RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions -TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0A1 / Noyau 0A1
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

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

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

Title - Sujet Email Transformation Initiative	
Solicitation No. - N° de l'invitation 2B0KB-123327/A	**Amendment No. - N° modif.** 002
Client Reference No. - N° de référence du client 20123327	**Date** 2012-07-11
GETS Reference No. - N° de référence de SEAG PW-$TSS-002-24459	
File No. - N° de dossier 002tss.2B0KB-123327	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2012-07-31**	**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: Knowles, Jason	**Buyer Id - Id de l'acheteur** 002tss
Telephone No. - N° de téléphone (819) 956-1418 ( )	**FAX No. - N° de FAX** (819) 956-5165
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
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**	

This revision is issued to provide industry with information as discussed at the Industry Day information session which took place on June 12, 2012 in accordance with the details set out in the Request for Information (RFI):

“Presentations made by Canada, the list of attendees and general responses to questions will be published on the MERX web site (www.MERX.com - the electronic tendering service used by Canada) after the Industry Engagement Day session.”

Attached:

- Industry Day Presentation
- Industry Engagement Day Summary Report
- Industry Engagement One-on-One Sessions Summary Report

There are no further changes to the information currently forming part of this RFI.


Email Transformation Initiative
Industry Engagement Day
June 12 2012
Welcome

Industry Day Objective

Industry Engagement Day Agenda

Time	Presenter	Description
1:30-1:35	Moderator	• Industry Day Objectives
1:35 – 1:50	President, Shared Services Canada	• Welcome
1:50 – 2:00	ADM, Acquisitions Branch, Public Works and Government Services Canada	• Procurement Opening Remarks
2:00 – 3:00	Shared Services Canada: Senior Assistant Deputy Minister of Transformation, Service Strategy and Design Director General, Email Transformation	• Email Transformation Initiative Description and Objectives • Current State • Scope and Requirements • Solution Options being Considered
3:00 – 3:15	Break	
3:15 – 3:35	Communications Security Establishment Canada	• Cyber and Supply Threats to the Government of Canada
3:35 – 3:50	Acquisitions Branch Public Works and Government Services Canada	• Industry Engagement • Overview of the Collaborative Procurement Solutions Approach
3:50 – 4:45	Questions and Answers	
4:45 – 5:00	Recap and Closing Remarks	

Shared Services Canada

Liseanne Forand,

President of Shared Services Canada

Respect ♣ Integrity ♣ Excellence ♣ Leadership

Serving GOVERNMENT, Serving CANADIANS.

Public Works and Government Services Canada

Tom Ring

Assistant Deputy Minister, Acquisitions Branch

Email Transformation Initiative

Industry Engagement Day Briefing

Benoît Long,
Senior Assistant Deputy Minister,
Transformation, Services
Strategy and Design

Gail Eagen
Director General
Email Transformation Initiative

Email Transformation Initiative

Email Transformation Initiative Overview

- Project Objective
- Business Drivers
- Desired Business Outcomes
- Current State
- Project Scope
- Email Service Delivery Options
- Key Requirements
- Other Considerations
- Areas we need your input …

Email Transformation Initiative (ETI)
Overall Project Objective

Business Drivers

Industry benchmarks for email have identified significant cost savings potential for the Government of Canada

Complexity

- 100 different email system configurations across the Government of Canada
- Within the 43 SSC Partner Departments and Agencies:
  - 81% using Microsoft Exchange
  - 13% Novell GroupWise
  - 6% IBM Lotus Notes –
  - A range of software versions installed
- Increasing demand for mobile access (Blackberry, Tablets, etc.)

Business Drivers

Security Pressures

- Citizens and private sector organizations rely on on-line services to communicate with the Government of Canada
- Email is a key channel
- Email security has been implemented using different strategies to meet departmental requirements
- Cyber-threats are on the rise

Service Delivery Consistency

- Varied service levels are in place across the partner organizations
- Complex email naming conventions are in place

Desired Business Outcomes

- Establishment of a consolidated email solution for the Government of Canada, starting with our partners and then offering to other departments and agencies
- Reduction in costs to deliver email services
- Continuous improvement to the security posture of email services so that programs and services can be delivered securely and reliably to Canadians
- Consistent naming standards
- Common service levels for all users
- Secure and reliable email service that can process emails - Classified up to Secret and Designated up to Protected C

Current State

Access for Canadian Citizens & Business

- Email is a channel of communications for citizens/business to access GC programs but not used extensively for transactions
- Current state is complicated by numerous departmental naming conventions, security and privacy concerns

Effectiveness – Productivity Tool

- The GC could make better use of email by segmenting users into groups based on the functions they need (i.e. Civilian and Military, or mobile and non-mobile users)
- Current systems do not promote collaboration among departments and agencies (i.e. Non-integrated calendaring)

Costs

- Benchmarks show the GC has significant opportunity for cost savings
- 63 email systems in 43 SSC partners
- 377,804 employees, 637,000 mailboxes and 70,000+ Blackberries
- 1700+ email servers

Security and Performance

- Current systems are complex:
  - Different technologies
  - At least 700 email directories
  - Distributed and centralized systems in place
- High diversity - difficult to standardize
- Systems require standardization for records management, retention policy and privacy

ETI: What is in Scope?

Functional

- Email
- Instant messaging
- Calendar
- Personal Contacts
- Personal and Shared Email Folders
- Email Fax Service Integration
- Historical Email Access (Email Archiving)
- Email Directory
- Email Anti-Virus / Anti-Spam
- Mobile Device Management (Blackberry, Smart Phone, Tablet)

Other

- Classified up to Secret and Designated up to Protected C
- All SSC Partner Locations in Canada, as well as all Embassies and Missions
- Data Migration and Transition
- Implementation and Training Support
- On-going Email and User Support
- Integration Support for GC ”Corporate” and “Program” applications (via standard interface toolkits)

ETI: What is out of scope?

Where we need more industry feedback…

Options	*Descriptions*	*Details*
Managed Service (Hybrid)	**Crown Owned, Vendor Operated**	**Vendor would design, build and operate the new email system on GC managed premise.**
Fully Outsourced Service	**Vendor Owned & Operated**	**Vendor would design, build and provide an email service to the GC.**

1. SSC recognizes that there is a “continuum” of infrastructure sourcing options for Managed Services and Full Outsourcing.
2. SSC is interested in hearing about any other options that industry considers viable and cost effective to meet SSC’s needs.
3. SSC has made significant investments in hardware, software, training and application integration. SSC is interested in hearing how industry would leverage this investment as Government Furnished Equipment (GFE).

