



Service | Innovation | Value

Mainframe Supply Chain Renewal Industry Day Session

Data Centre Consolidation Program
Shared Services Canada (SSC)
Transformation Overview

Benoît Long
Senior Assistant Deputy Minister
Transformation, Service Strategy & Design
Shared Services Canada

September 30, 2014



Shared Services
Canada

Services partagés
Canada

Canada 

SSC Transformation Overview

Agenda

- Objective
- SSC Transformation Objectives and Purpose
- Transformation Timeline
- Target End State
- Business and Functional Requirements

SSC Transformation Overview

About the session with Industry

- **Context:**

- In preparation for its Supply Chain Renewal, Shared Services Canada wants to present an overview of its mainframe transformation strategy including the go-forward activities, the timelines and the challenges.

- **Objective:**

- The session's main objective is to seek input from Industry on mainframe transformation activities.
- Those who attend will be expected to propose responses to questions raised.



SSC Transformation Overview

Transformation Objectives

SAVINGS



Transformation will realize material cost savings and avoid future costs

SERVICE



Transformation will match service levels to partner priorities

SECURITY



Transformation will provision a secure environment to meet program needs

SSC Transformation Overview

Purpose of Transformation

SSC will transform the GC's aging IT infrastructure by delivering:

One Email Solution

Objective: Migrate the GC to a single, outsourced, secure email system

EMAIL

WORK-
PLACE
TECHNOLOGY
DEVICES

Consolidated procurement of end-user device hardware and software
Objective: Consolidate procurement of end-user devices & related software

A government-wide footprint of 7 data centres

Objective: Consolidate the GC's 485 data centres into 7 modern and efficient facilities

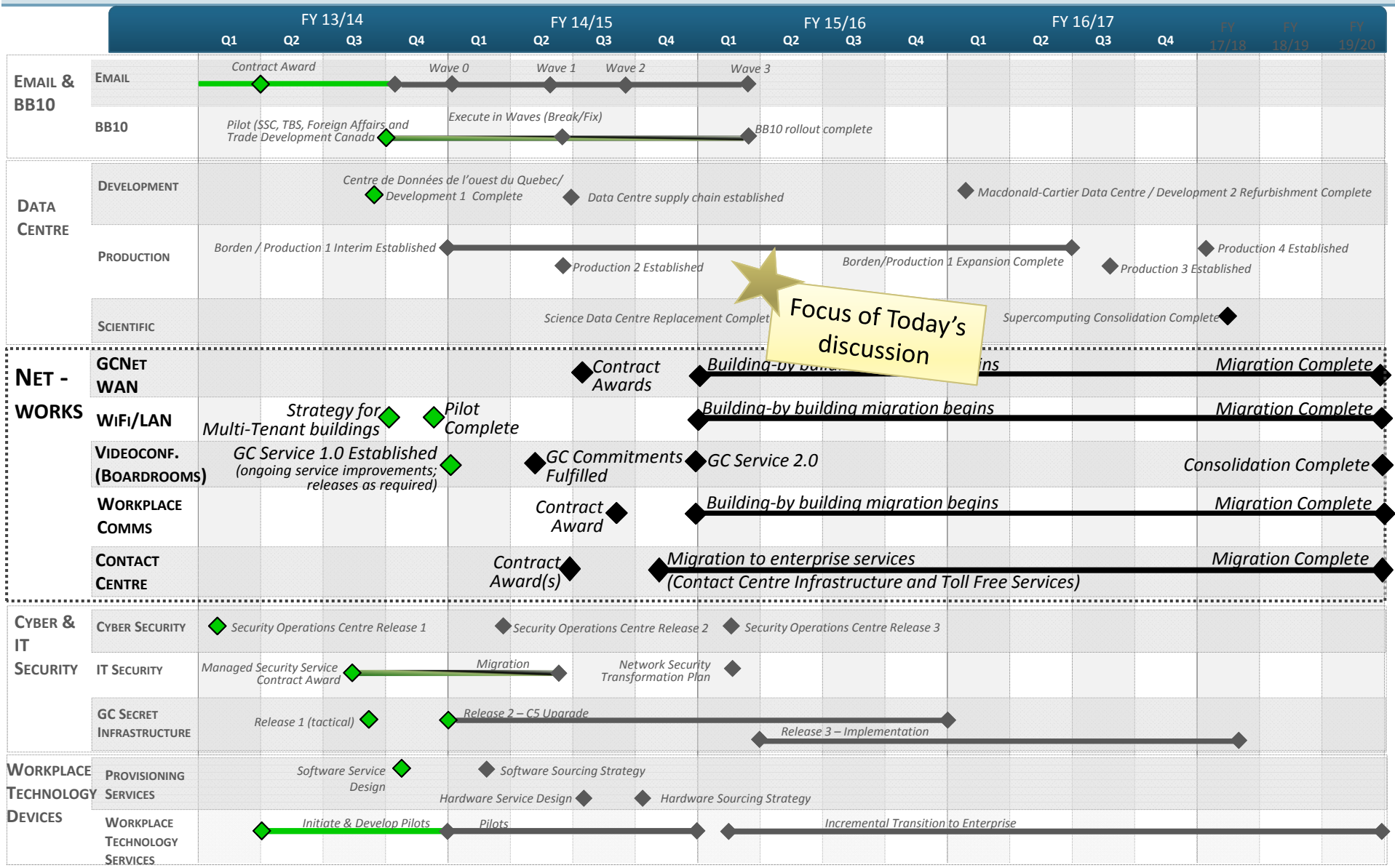
DATA
CENTRE

NET-
WORK

A single government-wide telecommunications network
Objective: Streamline and modernize the GC's telecommunications infrastructure and services

SSC Transformation Overview

Timeline



Target End State – Enterprise Data Centres

Target end state: Seven data centres

- Established in pairs for redundancy
- Mostly private sector-owned
- Most outside of the National Capital Region

