouver	

Montreal		Winnipeg	

Please provide an email address that PWGSC can use to reply to you for confirmation of the address/room location:

Email Address: _____