Key Requirements

BUSINESS AND FUNCTIONAL REQUIREMENTS

1. **CONSOLIDATED EMAIL** - The email solution must consolidate and modernize Shared Services Canada (SSC) mandated email services for SSC and its Partners. The new solution must be made available to the rest of the Government of Canada.

2. **USER FRIENDLY** - The email service must be user-friendly and intuitive, requiring limited formal training.

3. **ACCESSIBLE –** The service must be available to all SSC partner locations in Canada, as well as all Embassies and Missions abroad. The system must be available in both official languages. The email solution must meet the standards on accessibility, and accommodate those with special needs, e.g. interoperability with applications to support visually and hearing impaired employees.

4. **MOBILITY SUPPORT** - The service must provide Mobile Device Management capabilities for platforms such as Research in Motion (RIM) Blackberries, Apple iPhones and iPads, and Android/Windows smart phones and tablets.

5. **AVAILABLE AND RELIABLE** - The email service has a target of 100% uptime for users, on a 24/7/365 basis.

Key Requirements

BUSINESS AND FUNCTIONAL REQUIREMENTS

6. **BROAD INTELLIGENT SEARCH -** The service must support end-user email message and content search.

7. **LOCAL EMAIL ADMINISTRATION SUPPORT –** The service must allow for SSC and partner personnel to perform email administrative functions such as adding and removing accounts, and resetting passwords.

8. **LEGISLATIVE AND POLICY ALIGNMENT** – The service must adhere to existing Legislation and Treasury Board instruments (e.g. policies, standards, guidelines). Note: Treasury Board Secretariat is addressing any policy gaps resulting from the implementation of a “cross government” email service.

9. **TIME SENSITIVE -** The end date for the implementation (including migration) is targeted for March 31, 2015.

10. **COST EFFECTIVE –** This initiative must enable the Government of Canada to deliver email services at costs that are on par with industry and peer groups.

Key Requirements

SECURITY and PRIVACY REQUIREMENTS

1. **SECURE** - The new email service must be certified to accommodate emails: Classified up to Secret and Designated up to Protected C.

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)
   - Protection for data in motion (e.g. encryption)

3. **TRUSTED SUPPLY CHAIN** – Please reference CSEC Presentation "Cyber and Supply Threats to the Government of Canada" for more information on this requirement.

4. **PRIVACY -** The service must ensure that information is accessible only to those authorized. The service must comply with the statutory obligations under the Privacy Act and the Access to Information Act.

5. **NATIONAL SECURITY EXCEPTION (NSE) –** The Email Transformation Initiative falls under the NSE recently invoked by PWGSC on behalf of SSC.

Key Requirement: Vendor Security Profile

- SSC will be finalizing the Vendor Security Profile requirements after the Industry Engagement phase.

- Our objective is to provide as much time as possible for companies to arrange their security clearance.
  - Please go to http://ssi-iss.tpsgc-pwgsc.gc.ca/questions/esosp-psos-eng.html for more information.

- 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.

Key Requirement: Data Sovereignty

Principle

SSC will safeguard the security and privacy of all data for which it is responsible and will ensure the Government of Canada's requirements with respect to data sovereignty are met. Vendors will be required to demonstrate their ability to maintain Government of Canada data sovereignty.

At a minimum:

1. All data are the property of the Government of Canada
2. 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. Off-site storage must be housed within secure approved location(s) in Canada
   c. 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. No data in transit will be saved or stored between the starting and end-point.
3. The email solution must contain access controls and/or monitors on data repositories and other computer systems, such that SSC may, at its discretion, restrict, monitor, and/or audit access to the government's data
4. No limitation of liability in the event of a security or privacy breach

Key Requirements

TECHNOLOGY PLATFORM REQUIREMENTS

1. **OPEN STANDARDS SUPPORT –** The service must be compliant with industry standards using open, non-proprietary standard interfaces.

2. **LEGACY SYSTEM INTEGRATION TOOLKIT –** The service must provide an integration toolkit for partners to leverage in order to integrate their business applications into the new email service.

3. **ACCESS MANAGEMENT –** The service must manage user profiles, credentials, authentication, and authorization.

Key Requirements

IMPLEMENTATION AND MIGRATION REQUIREMENTS

1. **EMAIL MIGRATION –** Existing email content/data must be migrated to the new service, including file attachments.

2. **SMOOTH TRANSITION –** Existing functionality must be in place during the transition wherever possible. Minimal impacts to users are expected. Minimal training will be required.

IT SERVICE MANAGEMENT REQUIREMENTS

1. **SSC IT SERVICE MANAGEMENT INTEGRATION –** The vendor will be expected to integrate with the IT Service Management processes and tools of SSC and its Partners. The level of integration may vary depending on service delivery sourcing option.

Areas we need your input…

1. Email Service Delivery options and considerations?
2. Email Application Platform options? How can GC leverage Government Furnished Equipment (GFE)?
3. Alternatives for the underlying Infrastructure Services?
4. Options for a user friendly identity, credential and access management?
5. Strategies to meet the security requirements of Secret email and the GC's requirements for data sovereignty?
6. Minimizing costs, complexity and business impacts for:
   I. Data Migration?
   II. Application Integration?
   III. User Training?
7. Emerging technologies? Lessons Learned? Case Studies?

Communications Security Establishment Canada

Cyber and Supply Threats to the GC

Carey Frey
Director of the Strategic Relationships Office

Cyber and Supply Chain Threats to the GC

E-mail Transformation Initiative
Industry Day

June 12, 2012

Carey Frey, Communications Security Establishment Canada

Canada

CSEC: What We Do

- CSEC: Canada's national cryptologic agency
- Our Mandate
  - Signals Intelligence
  - IT Security
  - Support to Lawful Access
- 'B' Mandate
  - To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada.

CSEC: IT Security Program

- We help prevent, detect and defend against IT security threats and vulnerabilities.
- CSEC provides unique technical expertise, capabilities and classified information that we use to complement commercial security technologies available to IT security practitioners.
- We use our own methods and operations to detect and defend against threats that are not in the public domain.