First pair: Development data centres

- GC-owned Macdonald-Cartier in Ottawa
- Bell Canada in Gatineau

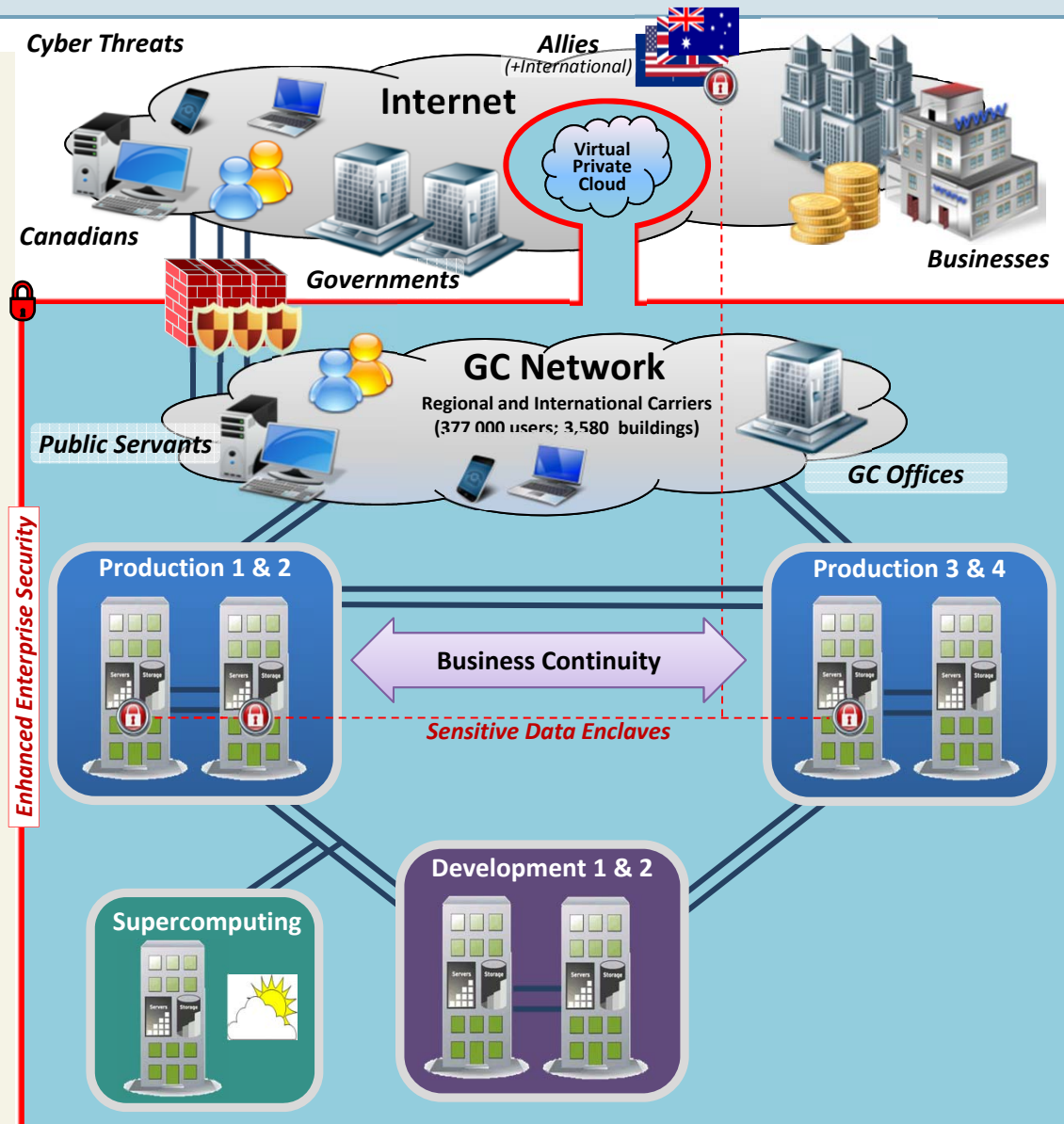
Second pair: First set of production data centres

- GC-owned facility on the Canadian Forces Base (CFB) Borden
- Site located within 100 km of Borden

Third pair: Next set of production data centres

- If/as required (to be confirmed)
- Located outside of NCR and ON

High-performance Computing - Specialized supercomputing facility



Target end state: Streamlined networks

- Connecting 377 000 public servants to each other and to Canadians
- Linking 3 580 GC-occupied buildings

Key components include:

- Single **enterprise-wide network** with enhanced capacity and robustness
- Ultra high-speed, no fail **connectivity between data centres**
- Greater, more secure **Internet connectivity**
- Streamlined and **wireless** telecom infrastructure inside buildings
- **Voice services (VoIP)** (wired and wireless)
- More desktop **videoconferencing services**
- Contact Centre Infrastructure Services
- **Enhanced security** through consolidated security services and increased perimeter security

SSC Transformation Overview

Business Requirements

- **Support a wide variety of federal government programs** and applications ranging from corporate file stores and routine data exchanges, to real-time government-wide mission-critical military, policy, health and public safety information
- **Enterprise** infrastructure and service management to eliminate silos and **facilitate interoperability** across departments and agencies
- **Reduce duplication** and inefficiencies
- **Ensure high availability** for mission critical applications
- **Standardize service levels** to ensure a consistent delivery and availability of Data Centre services across all SSC partners and agencies
- **Built-in, on-going competition** to ensure best value, continuous improvement and innovation of services
- **Security:** Supply must meet the **Trusted Supply Chain Requirements** (identified in the “Supply Chain Integrity” presentation to follow)

SSC Transformation Overview

Functional Requirements

- **Supplier diversity**
- **Open standards** to allow for workload mobility / portability across suppliers
- **Certified compliance and compatibility** with SSC reference architectures
- Must support **self-service / self-provisioning** of local area network services
- Must support **just-In-time capacity**
- **Frequent market checks** to take advantage of technology, economic or market shifts
- **Provisions for annual price competition** to ensure best value to Canada
- Must support a **secure, multi-tenant environment** (GC Domains and Zones)



SSC Transformation Overview

Thank You!





Service | Innovation | Value

Government of Canada's IBM Mainframe Infrastructure Supply Chain Renewal

September 30, 2014

Peter Littlefield
Director General
Data Centre Consolidation



Shared Services
Canada

Services partagés
Canada

Canada 

Purpose and Objectives

Purpose:

Provide an overview of Shared Services Canada's (SSC's) IBM Mainframe Transformation Strategy and the launch of the related procurement processes.

Objectives:

- Outline the SSC launch of a mainframe software procurement process, starting with the Mainframe Industry day activity
- Explain how SSC plans to proceed with “Mainframe Transformation”, which is being done to achieve efficiencies
- Seek advice and help from industry in order to achieve objectives
- Look to industry for ways to help enable mainframe workload consolidation and transformation

Outline

- 1) Mainframe transformation strategy and SSC's overall vision
- 2) Partners and clients utilizing IBM mainframes
- 3) Techniques to be used to achieve Mainframe Transformation
- 4) Mainframe hardware - current state
- 5) Mainframe software rationalization
 - Current state
 - Opportunities for competition
- 6) Proposed mainframe end state
- 7) Required activities to achieve end state
- 8) Challenges and dependencies
- 9) End state path:
 - Software rationalization/standardization
 - Mainframe consolidation/workload migration
- 10) Questions to Industry
- 11) Procurement process – next steps



Context: Transformation Tenets

Integrated Planning

Holistic planning for the **integration of application ecosystem components** across multiple platforms and data centres will facilitate smooth workload migrations and transformation.

Cooperative Development

Engage partners in developing multi-year plans for their application development, incorporating software roadmaps of the mainframe environment.

Enterprise Support

A **single, horizontal mainframe support team** will enable transformation activities and enterprise operations:

- Provides more efficient resourcing to ensure continued smooth operations;
- Better utilization of resourcing with specific partner needs when and where required.

Technical Excellence

Provide **capability for robust parallel sysplex environment**, which could be leveraged by all partners and clients (includes high intra-data centre availability, with full inter-data centre disaster recovery).



Context: Transformation Techniques

S

STANDARDIZATION

- Adjusting software runtime, engineering, installation, maintenance environments and SSC processes, for all partners/clients, to a single standard environment.

