Public Works and Government Services Canada

Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Title - Sujet
Financial Management Industry Day

Solicitation No. - N° de l'invitation	Date
24062-140079/A	2013-08-16
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
24062-140079	PW-$$XL-116-26311
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
116xl.24062-140079	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2013-08-30

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
Yang, Annie	116xl
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(819) 956-1560 ( )	(819) 953-3703

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

Specified Herein
Précisé dans les présentes

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

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

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

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

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

Signature **Date**

Issuing Office - Bureau de distribution
Shared Systems Division (XL)/Division des systèmes partagés (XL)
4C1, Place du Portage Phase III
11 Laurier St./11, rue Laurier
Gatineau
Québec
K1A 0S5

Canada

******AMENDMENT # 1******

To attach Industry Day decks presented on August 16, 2013.

Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Better government: with partners, for Canadians

Industry Engagement Day

Financial Management Applications Rationalization

August 16, 2013

Canada

Safe Harbour Statement

This presentation contains information regarding a strategy that the Government of Canada may choose to undertake

Information provided here is solely for the purposes of gathering further information to support the development of that strategy, and is subject to variations and uncertainties

Information and opinions presented here reflect our current knowledge and directions as of the date presented, and you are cautioned not to place undue reliance on this information

Industry Day Objective

Today's goal is to begin a process to transform the way in which the Government of Canada supports and delivers Financial Management (FM) Applications and Application Management Services.

We will endeavour today to inform and seek feedback from industry on a proposed Government of Canada Financial Management Applications Rationalization strategy.

Our objectives for our Industry Engagement phase include:

- Providing an overview of the initiative and its expected business outcomes
- Assessing the level of interest/capacity of industry to provide the GC with a modern FM IT applications platform
- Gather input on the potential application management service delivery options available
- Determine the key service elements and parameters that drive pricing and availability

Agenda

FM Applications Rationalization– Industry Engagement Day

Participant Registration : 8:00 am – 9:00 am

Overview	Wade Daley, Chief Technology Officer of the Government of Canada
FM Transformation	Patricia Sauvé-McCuan, Assistant Comptroller General, Financial Management Transformation, Office of the Comptroller General
Key Requirements and Procurement Approach	Wade Daley, Chief Technology Officer of the Government of Canada
Cyber & Supply Chain Threats to the GC	Communications Security Establishment Canada
Closing Remarks and Questions	Wade Daley, Chief Technology Officer of the Government of Canada

Business Drivers

*"…committed to **streamlining, consolidating and standardizing** administrative functions and operations within and across organizations."*

Budget 2012 and Economic Action Plan 2012, Government of Canada

*"…reducing duplication of effort, **streamlining our processes**, taking advantage of **new technologies**, and leveraging the Government of Canada's considerable purchasing power, we will improve our services, increase our productivity, and **reduce costs**."*

Twentieth Annual Report to the Prime Minister on the Public Service of Canada, 2013

Overall Project Objectives

The FM Applications Rationalization Project will standardize, consolidate, and modernize the Government of Canada's FM applications IT landscape to reduce costs, achieve efficiencies, and allow for greater mobility of the IT back office workforce

The GC is seeking to obtain the services of a private sector supplier of Managed Application Services to support GC FM application services based upon a yet to be developed GC configured instance of SAP ERP

Public Works and Government Services Canada will manage the new service delivery arrangement on behalf of the Government of Canada

Shared Services Canada will support the secure integration of this new service with the GC IT environment

Desired Business Outcomes

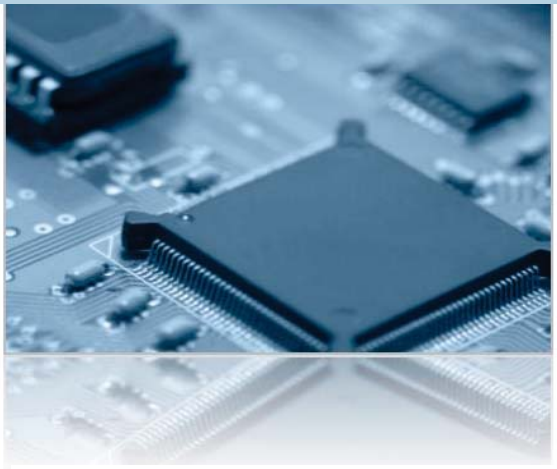
- Establishment of a consolidated FM IT applications platform for the Government of Canada
- Reduction of costs to deliver and renew and manage GC FM applications
- Evolution of the SAP platform to become part of a consistent technology landscape to enable the broader back-office improvements

The Approach

- One enterprise IT platform for the Financial Management (FM) System of the GC
- Procurement of an outsourced, managed IT Application Management Service (AMS) for the Financial Management application
- Departments to transition in waves from their legacy FM IT applications to the outsourced GC standard FM IT application
- IT platform to include infrastructure, application with configuration/customizations reflecting GC requirements, related applications maintenance and enhancement services
- GC retains business process service delivery and end user support
- GC FM IT Application will align and evolve with business design changes directed by the GC FM System Business Owner (OCG)