Effects of Market Forces on Technology

- Market forces favour commercial and personal technologies over requirements for security features
- Our society is almost totally dependent on software and hardware commercial technology providers from global markets
- New products and new versions of products are rapidly produced
- No regulatory framework exists for hardware/software safety and security
- Traditional government policies and processes impose security requirements after products and systems have been developed
- Few incentives for commercial technology developers to invest in security

Technology Vulnerabilities

- "People write software sloppily. Nobody checks it for mistakes before it gets sold"
  - Peiter Zatko (Mudge), WhiteHouse Cyber-Security Summit (2000)
- Unintentional vulnerabilities or weaknesses
  - Design flaws
  - Implementation errors
- Cyber Threat – A threat actor, using the Internet, takes advantage of a known vulnerability in a product for the purpose of exploiting a network and the information the network carries
- Intentional vulnerabilities or weaknesses
  - Predetermined deliverables can be implanted in a product with or without knowledge of company
- Supply Chain Threat – a product can be easily tampered with in the supply chain to later facilitate a cyber-intrusion against that product in order to exploit a network and the information the network carries

The Evolving Cyber-Threat

- Only a few years ago the situation was very different
- Today, cyber-attacks occur daily against Canada and our closest allies
- Threat actors range in sophistication from malfeasant hackers to organized crime groups, to terrorists to nation states
- Canadians trust the GC to defend Canada's cyber sovereignty and protect and advance our national security and economic interests

An Issue of National Security

- Risks from vulnerable technologies
  - Persistent, covert access by cyber threat actors to GC e-mail systems threatens the sovereignty of GC information and the integrity of government operations
  - Cyber threat actors are effective at exploiting both e-mail technologies and human behaviours through the use of e-mail systems

- Risks from complexity
  - Consolidation of the GC e-mail systems are a prerequisite for manageable cyber protection & defence
  - Security through obscurity is not a viable long-term strategy to deter cyber threat actors

- Risks from the supply chain
  - Increases opportunities for threat actors to compromise systems that have been hardened against cyber-intrusions
  - More difficult for the GC to detect and remediate

Counterfeit Cisco Equipment **

- An FBI investigation resulted in the discovery of 3500 counterfeit Cisco components in networks of US military agencies, military contractors and electric power companies
- "…a number of industry executives and technologists said that the threat of secretly added circuitry intended to subvert computer and network gear is real."
- Counterfeit equipment is sold over the Internet and then resold to government as legitimate equipment at the full price
- Government procurement processes which use layers of contractors and subcontractors adds to the problem

** New York Times (May 9, 2008)

US Military Bans Disks, USB Drives **

- A virus called Agent.btz spread by copying itself to thumb drives and other removable computer media
- The most significant incident ever acknowledged by the Pentagon
- “Someone was able to get past the firewalls and encryption devices of the US military and sit there for days…they could read documents…the could interfere with things”
- “(Jim) Lewis believes it was done by foreign spies who left corrupted thumbnail drives…around…in places where…personnel were likely to pick them up.”

** 60 Minutes (Nov 8, 2009)

GC Shared Services Procurements

- Shared Services Canada, CSEC & PWGSC are working in partnership to mitigate the risks to the GC from cyber threats & global supply chain vulnerabilities.

- CSEC will provide follow-up briefings on supply chain risk mitigation to interested suppliers for GC shared services.
  - Companies must be willing to sign a CSEC non-disclosure agreement to receive this information

- Security requirements for cyber-protection, cyber-defence and supply chain risk mitigation must be met by suppliers in order to successfully bid on GC shared services initiatives.
  - As the IT Security authority for the GC, CSEC will seek long-term partnerships with successful suppliers.

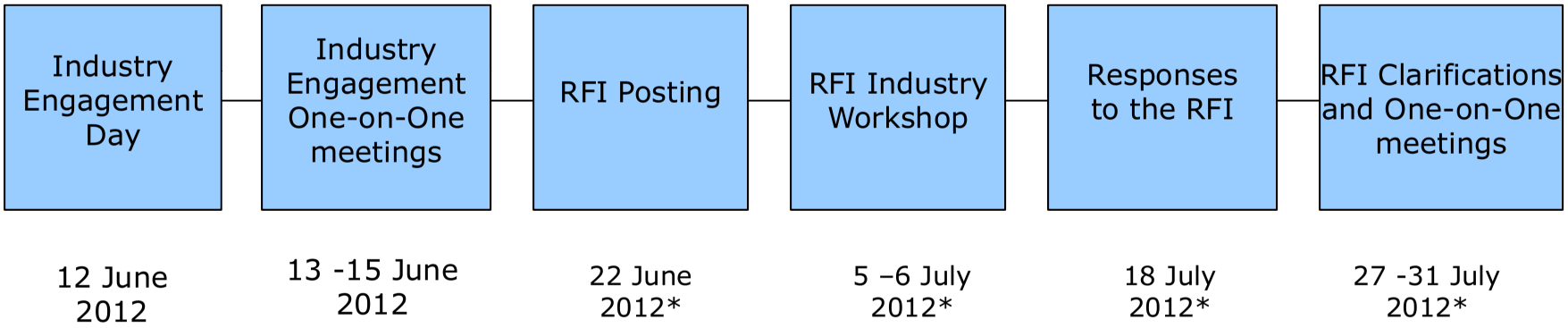
- Examples of these requirements can be found on CSEC's website under Technology Supply Chain Guidance.