R

RATIONALIZATION

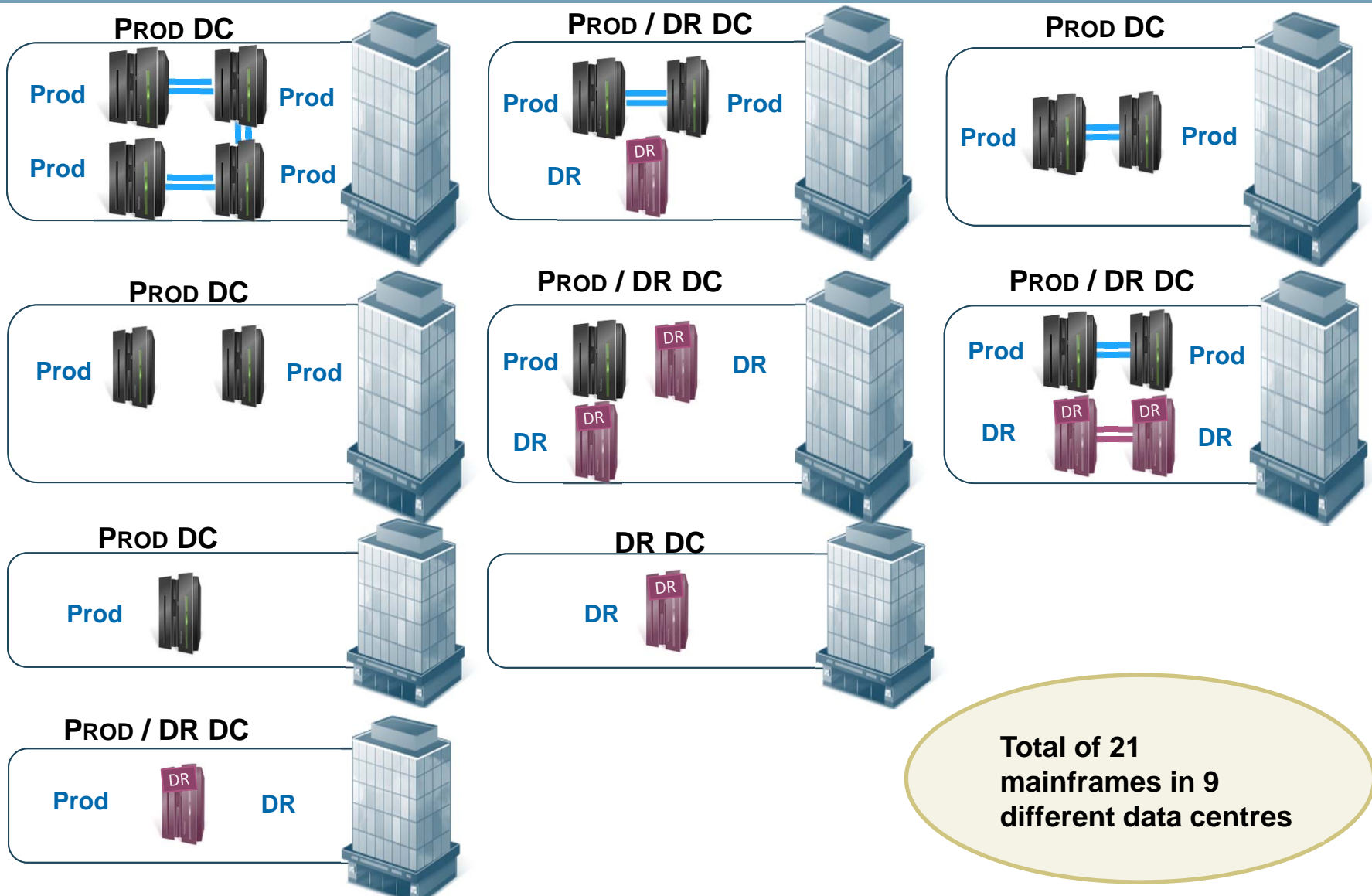
- The consolidation to a small number of software products within product categories (e.g. workload scheduling), to achieve a more cost effective and efficient operating environment.

C





CONSOLIDATION

- Physical consolidation of mainframe application workloads to a smaller number of larger mainframe servers in end state data centres.
 - In conjunction with and synchronized to the transformation of the application workloads hosted in midrange technology (the application 'eco-system').

Mainframe Hardware: Current State



**Total of 21
mainframes in 9
different data centres**

LEGEND:  SSC Managed Data Centre (DC)  Production Mainframe
 Parallel Sysplex - Mainframe Clustering  Disaster Recovery (DR) Mainframe

Mainframe Software Rationalization: Current State

CURRENT STATE ISSUES

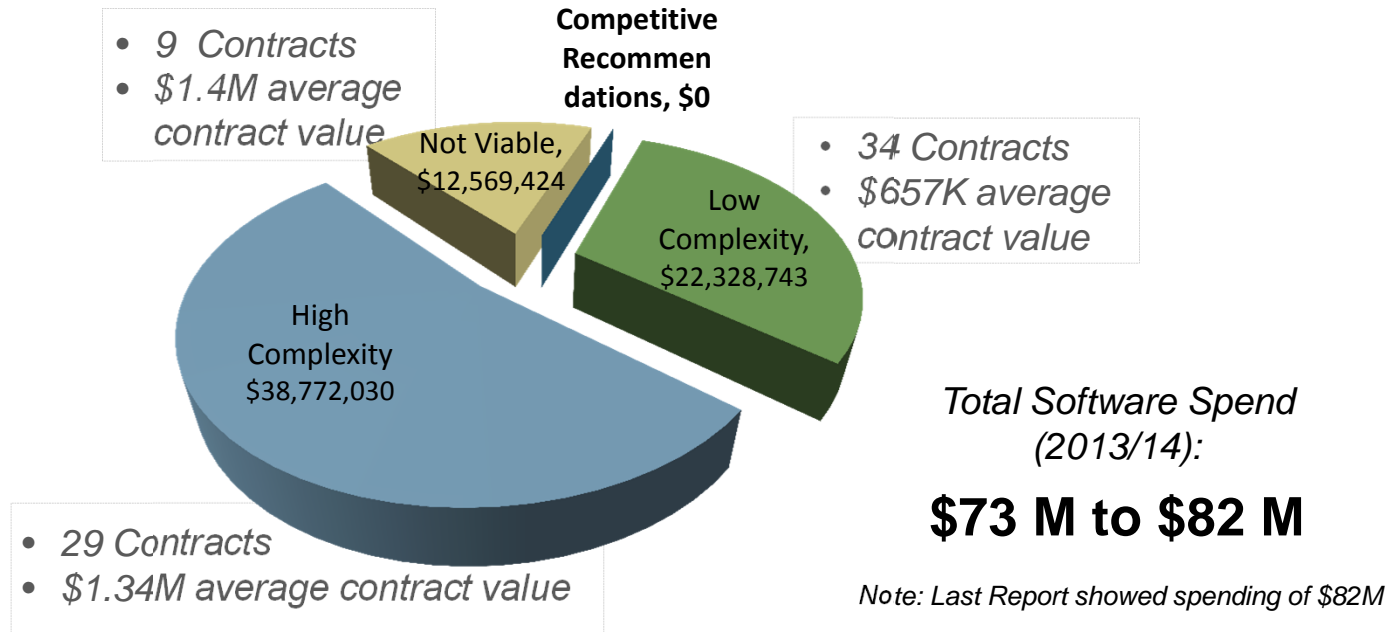
- **Significant annual expenditure** for mainframe software - **\$73M to \$82M.**
- Most Mainframe software was **not acquired through a competitive process.**
- More than 63 different software vendors
- More than 70 different contracts
- Many different facilities are hosting the same products
- Duplication in functionality being delivered by different products on the same or on different mainframes
- Many mainframe software products have a **machine capacity based license model** which is not conducive for consolidation to larger mainframe servers – revisit terms and conditions of the contracts

RATIONALIZATION OPPORTUNITIES

- **Competition has high potential for real savings.**
- Process to rationalize will utilise competitive tender process (Request for Proposal (RFP)), with intent to leverage products base already installed.

Mainframe Software Rationalization: Opportunities for Competition

SOFTWARE PRODUCT COSTS BY VIABILITY / COMPLEXITY



COMPETITION VIABILITY / COMPLEXITY SCALE

➤ Low Complexity

- Technically viable, with low Partner impact.
- Main complexity is financial, i.e. return on investment (ROI) analysis, total cost of ownership (TCO) analysis.
- Detailed assessment required to further assess impacts.