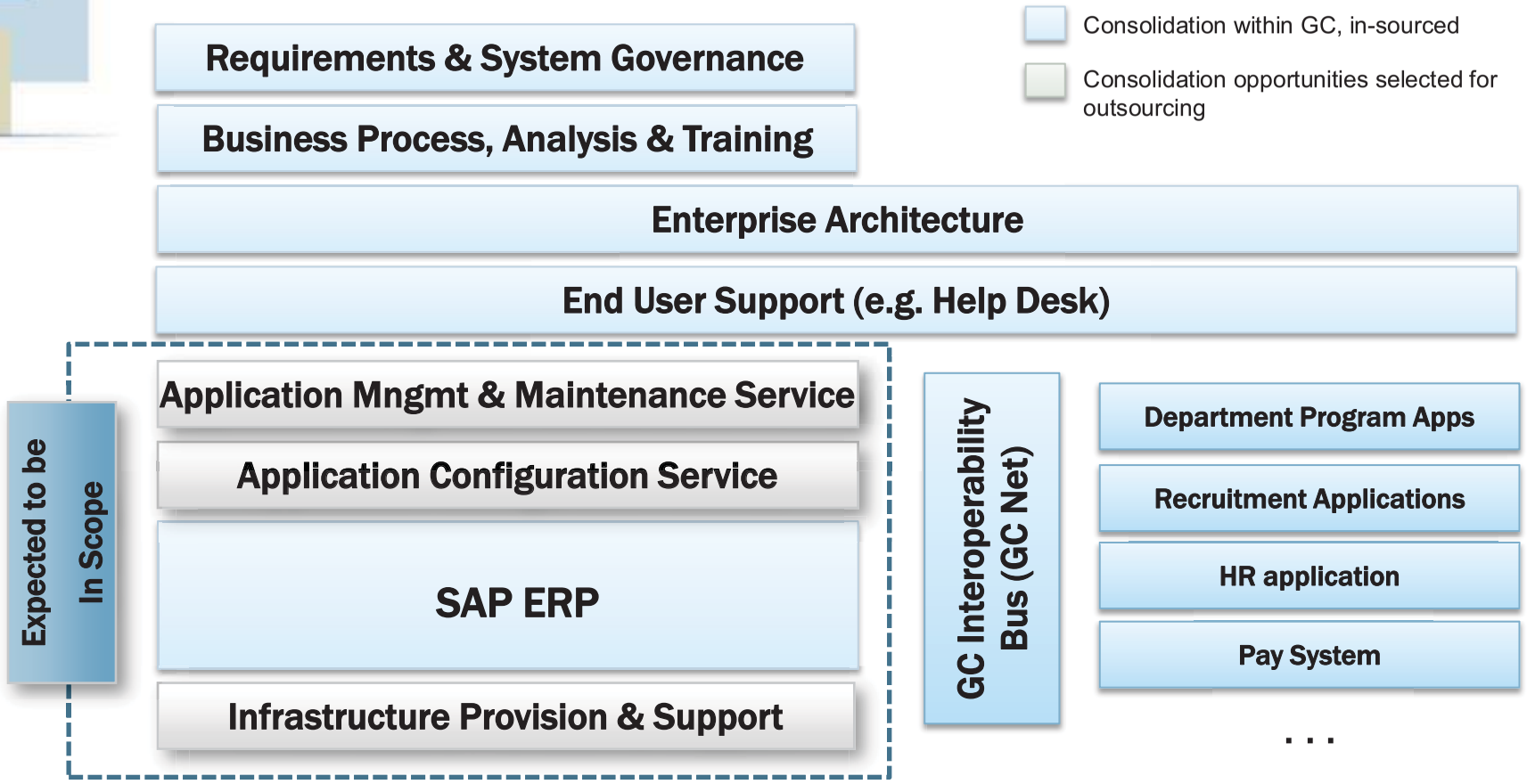
The GC will adopt a collaborative procurement solution similar to the recent Shared Services Canada Email Transformation Initiative and follow an approach of progressive, incremental outsourcing

FM Application Rationalization

One Enterprise Business Model	One Application	One Provider
		
Enterprise Business Needs Enterprise Processes Enterprise Data	OCG is leading an effort to create the GC solution for financial management. The first GC common version targeted for 2014.	Industry Day begins a process that will result in the selection of a single provider of application management services for GC.