Email Transformation Initiative

Procurement Approach

Normand Masse,
Director General,
Services and Technology
Acquisition Management Sector

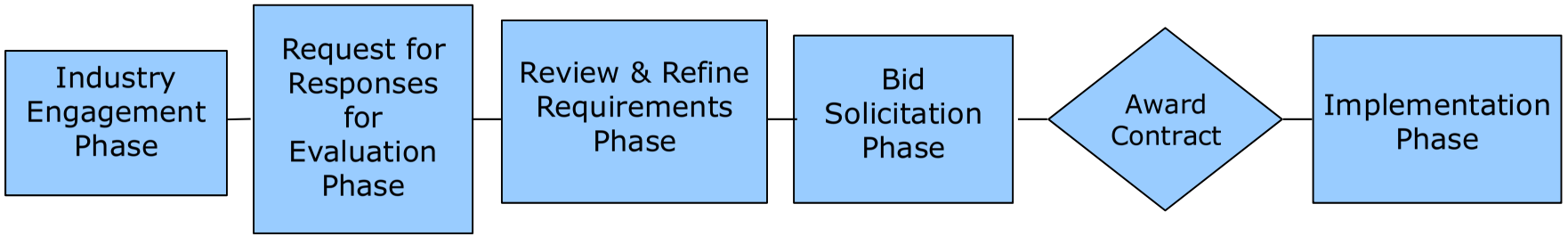
Industry Engagement Phase



*Dates are tentative

Procurement Approach

Collaborative Procurement Solution (CPS)



Request for Response for Evaluation (RFRE)

- Identify respondents to advance to the Review and Refine Requirements phase
- RFRE evaluation could be based on:
  - Capability and experience to deliver email services in a secure and timely manner
  - Financial Viability
  - Security clearance
- Your input on these elements will be sought during the RFI portion of the engagement phase

Review and Refine Requirements

- Successful respondents from the RFRE will work jointly with Canada to review and finalize the technical and solicitation requirements
- The successful respondents may be asked to demonstrate how their solution will meet specific requirements
- The results will be used to finalize the formal Request for Proposal (RFP) document

Bid Solicitation

- Formal RFP issued to the successful respondents that have completed the Review and Refine Requirements phase
- Each successful respondent to formally respond to the full set of requirements
- Canada will conduct a comprehensive evaluation and select the proposal which provides the best value to Canada

Contract Award and Implementation

- Contract Award
- Implementation / migration period estimated at 18 to 24 months
- The new solution is expected to be fully in-service by the end of March 2015


Canada

Shared Services Canada
Transformation Office

Unclassified

Industry Engagement Day Summary Report
Email Transformation Initiative

June 29, 2012
Version 2.0 (Final)

Shared Services Canada
Services partagés Canada

Canada

Table of Contents

1. INDUSTRY ENGAGEMENT DAY SUMMARY 1
2. ONE-ON-ONE SESSIONS 2
3. NEXT STEPS 2
ANNEX A – INDUSTRY ENGAGEMENT DAY, INDUSTRY ATTENDEES 3
ANNEX B - QUESTIONS AND ANSWERS 7
ANNEX C – AGENDA 16
ANNEX D – PRESENTATION 17

1. Industry Engagement Day Summary

Shared Services Canada (SSC) held the Email Transformation Initiative (ETI) Industry Engagement Day session on June 12, 2012 in Gatineau. In attendance were a total of 82 firms/associations, as well as government representatives, for a total of 166 attendees, with a few joining via videoconference from Vancouver, Edmonton and Halifax. A full listing of industry attendees is available in Annex A.

The session was moderated by Jérôme Thauvette who opened by explaining that the objectives of the session were to inform and seek feedback from industry on the Email Transformation Initiative. He then introduced Mme Liseanne Forand, President of Shared Services Canada, who welcomed everyone and explained that modern technology management is no longer just about the technology. Our goal at Shared Services Canada is to demonstrate that we can effectively deliver and manage the digital foundation on which the Government of Canada (GC) can rely on to deliver its programs and services to Canadians. SSC is aiming for efficiency and best value but the organization is also focused on sustainability over the long-term. Industry Engagement Day is about challenging ourselves; about asking the right questions which will lead us to the right solutions. It's about how we can decide to take calculated risks to be leaders in defining ground-breaking solutions. It's about uniting our strengths to position ourselves to respond to both the current and future needs of Canadians.

Mme Forand was followed by Mr. Tom Ring, Assistant Deputy Minister, Acquisitions Branch (AB), Public Works and Government Services Canada (PWGSC), who shared with the audience the procurement principles for the Email Transformation Initiative. First, he mentioned that SSC will engage industry stakeholders. SSC and PWGSC want to hear from industry in order to collectively consider industry's expertise for identifying the "best-fit" solution while promoting IT innovation for the Canadian economy. The second principle is the way we intend to govern the process to ensure a fair result. An important element of these efforts is the establishment of a clear governance structure consisting of an interdepartmental committee of Assistant Deputy Ministers to provide an oversight function and a key decision making body to achieve results in a manner that enhances access, competition and fairness. The third and last principle is the use of third-party experts. Multiple layers of oversight, and full transparency and engagement with suppliers at every step of the process will ensure that when people look back at the entire ETI process, they will discover how it embodied all three principles.

Following these opening remarks, the speakers / panellists presented the Industry Engagement Day material. The session then ended with an open forum and discussion, the results of which are attached in Annex B.

2. One-on-One Sessions

A high-level summary of the Industry Engagement One-on-One sessions will be published separately at a later date.

3. Next Steps

A Request for Information (RFI) was posted on MERX on June 22, 2012 to allow the Government of Canada to obtain further information in order help shape and define the Email Transformation Initiative strategy.

Annex A – Industry Engagement Day, Industry Attendees

	Company Name	Representative 1	Representative 2
1	1597705 Ontario Inc	Dan Murphy	N/A
2	Accenture Canada	Blair House	Adnan Moten
3	AdecoTech Inc	Jeff Thoms	Sean Griffin
4	Advanced Micro Devices	Lucille De Haitre	N/A
5	aTrust Inc.	John Davey	N/A
6	Avnet Technology Solutions	Victoria Gladwish	N/A
7	Bell Canada	Joanne Hanlon	Ian Ford
8	Blueprint Inc.	Jeff Braybrook	N/A
9	Buchanan Associates	Tim Huitema	N/A
10	CA Canada Company	Brent Kirwan	Robert Chikarians
11	Canadian Information Technology Providers Association (CITPA)	Herman Yeh	Tony Carlson
12	Canadian National Institute for the Blind	Christine Robbins	N/A
13	Ceryx Inc	Elia Stathopoulos	N/A
14	CFN Consultants	George Butts	N/A
15	CGI	Alain Brisson	N/A
16	Chamberlain Consulting	Sharon Chamberlain	Tony Baldock
17	Cisco Systems Canada Co	Douglas Vannest	Luigina Polidori
18	CommVault Systems	Tim Dooley	N/A
19	Computer Generated Solutions Canada Ltd (CGS Canada Ltd)	Corey Stephen	Jeff Goreski
20	Coradix	Tony Carmanico	N/A
21	Dell Canada Inc	Mike McDonald	Angelo Gatto
22	Deloitte Inc	Michelle Schulte	N/A
23	Donna Cona	Dave Gelineau	N/A