➤ High Complexity

- Technically viable, with varying Partner impact.
- Complexity factors include the potential for technical challenges, business issues (e.g. application Interoperability) and/or Partner impacts.
- Detailed analysis for risks and impact is required.

➤ Not Viable

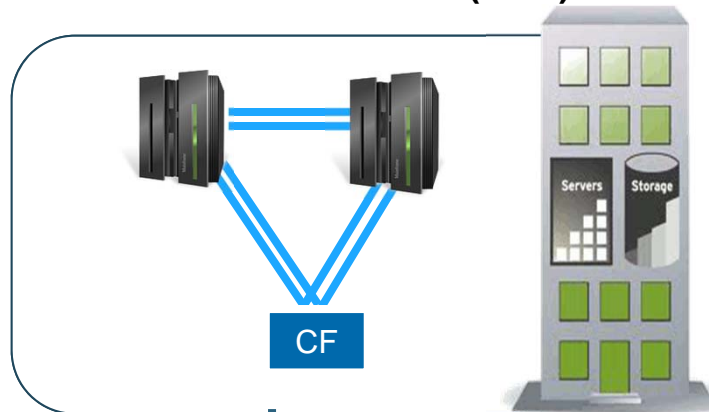
- Reasons include technical viability, lack of competition, Partner impact, etc.

Proposed Mainframe End State

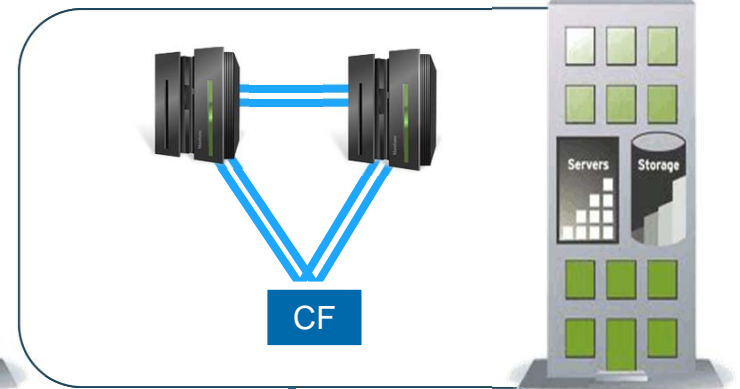
KEY ATTRIBUTES

- The design separates workloads based on profile of partners/clients.
- Production workloads will be split relatively even based on processing needs.
- Provides highest intra-data centre resiliency while achieving significant savings and workload balance.
- Mitigates risk by distributing mission-critical mainframe processing.
- Out-of-region DR is provided to mirror production.

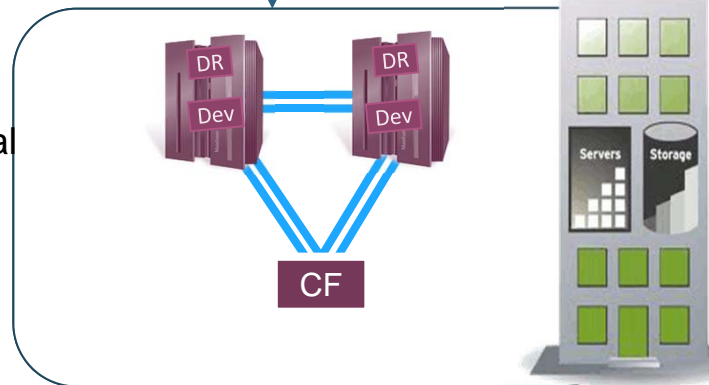
ENTERPRISE DATA CENTRE (EDC) PROD 1



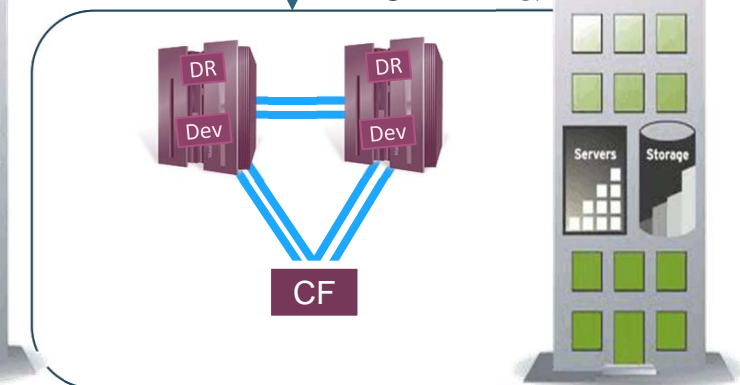
EDC PROD 2






EDC DEV2 & DR2



EDC DEV1 & DR1



Note: only two Primary MF servers are illustrated in each datacentre, however additional MF servers may be required.

LEGEND:  End State SSC Managed Data Centre (DC)  Mainframe (MF) CF= External Coupling Facility for Parallel Sysplex (smaller MF used as CF)  Parallel Sysplex (Mainframe Clustering)  Disaster Recovery Mainframe/Development workloads

Required Activities to Achieve End State

- Renew the supply chain to deliver both tactical and strategic hardware and software requirements:

- *Tactical requirements* will meet partners current and near term business needs;
- *End state hardware and software* will support an efficient, advanced hosting platform.

Supply Chain Renewal

Upgrade Mainframe Capacity

- Implement short and medium-term mainframe hardware capacity or machine upgrades to relieve critical pressures facing organizations while supporting transition to end state.

Workload Migration

- Ensure connectivity between old and new environments for the continued operations of applications hosted on end state mainframes and to enable workload migrations.

Software Rationalization

- Conduct review of current software positions across all partners/clients to identify key opportunities for change, which will enable physical workload consolidations and support the achievement of efficiencies.

Standardization

- Standardize current mainframe environments prior to physical consolidation in order to ensure seamless migration.

Completion of these activities will require a close working relationship between SSC and partners / clients

Challenges and Dependencies

SOFTWARE RATIONALIZATION

- Changes to operating environments for some mainframe partners/clients, may have cost impacts.
- Competitive process will lead to product and process changes to partners and clients. The full impact yet to be determined.
- Not all software is within SSC scope of control and may require more partner involvement and negotiation.

End State Path: Software Standardization/Rationalization

- 1) Leverage the strong partnership that SSC has with mainframe partners / clients to ensure ongoing cooperation and collaboration for the successful transition from current to end state.
- 2) Establish formal communication channels regarding business intake throughout the transformation to ensure issue identification and avoidance.
- 3) Conduct detailed ongoing dialog with mainframe partners / clients at multiple levels of the organization to ensure proper transition.
- 4) Hardware Consolidation and workload Migration may begin prior to having completed standardizing and rationalizing some of the various software.
- 5) SSC will look to enter into discussions with the various software vendors to adjust the Terms and Conditions of the existing contracts that would allow SSC to enable consolidation to a smaller number of larger machines with no uplift in cost based on equivalent product usage.

End State Path:

Software Standardization/Rationalization (continued)

- 6) SSC will institute a process to standardize on certain product/software categories, possibly as follows:
 - a) Base Security Product
 - b) Tape Management & Tape Utilities
 - c) Workload Scheduling
 - d) Session Management
 - e) Data Utilities
 - f) Data Movers
 - g) Storage Backup & Recovery
 - h) Application Testing and Debugging
 - i) Data Archival/Retrieval
 - j) Print Servers or Managers
 - k) Others ...