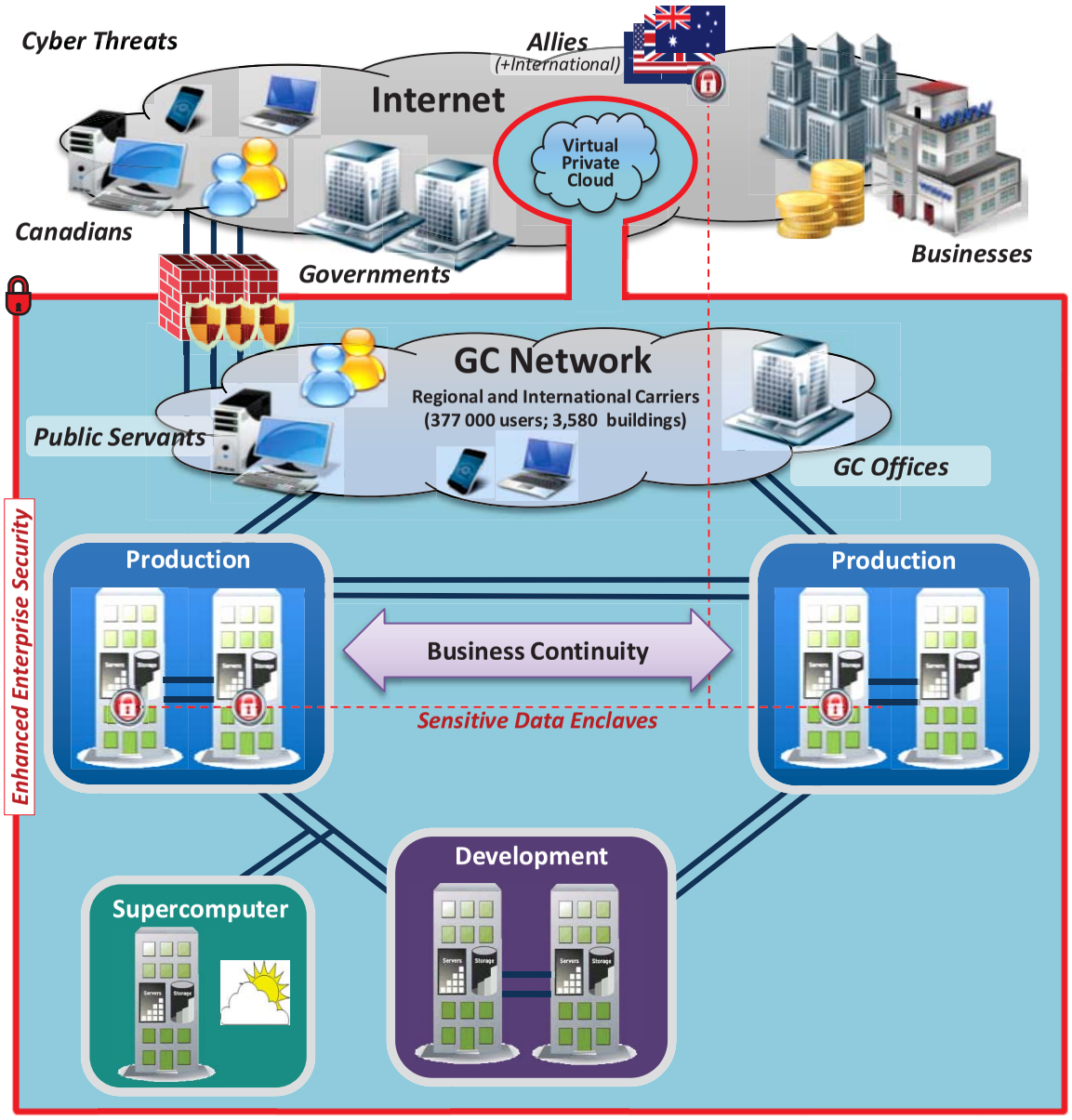
One Back Office

Desired Future State



- The solution will interoperate with other IT application domains through a future GC interoperability bus and future GCNet

GC IT Services Reference Architecture



Benefits of New Approach

- More timely convergence to a modern, standard GC FM IT application
- Departments will no longer have to fund individual upgrades and renewals of FM IT applications
- Leverages private sector more strategically to reduce upfront GC investment in new IT infrastructure
- Allows for departmental IT capacity to be focused on mission critical systems
- Less complex departments to benefit from enterprise grade platforms
- Complements SSC's 7-year transformation strategy
  - Opportunity to reduce migration workload to new Data Centers and infrastructure