	Company Name	Representative 1	Representative 2
24	Eagle	David O'Brien	Cheryl Gingras
25	EMC	Paul Katigbak	Peter Alexiou
26	Entrust Limited	Paul McBride	Mark Joynes
27	Forrester Research	Blake Carruthers	N/A
28	Fujitsu Consulting (Canada) Inc.	Francois Le May	Denys Rivard
29	GJH Strategies	Gordon Hunter	Jessica Poulin
30	Global Knowledge Training LLC	Anne Crupi	Shannon Buchanan
31	Global Relay Communications Inc.	Chelsea Chase	Warren Roy
32	Google Inc	James Lambe	N/A
33	Hewlett-Packard (Canada) Co. (HP)	Jim Garnier	Arnold Liwanag
34	Hitachi Data Systems	Michel Gagnon	Stephen Brown
35	Hypertec Systems inc	James Chabot	N/A
36	IBM Canada Ltd	Ryan Wires	Louis-Paul Normand
37	Information Technology Association of Canada (ITAC)	Cindy Baker	N/A
38	Infosys Ltd.	Dominika Wrona	Shabbir Mahesri
39	Insight Canada Inc	Garry Brunet	Gord Rudko
40	Integra Networks Corp.	Joseph Colvey	Rami Courtemanche
41	IT Services Canada Inc. (operating as NATTIQ)	Robert Stanton	N/A
42	IT/NET Ottawa Inc.	Andrew Brewin	Lynne Leier
43	Itergy International Inc.	Jean Poirier	N/A
44	Kanatek Technologies Inc	Angie Mohr	N/A
45	Manpower Services Canada Ltd. d/b/a Experis, ManpowerGroup	Christina Daly	Tracy Wuest
46	Maplesoft Group co	Jocelyn Legault	N/A
47	MarketWorks Ltd	Kelly Hutchinson	N/A
48	Mcafee	Paul Tanasi	N/A

	Company Name	Representative 1	Representative 2
49	Messa Computing Inc	Cathy McCallion	N/A
50	Messaging Architects Inc	Martin Dupuis	Charles Nguyen
51	MGIS inc	Matt Page	N/A
52	Microsoft	John Bradley	Jamie Hart
53	Mocana Corporation	Sandeep Gupta	N/A
54	Modis Canada Inc.	Michel Plouffe	Pat Dunnigan
55	NetApp	Andrew Acheson	Carmine Caloia
56	Nisha Technologies	Daya Elangange	N/A
57	Novell Canada Ltd.	Victor Blanchette	N/A
58	Phirelight Security Solutions	Doug Kirkpatrick	Chris Dodunski
59	PricewaterhouseCoopers LLP	Ellen Corkery-Dooher	Roger de Montfort
60	Proofpoint Inc	Micah San Antonio	N/A
61	PureLogic IT Solutions Inc.	Coreen Bouchard	N/A
62	Quest Software	Marcel Lavoie	Alvaro Vitta
63	Research In Motion Limited	Nick Dawson	N/A
64	S.I. Systems	Eric Brown	N/A
65	Scalar Decisions Inc	Peter Ellis	Fiona Griffiths
66	Secure Technologies	Bob Pjontek	N/A
67	Softchoice Corporation	Rob Fearon	Janice Rakowski
68	SOMOS Consulting Group	Britton Knight	Adam Jasek
69	Spearhead Management Canada Ltd	Sue Laycock	N/A
70	Symantec Corporation	Alex Payne	Ian Shaw
71	TEK Systems Canada	Kyler Crawford	N/A
72	TELUS Communications Company	Kathy Moore	Matthew Toal
73	TeraMach Technologies Inc.	Raymond Hession	John Wong
74	The Capital Hill Group	Frank Drouin	N/A

	Company Name	Representative 1	Representative 2
75	The Devon Group Ltd	David Watts	Perry Henningsen
76	TITUS Inc.	Stephane Charbonneau	Trevor Rothwell
77	TPG Technology Consulting Ltd	Donald R. Powell	Phil McDonald
78	Turtlehawk Solutions	Craig Workman	John Moore
79	Unisys Canada	Louise Dunne	N/A
80	VanceInfo Creative Software Technology Ltd	Wei Shen	N/A
81	VMware Canada	Byron Driscoll	Pam Turenne
82	Zylog Systems (Ottawa) Ltd	Guylaine Ure	Dennis Martel

Annex B - Questions and Answers

Q1: Single Sign-On (SSO)

If going to single email architecture, are we going to need SSO where government manages the passwords on LDAP (Lightweight Directory Access Protocol) or use SAML (Security Assertion Markup Language) for authentication purposes? Do you expect the vendor to provide feedback?

Answer: Gail Eagen

Our goal is to eventually have SSO for the 43 SSC departments. Desktop and password management is shared between departments and SSC. We would want to have the user's identity confirmed through one directory and have it linked to our internal directories; it would probably have to be a federated model. We will seek feedback from industry on this and will work with TBS on this.

Q2: Email Directory

Regarding Email Directory – Aside from SSO, are you assuming that when we move to the consolidated system, you would federate the directories? Do you want a single email directory?

Answer: Benoît Long

Single sign-on is not in scope of the project (to merge / consolidate all email directories) however, there is a desire to go to a simplified, single directory. If we move to a single directory, it will likely be federated and trusted with other departments. We are familiar with standards like SAML. To summarize, yes we would like to have a single email directory, and we are looking for insights from industry on the best way to proceed.

Q3: Foreign Firms

Is this bid open to a foreign firm or do we need to be established in Canada?

Answer: Normand Masse

The Crown has not yet defined or imposed any restrictions on our requirements as we want feedback from industry on different ways we could proceed. That being said, there is a security aspect to protect data and data flow, therefore we must contemplate different ways. The goal is to keep the competition as broad as possible, however we still need to protect the data and information. SSC may end up having some restrictions however they are not defined yet.

Q4: Green Services

Green services are of interest to Canadians broadly. Is there a requirement for the GC to have green data centres?

Answer: Benoît Long

The Government has established a number of Green IT standards, and we have not gone down the list for Green requirements yet, however we could be asking that the solution meet some GC standards and policies. My guess would be that we will ask, however I can't specify at this time.