End State Path:

Mainframe Consolidation / Workload Migration

- 1) Migrate from 21 mainframes down to as few as 8 larger sized machines
- 2) Four DCs in all, two for production DCs and two for non-production DCs (DR and Dev)
- 3) High Resiliency within region
- 4) Out-of-region disaster recovery capabilities
- 5) Initial work partitioning will be based on partner / client as it is today
- 6) Initial LPAR sizing will also be based on today's usage / numbers
- 7) Similar profiles workloads will be hosted on the same machine

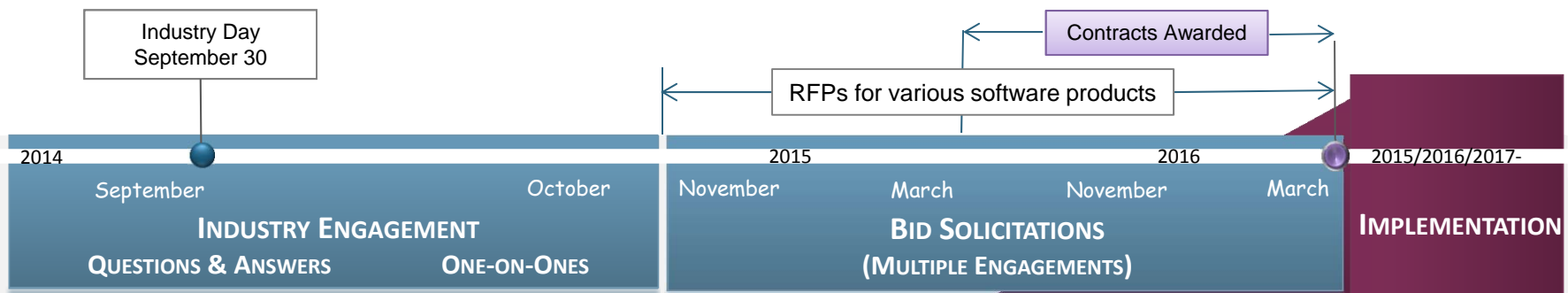
Questions to Industry

SSC is soliciting feedback on the following:

- Software Rationalization
 - 1) What software licensing models and options are available that could enable consolidation to a smaller number of larger machines with no uplift in cost based on equivalent product usage?
 - 2) How can the Government of Canada best leverage existing investments in software licenses through the procurement process, in order to maximize value for money?
 - 3) What contract agreement length-duration would be optimal?
 - 4) Should SSC own the hardware and the software?
- Services
 - 1) SSC is seeking advice regarding the feasibility of services which would assist SSC to achieve its goals with respect to hosting and supporting mainframe environments and services. What services are available and how would you advise SSC use them?

Procurement Process & Next Steps

- Industry Day Questions (Request for Information (RFI)) –
 - SSC will request one-on-one sessions with specific vendors based on the responses received from the “Questions to Industry” component
- Industry one-on-one engagements* to obtain further clarification on the discussion questions presented at Industry Day
- Finalize analysis of competitive software landscape – a final breakdown of the software that can be rationalized for the mainframe
- Individual procurement processes for software



* Note: Vendors may be invited to one-on-one sessions based on their responses to the “Questions to Industry” component.



Service | Innovation | Value

Data Centre Consolidation Mainframe Transformation Collaborative Procurement Solutions Approach

Andrea Totten

A/Supply Team Lead

Procurement and Vendor Relationships

Shared Services Canada

30 Sept 2014



Shared Services
Canada

Services partagés
Canada

Canada

Agenda

- Procurement Considerations for Mainframe Transformation
- Supply Methods
- SSC Procurement Processes
- Descriptions of the Various Phases
- Industry Engagement Activities Schedule

Procurement Considerations for Mainframe Transformation

- A National Security Exception (NSE) will apply
- Mainframe Transformation may leverage the PWGSC Fairness Monitor Program to oversee specific procurements and activities. Please go to <http://www.tpsgc-pwgsc.gc.ca/se-fm/index-eng.html> for more information
- It is anticipated the vendors will be required to hold a valid security clearance, the levels of which may vary depending on the procurement
- Depending on the procurement, data sovereignty may apply

Supply Methods

Contract

- A voluntary, deliberate, and **legally enforceable agreement** between two or more competent parties
- Order work using task authorizations (TAs), service orders (SOs), requisitions on a contract (ROCs), etc.

Standing Offer (SO)

- A continuous offer from a supplier to the government that allows the government to purchase goods and/or services at **pre-arranged prices, under set terms and conditions**, when and if required
- Not a contract until the government issues a call-up

Supply Arrangement (SA)

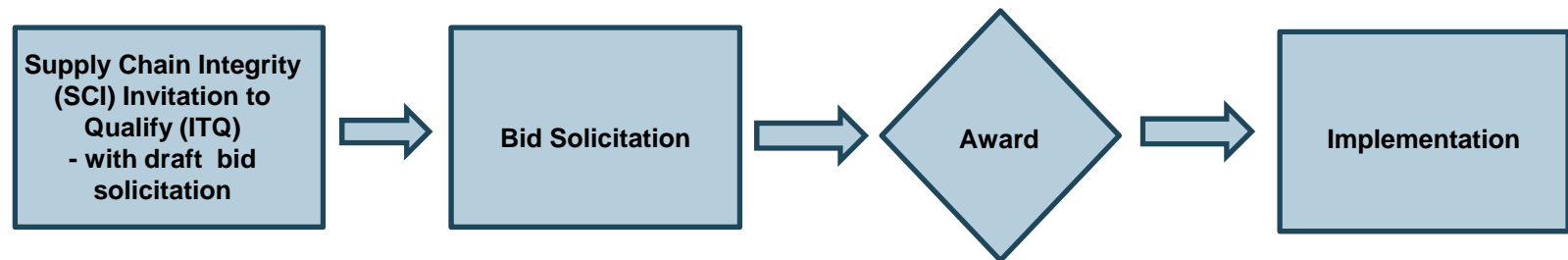
- An agreement between the government and a set of **pre-qualified suppliers that includes predetermined conditions and ceiling prices** that will apply to bid solicitations and resulting contracts

SSC Procurement Processes

Traditional Bid Solicitation*



Two-Phase Approach (Supply Chain Integrity (SCI) Invitation to Qualify (ITQ))*



Three-Phase Approach (Collaborative Procurement Solutions – CPS)*



Most likely to be used for Mainframe Transformation Procurements

* Engagement activities such as Industry Days, Letters of Interest, Requests for Information, etc. may precede the formal tendering process

Two-Phase*

- To qualify suppliers based on their Supply Chain Security Information (SCSI)
- No limit to the number of suppliers that can qualify as it is solely based on the SCSI passing the Supply Chain Integrity (SCI) assessment

Three-Phase

- To qualify suppliers who have demonstrated and proven skills and experience in implementing and providing the goods/services in question
- Evaluation criteria will focus on the supplier's capabilities and experience to deliver
- Suppliers who meet the mandatory ITQ evaluation criteria will be deemed "Qualified Respondents" and will proceed to the RRR phase
- There may be multiple streams for which vendors can qualify
- There may be rated criteria

* Standard process

Two-Phase

- No RRR Phase

Three-Phase

- Qualified Respondents will be provided with a draft bid solicitation and other documents (e.g. Statement of Work (SOW))
- Canada will collaborate with Qualified Respondents to seek feedback and clarification on Canada's requirements to refine the draft bid solicitation and other documents
- RRR sessions may have various formats (e.g. workshops, one-on-one sessions, Q&A documents, etc.)
- SCI process may also be started/completed during this stage