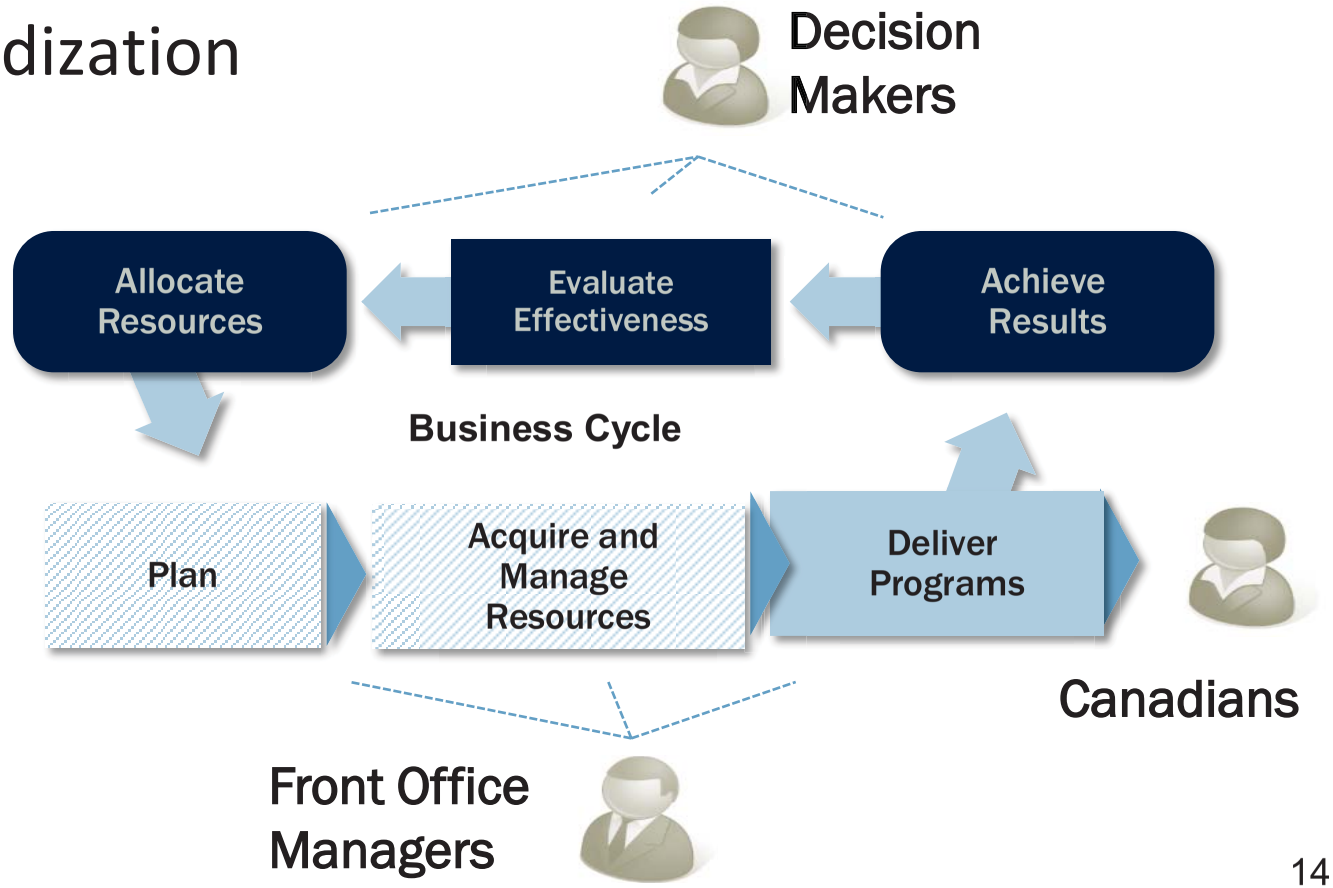
Moving more quickly to common IT systems for FM business functions may enable or assist in the more timely transformation of FM services

Financial Management Transformation

" To implement a streamlined, consolidated and integrated Enterprise Model for financial management in the Government of Canada"

FMT - Strategic Business Objectives

- Support for decision makers
- Efficiencies and economies
- Standardization



FMT - End State Benefits

- Better information for decision-making at both departmental and Government of Canada-wide level
- Effective, efficient and economical use of resources to achieve government objectives
- Financial Management System environment that is consolidated, standardized and provides greater value for money where functionality is optimized for business value
- Application management services are delivered in Government of Canada service model
- Favourable conditions to respond to evolving needs, adopt emerging practices and seize further opportunities for savings and/or service optimization