Normand Masse: There is a green procurement policy that we must always consider.

Q5: Scope, and Data

In your current state data we did not see any information about the size of the data. Is this information available? That will allow the vendor to gauge if the two year period is adequate.

Answer: Gail Eagen

We've completed a current state analysis and estimate it to be in the three petabytes (3PB) range for mailbox sizes across the 43 Partner departments and agencies. This includes offline and online storage.

Q6: Mobile Device Support

You mentioned that there will be several mobile devices in the system. Will government regulate and control these devices at a departmental level or will it be an employee device?

Answer: Gail Eagen

Currently, the government controls the mobile devices used by employees. Although in the future it could change, however we would always have to be compliant with our security requirements.

Q7: Mobile Device Application Support

Are the applications currently running on the mobile devices for email only or are there some additional applications?

Answer: Gail Eagen

Currently departments run other applications on mobile devices and ETI needs to respect this usage and incorporate this into our business requirement.

Benoît Long: The mandate of SSC is email, data centre, and network, and any evolution of allowing employees to integrate other applications on their own devices is not within our accountability. Our focus today is on email.

Q8: Options

Hybrid model vs. outsourced model, for your managed service option there is an underlying technology stack and environment such as software vendor, distributors etc. How will SSC deal with the various supply chains in either model?

Answer: Benoît Long

We are leaving the options open and we are open to any and all suggestions. We don't want to reinvent companies and vendors coming together and we don't want to prevent vendors from coming together and presenting a solution. We have left our options open on what can be done and we want you to advise the GC. This project will be done on a national scale and we are hoping to tap into the smartest ideas that come forward. We are looking at solutions and platforms as well. The Government has multiple goals and values, including cost savings. The way the work actually gets done, the stages for the solution and the services, and how the puzzle is put together, this is how you can make a difference and help us shape this. Our goal is to move as quickly as possible.

Normand Masse: We are open to your suggestions, especially during the one-on-ones.

Q9: Deployment Models

In terms of the options, you seem to exclude options for in-sourcing? Has there been a decision made?

Answer: Benoît Long

No decision has been made to-date. SSC has consulted industry, and we are looking at different vendor partnerships / solutions. There is no fixed model that exists or pre-existed. It is SSC's desire to engage all parts of the ICT sector to encourage open dialogue with Industry for ideas. SSC is interested in learning about the right mix or right blend to create the most value for tax payers.

Q10: Managed Service

The managed service portion slide mentions that the vendor will design, build and operate. In the industry, the design, build and operate phases could be done by separate vendors. If you are looking for a single contract that would provide all three services, this would be limiting the number of companies. Can you please comment?

Answer: Benoît Long

No decision has been made on contracts and number of contracts. We mentioned that we see managed service options as a "continuum"; help us shape and group certain things together, keeping in mind the goal of our timeline. SSC needs to evaluate how we are going to get to our decisions and meet our objectives of stability in operations and a transformed service. We need to figure out how we are going to deliver these benefits. Do not assume that the GC has made any decisions. We want to listen to good ideas.

Q11: Data sovereignty, Limitation of Liability

Under data sovereignty you have a requirement for unlimited liability. Can you please explain?

Answer: Normand Masse

The goal is to ask suppliers to fully indemnify with the Crown for security and privacy breaches. So we focus on these breaches of information as an important factor for us to protect the data. We want to hear how you would ensure the necessary security and privacy levels and what you would consider to be reasonable liability.

Q12: Limitation of Liability

Question: How would that play on Government Policy on Limitation on Liability? Is it the same?

Answer: Norman Masse

They are not the same. We can ask for limitation of liability or we can stay silent. In the end, it depends on the risk position of the GC and SSC.

Benoît Long: We chose these words. The role we play is to consolidate infrastructure including data. Since we are aggregating data, our requirements are greater. A breach in an infrastructure that is consolidated will be considered extremely significant, and that is why we need to look at limitation of liability as it relates to privacy and security. The statement was included to give the vendor guidance and to receive their feedback. We all need to be clear on what we are trying to accomplish, and ensure that the data is safe and secure.

Q13: Scope of Project

The question is on functionality. You are excluding the collaboration/unified communications in your scope statement. Is there an expectation to integrate with existing collaboration/unified communication tools already in use in the GC? How will the existing application integration come into play and what would be the expectation?

Answer: Benoît Long

Our mandate is clear, and the rationale of scope language for the project is focused on email messaging. What is sufficient to include in the scope is the benefits and value from consolidation of the email service. We expect the new email service to inter-operate with Unified Communications, Record Management, collaboration tools, etc. The idea is to maintain the scope on something we know very well. Our mandate is email, and SSC realizes that the evolution of the new email service will have to be future-proof and future ready circa 2015, 2020. The goal is not to expand beyond our mandate.

Gail Eagen: According to our preliminary current state information, there are approximately 2300 applications in our 43 departments that will need to be integrated into the new email service. We are now looking at how complex the integration is going to be. The responsibility of changing and integrating the applications will be the departments'. We want guidance on interfaces for the departments. What has been done before? We need industry's input on this.

Q14: Identity, Credential, and Access Management

Question: ICAM

What are your views on identify, credential and access management?

Answer: Benoît Long

We do have some departments that already have single sign-on. However, within SSC, there is a big diversity between what is currently provided. The goal is to provide a version of a single sign-on and to put a solution in place without increasing the complexity of sign-on. We want it to be easy and accessible for users. We are looking forward to your ideas on this topic.

Q15: Identity Management

Regarding Identity Management, can you be more specific? Are you talking about single sign-on or controlling the life cycle?

Answer: Gail Eagen

In the long term, we want to have single sign-on and full control of the life cycle. We are working with TBS on identity management, however in short term, we need to get suggestions on how to deal with ICAM. Short term solutions will be different than long term solutions.

Q16: SLA/SLO

Do you have SLOs/SLAs in place?

Answer: Gail Eagen

This will be ongoing during the migration, and the objective is to minimally impact and disrupt users during the migration. SSC will keep some systems running simultaneously during migration. We are looking for your input in this area to facilitate the future migration.

Benoît Long: SSC currently manages all email services for 43 Partner departments and agencies so execution of migration and implementation rests in our hands. There are migration questions we want to answer through the procurement process, and if you have experience in this area, we would really like to hear from you.