Two-Phase

- Canada may issue one or more formal bid solicitations directly to the Qualified Respondents who have received an approval letter for their Supply Chain Security Information (SCSI)
- Each Qualified Respondent will be permitted to formally bid on the requirements set out in the bid solicitation(s)

Three-Phase

- Canada may issue one or more formal bid solicitations directly to the Qualified Respondents who have qualified at the ITQ phase
- Each Qualified Respondent will be permitted to formally bid on the requirements set out in the bid solicitation(s)
- SCI process may be completed during this phase

Two-Phase and Three-Phase

- Contract Award will occur after completion of the Bid Solicitation Phase
- One or more contract(s), standing offer(s) or supply arrangement(s) may be awarded based on the bid solicitation(s)

Industry Engagement Activities Schedule

Mainframe Transformation Industry Engagement Activities



Written Submissions

Questions?
(for vendors only)





Cyber & Supply Chain Threats to the GC

Mainframe Industry Day

September 30th, 2014

Brad McInnis, Communications Security Establishment



Communications Security
Establishment

Centre de la sécurité
des télécommunications

Canada

CSE: What We Do



- CSE: Canada's national cryptologic agency
- Safeguarding Canada's security through information superiority
- 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



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



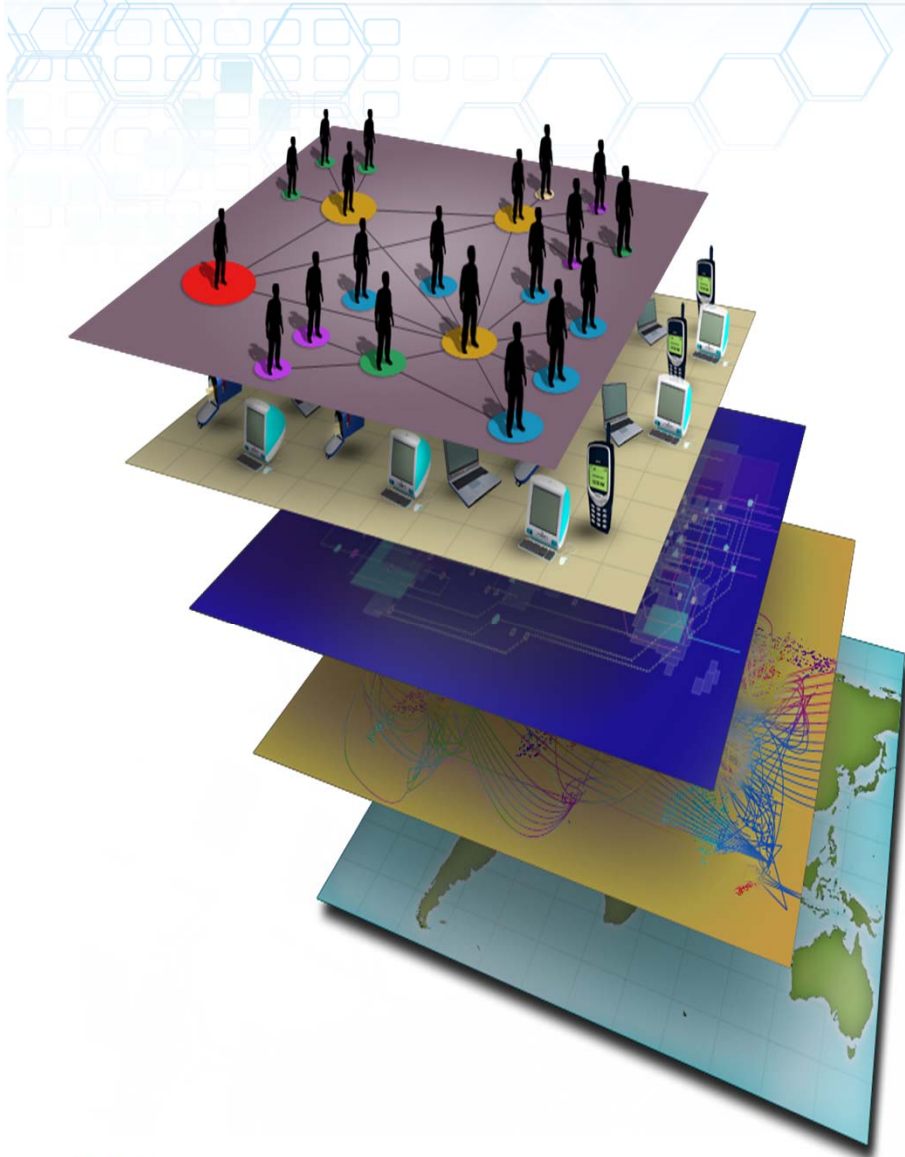
Technology Vulnerabilities



- Unintentional vulnerabilities or weaknesses
 - Design flaws
 - Implementation errors
- 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



How they get in: Access Methods



Persona



**Insider or CNE
or HUMINT**

Cyber Persona



**Computer
Network
Exploitation**

Logical Network



Physical Network



Supply Chain

Geographic



**Passive, Diffusion,
collection**



Cyber Threat Environment



- **Cyber Threats** are the possibility of a malicious attempt to damage or disrupt a computer network or system

Information Theft

Includes intellectual property theft, identity theft, electronic bank heists, illicit trade and theft of sensitive government information

Disruption

Includes disrupted communication networks, website defacement and denial of service attacks

Destruction

Includes attacks on a country's critical infrastructure and cyber warfare



CSE: IT Security Program



- We help prevent, detect and defend against IT security threats and vulnerabilities
- CSE 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 favor 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



An Issue of National Security



- **Risks from vulnerable technologies**
 - Covert and persistent access by cyber threat actors in GC departmental networks threatens the sovereignty of GC information and the continuity of government operations
 - Cyber threat actors are effective at exploiting inter/intra-connected network element technologies and management systems used to administer and operate network infrastructures
- **Risks from an overly complex and decentralized threat surface**
 - Consolidation of GC networks through DCN is 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 circumvent GC cyber security measures
 - More difficult for the GC to detect and remediate



GC Shared Services Procurements



- Shared Services Canada and CSE are working in partnership to eliminate or significantly reduce risks to the GC from cyber threats & global supply chain vulnerabilities
- CSE will provide follow-up briefings on supply chain risk mitigation to interested suppliers for GC shared services
 - Companies must be willing to sign a CSE 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, CSE will seek long-term partnerships with successful suppliers
 - CSE will assist Shared Services Canada in the pedigree analysis of supply chain information provided by respondents
- Examples of these requirements can be found on CSE's website under Technology Supply Chain Guidance





Questions?



Communications Security
Establishment

Centre de la sécurité
des télécommunications

Canada



Service | Innovation | Value

Mainframe Technology

Supply Chain Integrity (SCI) Assessment Information Session



SCI Process Overview

Patrick Mountford
Director
Cyber and IT Security Transformation



Shared Services
Canada

Services partagés
Canada

Canada

Agenda

- ✓ Context
- ✓ Supply Chain Integrity Process
- ✓ IT Product List Template
- ✓ SCI Scope Diagram
- ✓ SCI Process Flowchart
- ✓ On-going SCI Auditing Flowchart

Nature of the SCI Process

- ✓ The purpose of the Supply Chain Integrity (SCI) process is to ensure that **no un-trusted equipment, software or services**, procured by SSC, are used to deliver and/or support GC services.
- ✓ Communications Security Establishment (CSE) assesses the Supply Chain Security Information (SCSI) and makes recommendations. SSC makes business decisions based on CSE's recommendations.
- ✓ Respondents, Qualified Respondents and/or Bidders **must successfully pass** the SCI process in order to be able to continue the procurement process.
- ✓ SCI process is subject to the Non-Disclosure Agreement contained in the procurement documents. Subcontractors may also be asked to sign non-disclosure agreements during the process.