Current State: by the numbers

113+ Departments and agencies

377 Thousand self-service users

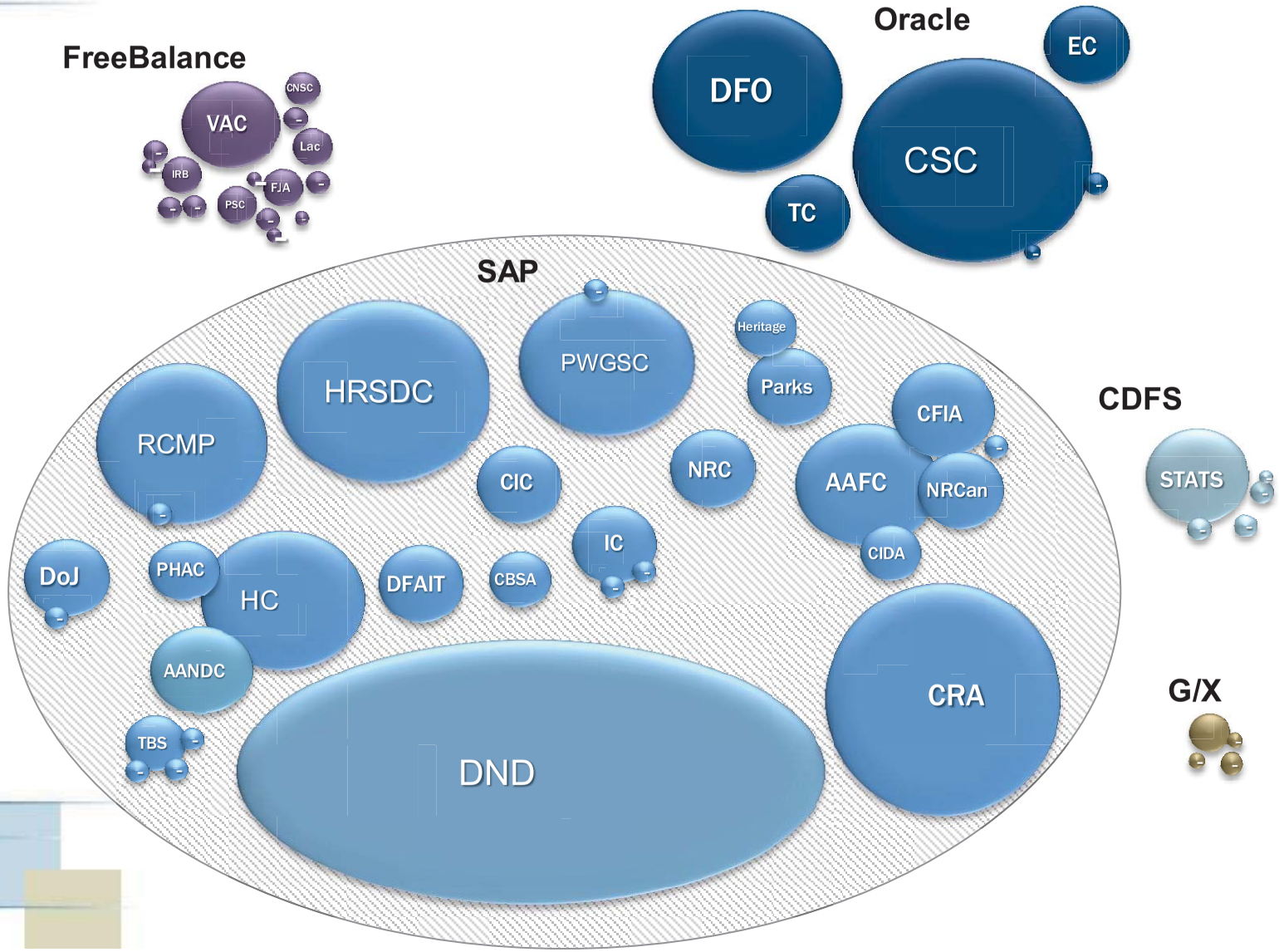
500+ Applications relating to financial management