Q17: Requirements for the Other Mandated Projects

1) Can you elaborate on sister projects or will there be follow-ups to this program?
2) You have identified your requirements, however are there constraints of what must be met?

Answer: Benoît Long

Our strategic mandate is to transform email, data center, and networks and they are all inter-related. We are now looking into data centers in more detail and there is a strategic 'plan for the plan' being worked on. By the time the email transformation and transition is ready, the data centre project will have a detailed plan ready. These plans can also change and will be impacted based on how we will implement email. The transformation of data centers and networks will take longer. However this does not prevent or change the requirements for the email project. If the recommended option is to move to a managed solution for email, then we will need to consider what is needed or not needed. The same applies if it is a fully outsourced solution.

We are currently upgrading the networks to ensure that they are interoperable and have network interconnectivity between the 43 SSC partner departments and agencies.

Normand Masse: Thus far, the development of the requirements has been broad and high-level, and this is done intentionally so we can have dialogue. The timeline for the initiative is important. As well, security is very important and we need to accomplish savings. We will build on the collaborative procurement solutions and keep the competition as broad as possible. We would like to get your feedback.

Q18: GFE Assets

Will SSC provide a list of inventory of GFE assets?

Answer: Jérôme Thauvette

We are working on providing you a comprehensive RFI, and within the document, more details pertaining to GFE will be provided.

Benoît Long: A more detailed current state of what we presented today will be presented and shared in the RFI.

Q19: Encrypted vs. Non-Encrypted

Regarding security, what's been inventoried for encrypted vs. non-encrypted?

Answer: Benoît Long

We will have a survey on this topic and we will provide you the answers as we progress on this journey. At this moment we don't have a clear number.

Carey Frey: CSEC's view is that there currently are no consistent standards for Secret email. The GC needs to define and address what we mean by secret email. The confidentiality requirements for secret email state that a message must be kept and archived for 20 years. More information regarding secret email is available on the CSEC website. The email solution that will be implemented will incorporate high assurance technologies and will need to comply with the security requirements. CSEC recommends how secret email and networking should be done on their website. The goal is to reduce threat exposure, through our networks but it is almost impossible to protect any data put on the Internet. This is a single concept, that will be available in 12-18 months.

Q20: User Profiles

Have you looked at user profiles on email users?

Answer: Benoît Long

There is work for WorkPlace 2.0 that has already been completed and we are hoping to leverage this work. We are also working with TBS CIOB on this topic. The work is underway however it has not been completed to-date. We are also looking forward to receiving your feedback on user profiles/user segmentation.

Q21: Question on terms and conditions, contract and workshops:

I want to go back to the Terms and Conditions. I realize that you are in early stages of your journey however these conditions are critical as it will impact on some companies' ability to respond. At the RFI stage, will there be more detail regarding the terms and conditions as well as the security conditions?

Answer: Jérôme Thauvette

Yes there will be more detail in the RFI.

Normand Masse: We also want feedback during the one-on-one sessions.

Carey Frey: Regarding the security requirements, CSEC has developed a document labeled NIST 800-63. We are also finalizing ITSG-33, which is our version of 800-63, and it will be provided to vendors who are interested in obtaining additional information. However the document will not be made publicly available. The Technology Supply Chain Document on CSEC's web site contains sample legal clauses that are becoming common in large scale deployments. ITSG-33 is currently in translation and will be supplied when available.

Q22: Contract Duration

What is the contract duration?

Answer: Normand Masse

Currently we are looking at implementation and contract terms for the email service SSC of five years, plus three, one-year options, so the potential of an 8 year contract. We are looking for your feedback on the duration.

Q23: RFI Workshop

Question: What will be the structure of the RFI Workshops?

Answer: Jérôme Thauvette

The RFI workshop session has yet to be developed. That being said, we will be looking at completing much of this work shortly.

Normand Masse: At the moment, we are looking at possibly hosting workshops in Toronto, Montreal and if there is interest, in Ottawa. SSC wants to be new and do things differently, therefore the organization is looking to potentially reaching those we don't normally reach.

Q24: Open Source Software

You mentioned that you have 3PB of data? Is it in one location or distributed? How do you deal with compliance requests today such as eDiscovery? What is your view on open source?

Answer: Benoît Long

Open source will definitely be considered. The current data and information is not stored in one location as it is distributed, and it is currently difficult to access information for eDiscovery purposes. We have email stored in Tier1 storage as opposed to Tier4. We are working on turning this into an enterprise environment and are looking at consolidating storage. We are hopeful that we will be able to change storage tiers by storing information in the right tier. Email is complex as it is really integrated into how people work and it is also the first transformation project we are deploying.

Annex C – Agenda

Time	Presenter	Description
1:30-1:35	Moderator	Industry Day Objectives
1:35 – 1:50	President, Shared Services Canada	Welcome
1:50 – 2:00	ADM, Acquisitions Branch, Public Works and Government Services Canada	Procurement Opening Remarks
2:00 – 3:00	Shared Services Canada: Senior Assistant Deputy Minister of Transformation, Service Strategy and Design Director General, Email Transformation	• Email Transformation Initiative Description and Objectives • Current State • Scope and Requirements • Solution Options being Considered
3:00 – 3:15	Break	
3:15 – 3:35	Communications Security Establishment Canada	Cyber and Supply Threats to the Government of Canada
3:35 – 3:50	Acquisitions Branch Public Works and Government Services Canada	• Industry Engagement • Overview of the Collaborative Procurement Solutions Approach
3:50 – 4:45	Questions and Answers	
4:45 – 5:00	Recap and Closing Remarks	

Event Moderator:

- Jérôme Thauvette

Event Speakers

- Liseanne Forand, President, Shared Services Canada
- Tom Ring, Assistant Deputy Minister, Acquisitions Branch, Public Works and Government Services Canada
- Benoît Long, Senior Assistant Deputy Minister, Transformation, Services Strategy and Design, Shared Services Canada
- Gail Eagen, Director General, Email Transformation Initiative, Shared Services Canada
- Carey Frey, Director of the Strategic Relationships Office, Communications Security Establishment Canada
- Normand Masse, Director General, Services and Technology Acquisition Management Sector, Public Works and Government Services Canada

Annex D – Presentation

Shared Services Canada | Services partagés Canada

Canada

Shared Services Canada
Transformation Office

Unclassified

Industry Engagement One-on-One Sessions Summary Report
Email Transformation Initiative

June 29, 2012
Version 2.0 (Final)

Shared Services Canada
Services partagés Canada

Canada

Please Note: This report contains Third Party information, and as a result, should the Crown receive an Access to Information and Privacy (ATIP) request, it would be required to seek consent from every vendor and industry association that engaged with the Crown during the Industry Engagement One-on-One Sessions.