SCSI Submission Requirements

- ✓ Respondents must submit the required information to the Contracting Authority before the imposed deadline. The mandatory elements will be clearly identified in the ITQ, RRR or RFP document:
 - a. **IT Product List:**
 - Information regarding all Products over which Canada's Data would be transmitted and/or stored that will be used and/or installed to perform any part of the Work described in the resulting contract
 - Products include any hardware that operates at the data link layer of the OSI Model and above, any software and Workplace Technology Devices.
 - Include Products used by both the Respondent and by each of their proposed subcontractors in any context (installation, testing, production, delivery, support, maintenance, etc.)
 - b. **Network Diagrams:** Conceptual network diagrams
 - c. **List of Subcontractors:** Includes all subcontractors that could be used to perform any part of the Work pursuant to any resulting contract (including subcontractors that are affiliated or otherwise related to the Respondent)

SCSI Assessment Process

- ✓ Canada will assess whether, in its opinion, the SCSI creates the possibility that the Respondent's solution (including the subcontractors used to implement that solution) could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information.
- ✓ In conducting its assessment, Canada may request from the Respondent any additional information that Canada requires to conduct a complete security assessment of the SCSI.
- ✓ Assessment of the SCSI requires that a complete package be submitted before the established deadline.

Outcome of Assessment

- ✓ All Respondents will be notified in writing regarding whether they remain qualified following the SCI process, or whether they have been disqualified as a result of their SCSI assessment.
- ✓ Any Respondents will be required, when responding to any bid solicitation, to propose a solution **consistent** with the version of the SCSI it submits as part of this SCI process that is approved by Canada.
- ✓ Once all the Respondent's SCSI (including the SCSI relating to its subcontractors) has been approved by Canada, no modifications * are permitted to the SCSI except under exceptional circumstances, as determined by Canada (this only applies to Products that were requested to be included in the SCSI form).

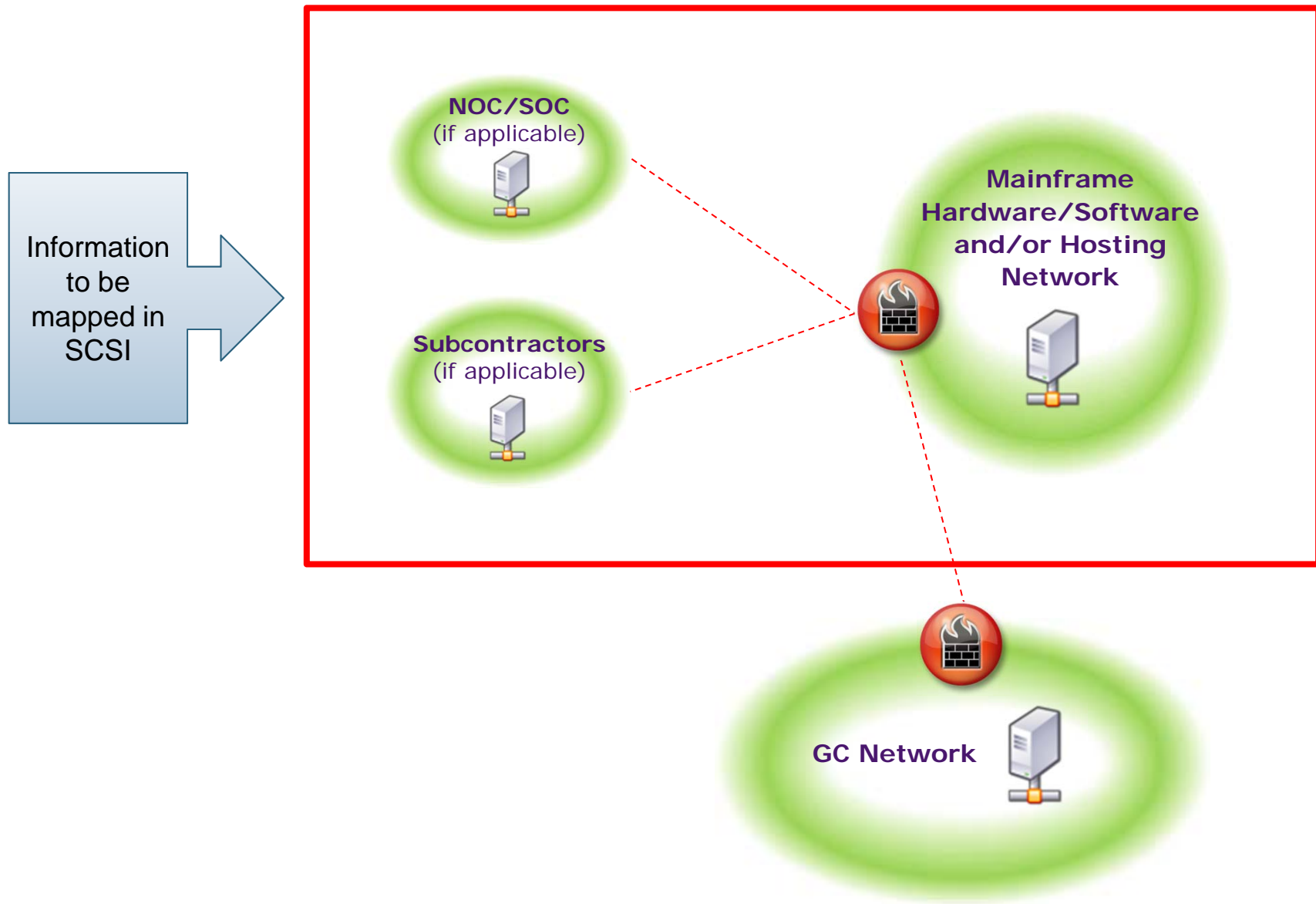
*If a Respondent believes that exceptional circumstances exist that may warrant such a modification, the Respondent may submit a request in writing to the Contracting Authority at any time prior to contract award.