Working in **1400** towns and cities throughout Canada

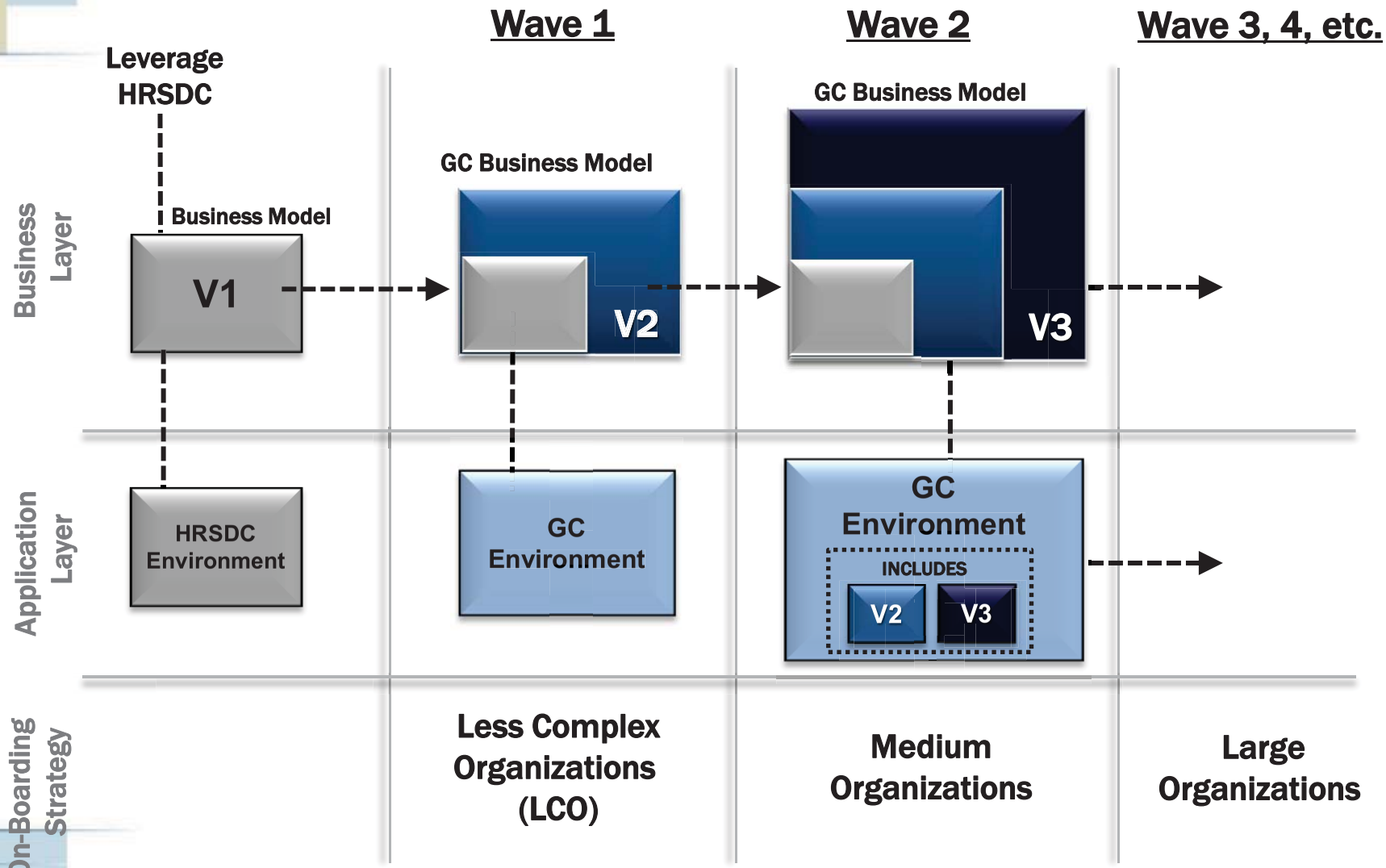
100's Of international locations

Indicative values: exact values will vary with time

Current State: Departmental Financial Management System Platforms



Modeled Approach toward GC Common Solution



Key Service Provider Requirements

Services

It is expected that the private sector supplier would provide the following services to the GC:

1. **APPLICATION MANAGEMENT & MAINTENANCE SERVICES:** May include;
   a. Application Maintenance: This comprises the support and management of the specific SAP business application functional modules implemented.
   b. AMS Problem Control and Resolution: Once the incident (e.g. Network access) is resolved, conducting in-depth analysis to identify the root of the incident to prevent future failures
   c. Capacity Management: Activity associated with reporting and controlling the systems usage and identifying areas of concern
   d. Performance Management: Activity associated with assessing the performance data for systems and business impact, continual monitoring of major and minor alarms to quickly rectify any server system problems

Key Service Provider Requirements

Services

e. Contract Service Level Management: Service level metrics provided to the service receiver; metrics generated periodically by business group, department or location

f. Security Management: The development and implementation of organizational processes that provide for the addition of new users, including granting these authorized users the right to use a set of services, or any particular service, and the deletion of employees leaving the enterprise or being assigned to new duties in the enterprise

g. Business Continuity Planning: Design, develop, and implement the Business Continuity Plan that provides recovery within the recovery time objective

h. On-Boarding Capacity Management: Services to monitor/influence the rate of on-boarding to the common application.

i. On-Boarding Program/Change Management Support: Review of and alignment to program change activities associated with on-boarding clients.

Key Service Provider Requirements

Services

2. **APPLICATION (SAP) CONFIGURATION SERVICES:** May include;
   a. Change Management: All activities and disciplines surrounding the change or implementation of a new software (SAP) release or service into the live environment including the evaluation, authorization (RFC), prioritization, planning (CAB) and testing, including provision of test environments as required for pre-production integration and interface testing by the GC
   b. Customization: Addition of functionality to the product that is not included in the base (configurable) installation of that SAP
   c. Maintain Configuration Information: Concerned with ensuring that only authorized and identifiable configuration items are accepted and recorded from receipt to disposal. It ensures that no Configuration Item (CI) is added, modified, replaced, or removed without appropriate controlling documentation
   d. Integration: Develop and maintain the functionality required to orchestrate processes and exchange data between multiple applications

Key Service Provider Requirements

Services

3. **INFRASTRUCTURE PROVISION AND SUPPORT:** High availability processing capabilities to meet the demands of the GC. May include;
   a. Asset Management: Procurement of products and the associated logistics to deploy product into common application
   b. Investigate and Diagnose: 2nd / 3rd line assessment of incidents transferred from Service Desk including further details, collection and analysis of all related information and resolution (including any workaround) or a route to on-line support
   c. Proactive Problem Management: The process of identifying, recording, appropriately communicating, resolving to client satisfaction, and reporting all issues regarding IT products and services that impact client operations
   d. Security Management: Sound processes to monitor the security of the infrastructure and proactively protect again security threats

Key Service Provider Requirements

Services

e. Monitor Infrastructure: The examination of the entire server infrastructure for automated alerts and other changes in the status of individual components from satisfactory to a status requiring attention, and the taking of specific actions to address these including initiating an incident or problem report with the Service Desk

f. Back-up and Archive Management: The execution and monitoring of backup and recovery procedures that are agreed to by the client

4. **SERVICE MATURITY:** Highly mature service delivery processes based upon industry standards and best practices

5. **ONBOARDING/MIGRATION:** Ability to onboard departments and agencies into the service provider's environment in an efficient and cost effective manner. Includes ability to rapidly provision infrastructure capacity on demand.