Table of Contents

1. One-on-One Session 1
1.1 Event Logistics 1
1.2 One-on-One Session Participating Companies 1
1.3 One-on-One Session Outcomes 2
3. One on Feedback 5
4. Next Steps 5

1. One-on-One Session

Following Industry Engagement Day, which was held on June 12, 2012, a set of 45 minute one-on-one sessions, designed for vendors to provide additional feedback on the procurement process, scope and requirements presented on Industry Engagement Day were held. There was no fixed agenda for these sessions, which took place from June 13, 2012 to June 15, 2012, in the National Capital Region.

The sessions were split between two teams consisting of staff from the ETI, PWGSC's Acquisitions Branch and a Fairness Monitor, and each team was led by either, the Senior ADM of Transformation, Service Strategy and Design (TSSD), Benoît Long, or the Director General (DG) of ETI, Gail Eagen. Thirty-nine firms/associations attended the one-on-one sessions.

1.1 Event Logistics

The majority of the vendors and industry associations decided to participate and attend the Industry Engagement One-on-One sessions on location, at various Government of Canada locations in the National Region. However, some vendors elected to participant via videoconference or teleconference from locations such as Vancouver, Montreal, Toronto or Dartmouth.

1.2 One-on-One Session Participating Companies

The following companies participated in a one-on-one session:

1. Accenture Canada
2. Adeco Tech TBC
3. aTrust Inc.
4. Bell Canada
5. Buchanan Associates
6. CA Canada Company
7. Canadian Information Technology Providers Association (CITPA)
8. Ceryx Inc
9. CGI
10. Computer Generated Solutions Canada Ltd (CGS Canada Ltd)
11. Dell Canada
12. Deloitte Inc
13. Eagle
14. Entrust Limited

15. Forrester Research
16. Fujitsu Consulting (Canada) Inc.
17. Global Relay Communications Inc.
18. Google Inc
19. Hewlett-Packard (Canada) Co. (HP)
20. Hitachi Data Systems
21. IBM Canada Ltd
22. Infosys Ltd.
23. Itergy International Inc.
24. Messaging Architects Inc
25. Microsoft
26. Mocana Corporation
27. NetApp
28. Novell Canada Ltd.
29. Quest Software
30. Research In Motion Limited
31. Scalar Decisions Inc
32. Softchoice Corporation
33. Symantec Corporation
34. TELUS Communications Company
35. TeraMach Technologies Inc.
36. TITUS Inc.
37. TPG
38. Unisys Canada
39. VMware Canada

The vendors that participated in one-on-one sessions included, but were not limited to those specializing in the following areas:

- Security;
- Data migration;
- Solution providers;
- Software vendors; and,
- Solution integrators.

1.3 One-on-One Session Outcomes

Although the diversity of presentations and ensuing conversations ranged from session to session, the teams noted several reoccurring themes during the meetings. Presented below are twelve themes, not ranked in order of importance, that were discussed more frequently.

Theme	What we heard
1. Population Segmentation	• Investigate the opportunities associated with segmenting the user population (e.g. worker type) – there is an opportunity to simplify and save significant costs. • These requirements will aid the migration process, the long-term support model, and possibly even the technical solution (e.g. hybrid model).
2. Government Furnished Equipment	• How is GFE defined: Software licenses only? Servers? Storage? Network? Data Center? • How should GFE be described to the supplier community (e.g. optional vs. mandatory), and at what level of detail, and by when? • The terms and conditions for existing licenses need to be documented. A comprehensive GFE list is required.
3. Secret Email Support	• Vendors want a better definition of what constitutes a Secret solution – is a secret infrastructure (network) included? • Vendors also want more clarity on how the solution will be certified and accredited. • Vendors indicated that Secret will increase complexity and costs, and may impact timelines.
4. Change Management & Transitioning	• Several bidders emphasized the importance of change management, expectations management, communications planning, and overall logistics.
5. Information Management Challenges	• Numerous bidders warned of the challenges associated with an absence of IM policy in the areas of compliance, audit, retention, archiving, eDiscovery, mobility, and information classification.
6. ICAM and other horizontal services	• Numerous bidders warned of the need for a well thought-out ICAM strategy covering identity lifecycle management, on-boarding, password management, assurance levels, and authentication. • "ICAM is a bigger challenge than email". There is a need to define roles, responsibilities and supporting policy. • Vendors suggested that vendor selection criteria should be

	ICAM references. • It was suggested that one way forward would be to prescribe existing GC solutions (e.g. MyKey).
7. Service Delivery Domains	• Many of the smaller, "best of breed" vendors suggested that there are opportunities to split the program into discrete sub-areas to deliver better value. • Industry suggested that an "on premise, private cloud" option should be considered due to security and cost concerns. • Some vendors indicated that they would not be able to submit a proposal if the current Unlimited Liability clause remained. This clause could inhibit consortiums.
8. Migration	• Numerous bidders warned of the enormous challenges associated with all aspects of the migration, including how much data, how to find it, how to move it, tools required, duration, parallelism, encrypted content, and cleansing.
9. Current State Detail	• Many bidders emphasized the need to have an accurate AS-IS with close communications with the partner departments. Vendors would like more information from the GC on current state.
10. Data Sovereignty	• Some large cloud based providers indicated that they would not be able to bid if this requirement remains. • Vendors asked for a clarification on what constitutes a "Canadian Company".
11. Product	• Many vendors are assuming a Microsoft Exchange solution (although this was not a position expressed nor implied by SSC).
12. Platform Mobility	• Some companies asked what functionality and device platforms need to be supported.

3. One on Feedback

During the one-on-one sessions, all vendors and industry associations were invited to provide any additional information or clarification on their material that might help focus the Request for Information (RFI) questions and process.

4. Next Steps

An RFI was posted on MERX on June 22, 2012 to allow the Government of Canada (GC) to obtain further information in order help shape the ETI strategy.