IT Product List Template

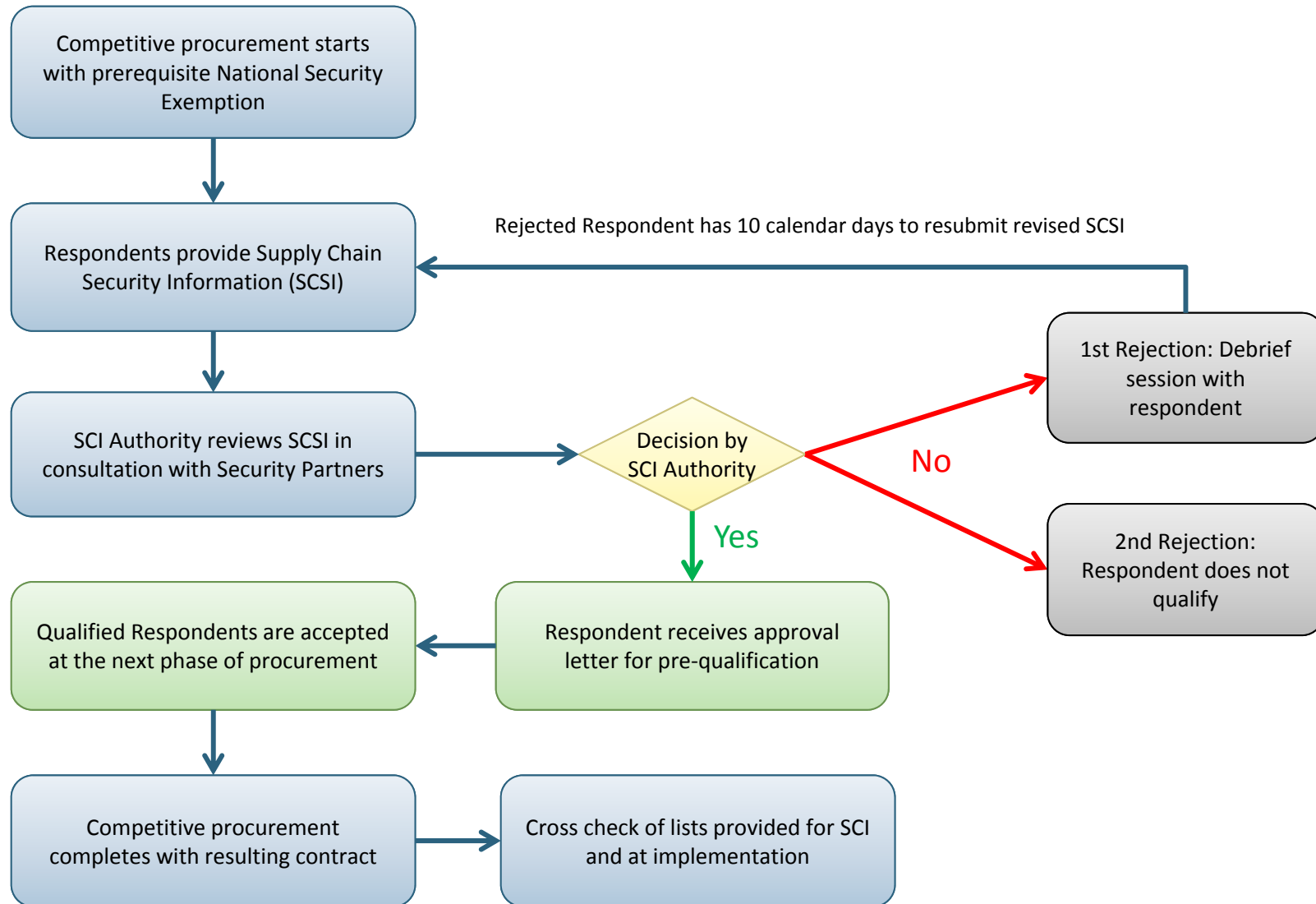
- ✓ Respondents are requested not to repeat multiple iterations of the same Product (e.g. if the serial number and/or color is the only difference between two products, they are considered the same Product with regards to Supply Chain Integrity).

<i>Product/Component</i>							
Line Item #	Location (Service Delivery Point, Contractor POP, NNI, Datacentre/hosting location, Third Party Location, Operations Center, Security Operations Center, etc.) Cross-referenced to network diagram (a)	Product Type (Appliance, Hardware, Software - Operating System, Software - Application, Module) (b)	IT Component (e.g. Firewall, Router, Switch, Server, Workstation, Laptop, Security Appliance) (c)	Product Model Name or Number (d)	Description and Purpose (e)	Product Manufacturer, Software Publisher and/or Original Equipment Manufacturer of embedded components (f)	Subcontractor (if equipment is being provided by a subcontractor) (g)

SCI Scope Diagram

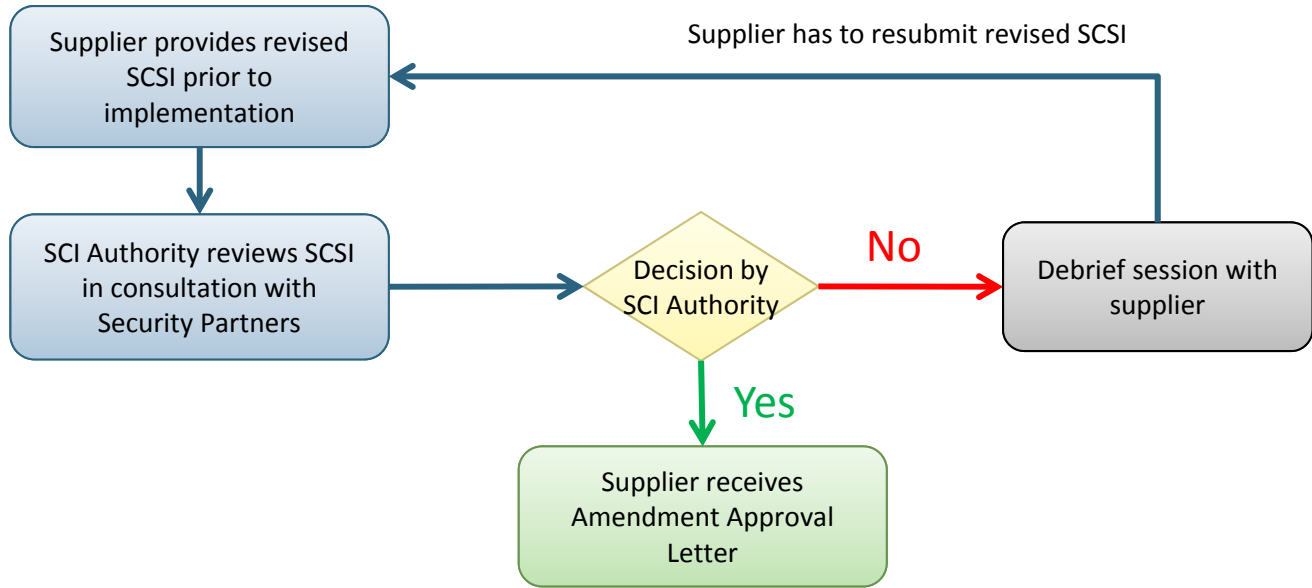


Supply Chain Integrity (SCI) Process

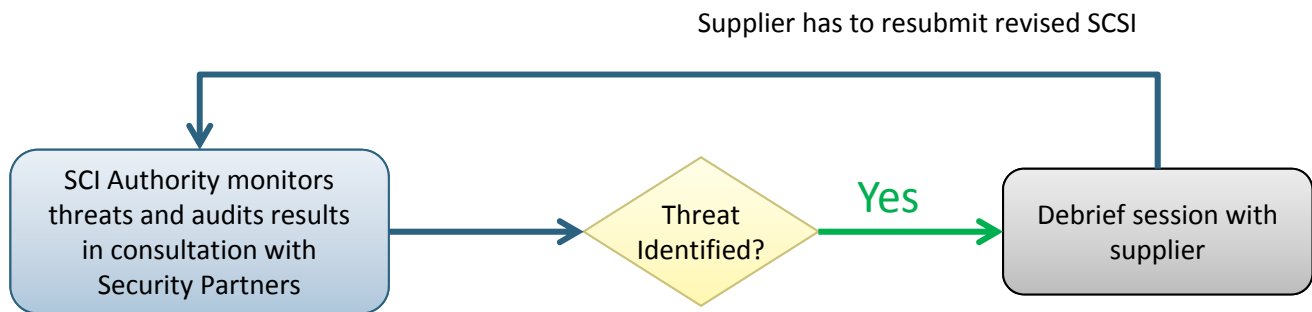


Ongoing SCI Auditing

On-going SCI auditing from the moment the contract has been awarded until it ends.



Internal threat evaluation can lead to the review of specific equipment or services



Questions?