Key Service Provider Requirements

Services

6. **PARTICIPATION:**
   a. Participate in Architecture and Planning: the service provider will be required to attend meetings and/or to provide technical expertise as input into the development and planning of enterprise architecture relating to SAP services and how SAP interacts with other GC systems and platforms.
   b. Involvement in IT Policy and Practice Development: the service provider will be required to provide consultative input into the development and documentation of key policies and practices such as Data Management, Software License Management, Application Management, Service Level Requirements, Product Evaluation & Usability Testing, etc. in relation to SAP services

7. **INTEROPERABILITY:** The service must be compliant with industry standards using open, non-proprietary standard interfaces

Key Service Provider Requirements

Security

It is expected that the private sector supplier's service delivery will meet the following security requirements:

1. **SECURE:** The new FM Applications solution(s) must pass or exceed GC security requirements

2. **DEFENSE-IN-DEPTH:** The service must support layered security controls, such as:
    1. Perimeter security services (e.g. firewall)
    2. Protection from threats to data at rest (e.g. access control)
    3. Protection for data in motion (e.g. encryption)
    4. Security operations
    5. Security incident management
    6. Ongoing security assessment and monitoring

Key Service Provider Requirements

Security

3. **TRUSTED SUPPLY CHAIN:** Solution must be compliant to the GC Technology Supply Chain Guidelines (TSCG)

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

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 Access to Information Act

Key Service Provider Requirements

Data Sovereignty

It is expected that the private sector supplier's service delivery will meet the following data sovereignty requirements:

1. The application services, the data, and infrastructure of the solution will be established within the Geographic Boundaries of Canada under Canadian control
2. Government information is secured at all times, at rest and in motion, and is only accessed by those authorized to access the data
3. It must be recognized:
   a) Canada's right to order the destruction or deletion of data
   b) Compliance with the GC privacy and security policy instruments and practices, and recognition of the GC notification regarding privacy and security breaches
   c) It is mandatory that the data remain sovereign and not accessible (nor disclosed) to any other jurisdiction

Key Service Provider Requirements

Vendor Security Profile

It is expected that the private sector supplier will meet the following security profile requirements:

- GC will finalize the Vendor Security Profile requirements following the Industry Engagement phase
- Our objective is to provide as much time as possible for companies to arrange their security clearance
  - Please refer to: http://ssi-iss.tpsgc-pwgsc.gc.ca/questions/esosp-psos-eng.html
- Companies can expect that personnel participating in this process will be required to be security cleared to Secret
- Companies can expect that at the RFP stage, all bidders must satisfy all security requirements including facilities

National Security Exception

- Canada may invoke its rights under national and international trade agreements to use a National Security Exception (NSE) for this procurement

- An NSE allows Canada to remove a procurement from some or all of the obligations of the relevant trade agreement where Canada considers it necessary to do so in order to protect its national security or other related interests specified in the text of the national security exceptions

Source: *Investment, Project Management and Procurement Policy Division. Treasury Board Secretariat*
http://www.tbs-sct.gc.ca/cmp/doc/nse-esn/nse-esn-eng.asp

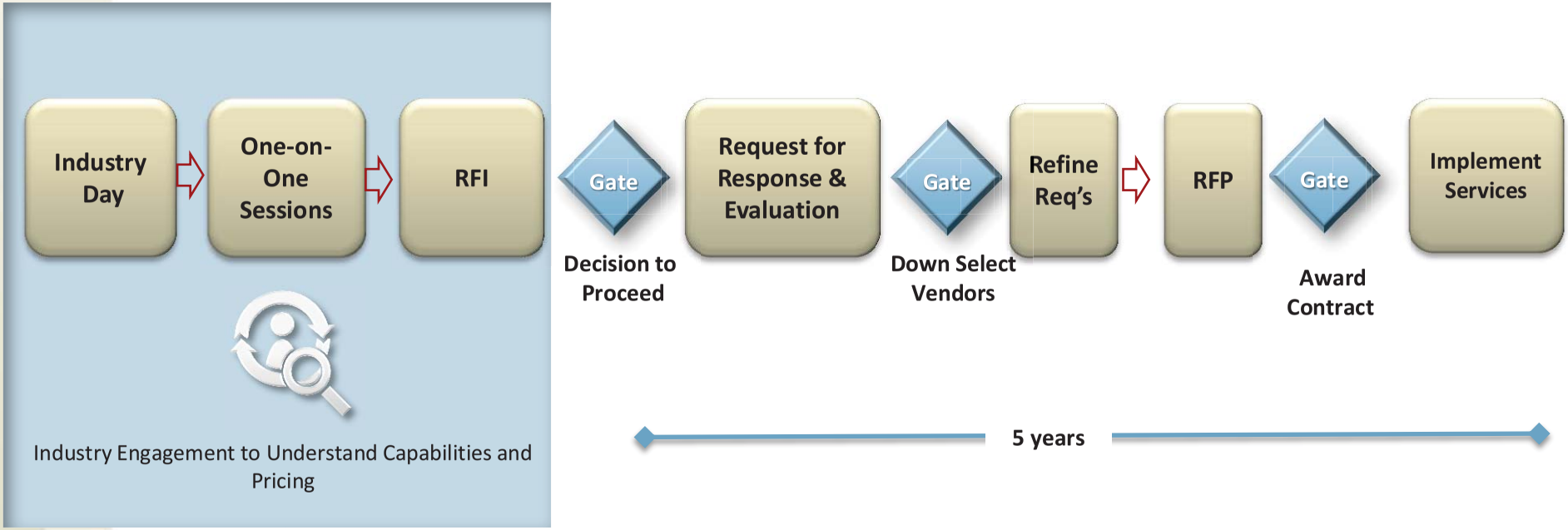
What is out of Scope?

It is expected that the GC will deliver and/or manage the following elements with participation of and/or consultation with the private sector supplier:

- Relationship Management with GC departments and agencies.
- Helpdesk: Tier one support
- Governance: Structures, membership, and terms of reference to make decisions for service delivery
- Business Analysis: Identifying the business needs of the enterprise and determining how these will be met in an integrated (minimally customized) SAP platform *(Please note: portions of the design work, especially SAP capability related, could be provided as a service to the GC)*
- Training: Training programs required to educate users
- Enterprise Architecture: The definition of standards in support of enterprise architecture
- Confirmation testing in a near production system
- Testing of SAP application interfaces with all departmental applications

Proposed Procurement Approach

Collaborative Procurement Solution



Current Industry Engagement Phase

One-on-One Sessions

- The one-one-one sessions will take place between August 19th and August 22nd. These will be 30 minutes per session and will take place in government offices. Instructions for registration contained within Industry Day Call Letter

  https://buyandsell.gc.ca/procurement-data/tender-notice/PW-XL-116-26120

- During the sessions you may present any information that you feel could help us scope this work to fit industry methods and capabilities towards achieving timely convergence to a GC SAP FM configuration.
- We need your input:
  - FM Applications services rationalization options, potential strategies and considerations
  - How can GC leverage Government Furnished Equipment (GFE)?
  - Minimizing costs, complexity and business impacts for:
    - FM application delivery, Data migration, Application integration and User training (to be done in-house)
  - Emerging technologies? Lessons Learned? Case studies?

Request for Information

The formal Request for Information is expected to be posted soon after the one-on-one sessions. Areas of interest for the GC include:

- Service characteristics that affect pricing and availability
- Service offerings and capabilities
- Indicative pricing for services
- Assist the GC in evolving the SAP solution from basic functions to full functionality while on-boarding rapidly
- Strategic considerations
- Vendor evaluation criteria to be used in the future Request for Response and Evaluation (RFRE) to pre-qualify vendors
- Evaluation criteria for a future Request for Proposal

Cyber & Supply Chain Threats to the GC

Questions/Clarifications?

Cyber & Supply Chain Threats to the GC

Financial Management IT Applications Rationalization Initiative Industry Day

Aug 16, 2013

Communications Security Establishment Canada

Canada

CSEC: What We Do

- CSEC: Canada's national cryptologic agency
- Our Mandate
  - Foreign 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

- Today, malicious cyber activities are directed against Canada and our closest allies on a daily basis
- 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**
  - Covert and persistent access by cyber threat actors in Canadian data centre / cloud infrastructures threatens the sovereignty of GC information and the continuity of government operations
  - Cyber threat actors are effective at exploiting enterprise technologies and management systems used to administer and operate data centre / cloud infrastructures

- **Risks from the supply chain**
  - Increases opportunities for threat actors to circumvent GC cyber security measures
  - More difficult for the GC to detect and remediate

GC Procurements

- CSEC is working in partnership with GC departments to eliminate or significantly reduce 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 consolidated initiatives
  - 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 consolidated initiatives
  - As the IT Security authority for the GC, CSEC will seek long-term partnerships with successful suppliers
  - CSEC will assist Treasury Board Secretariat of Canada (TBSC) and Public Works and Government Services Canada (PWGSC) in the pedigree analysis of supply chain information provided by respondents
- Examples of these requirements can be found on CSEC's website under Technology Supply Chain Guidance