Service | Innovation | Value

TELECOMMUNICATIONS TRANSFORMATION PROGRAM

Network Solutions Supply Chain

Industry Day

May 28, 2014

Shared Services Canada Services partagés Canada

Canada

Network Solutions Supply Chain Industry Day

Industry Day Objectives

- Share Telecommunications Transformation plans with industry suppliers and engage in a dialogue regarding Network Solutions Solutions Supply Chain

- Explain the proposed “Collaborative Procurement Solutions” approach

- Address the Cyber Security Supply Chain Threat

- Elicit written feedback from suppliers on the questions posed during this presentation

Network Solutions Supply Chain Industry Day

Agenda

Time	Presenter	Description
1:00 - 1:05 pm	**John Dullaert** *Director, Telecommunications Transformation Program, Shared Services Canada (SSC)*	Opening Remarks and Industry Day Objectives
1:05 – 1:35 pm	**Benoît Long** *SADM, Transformation, Service Strategy and Design, SSC*	SSC Transformation Overview
1:35 - 2:30 pm	**Michel Fortin** *DG, Telecommunications Transformation Program, SSC*	Network Solutions: *Overview, High Level Requirements and Discussion Topics*
2:30 – 2:35 pm	***Break***	
2:35 – 3:20 pm	**Michel Fortin** *DG, Telecommunications Transformation Program, SSC*	Network Solutions: *Key Questions*
3:20 – 3:50 pm	**Tom Mercer** *Manager, Telecommunications Systems Division, Procurement and Vendor Relationships, SSC*	Collaborative Procurement Solutions Approach
3:50 – 4:20 pm	**Brad McInnis** *Security Strategic Relationships Office, Communications Security Establishment Canada* **Simon Levesque** *Sr. Director Planning and Design, Cyber and IT Security Transformation Program, SSC*	Supply Chain Security Information Assessment (SCSI)
4:20 – 4:50 pm	**John Dullaert** *Director, Telecommunications Transformation Program, SSC*	Questions and Answers, Recap / Closing Remarks

TELECOMMUNICATIONS TRANSFORMATION PROGRAM Network Solutions Supply Chain (NSSC) Industry Day

Shared Services Canada (SSC) Transformation Overview

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

May 28, 2014

SSC Transformation Overview

Agenda

- Industry Day Objectives
- SSC Transformation Objectives and Purpose
- Transformation Timeline
- Transformation Phased Approach
- Current State
- Target End State
- Business and Functional Requirements
- Engagement
- Wrap up

SSC Transformation Overview
Purpose of Industry Day

- To provide **background** on telecommunications transformation with a focus on Intra-building Local Area Network transformation
- To **continue a dialog** with Industry to learn what are the best and most innovative options available in the market today that will support the Government of Canada's requirements for developing a Network Solutions Supply Chain
  - Obtain industry input on the strategy for developing a comprehensive strategy for transforming Intra-building Local Area Networks while maintaining the existing environment
  - Advice that could lead to better pricing (based on past experience)
  - Address questions regarding process
  - Set the stage for the supplier written responses

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

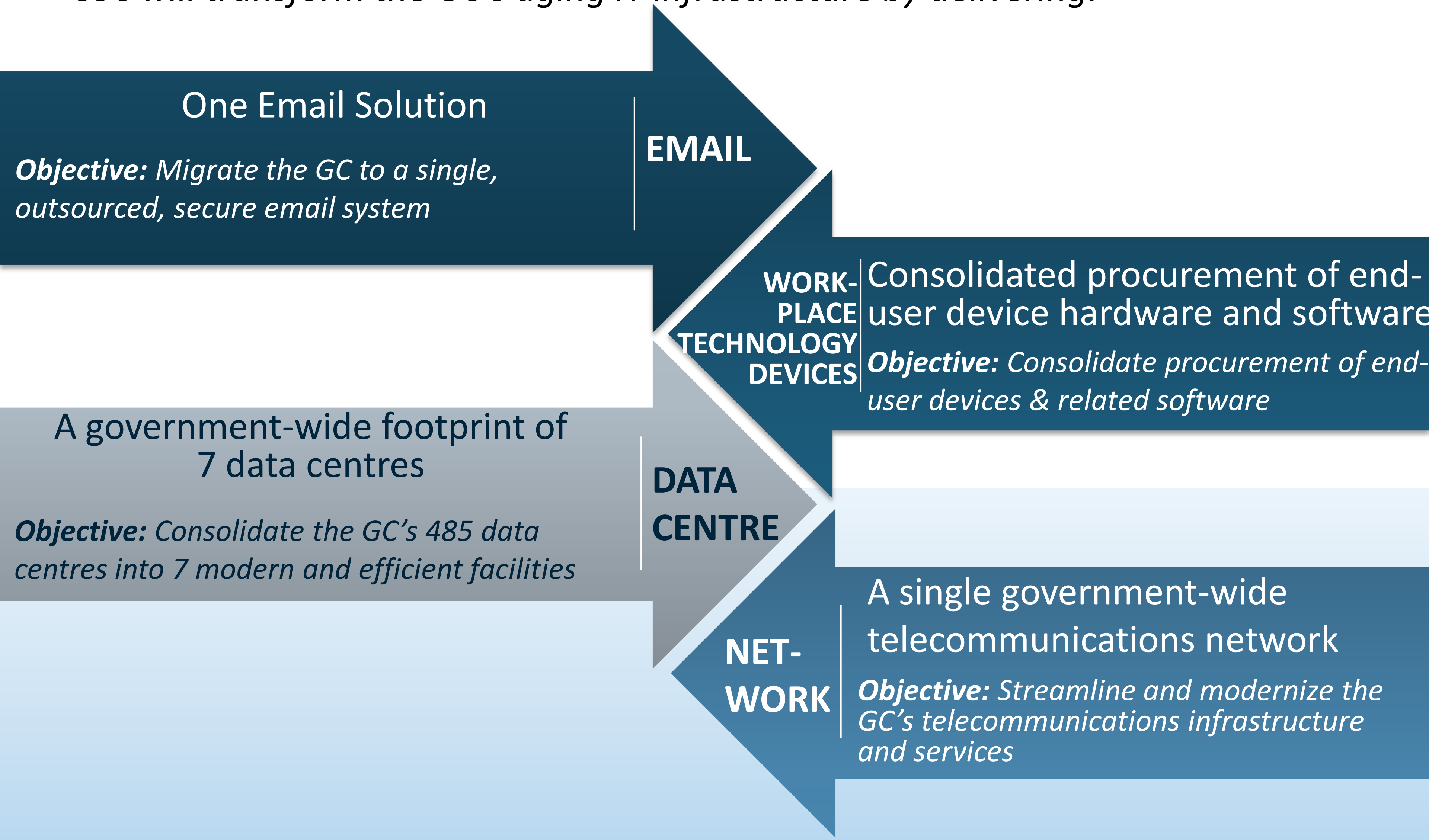
Security

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:



EMAIL

One Email Solution

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

WORKPLACE TECHNOLOGY DEVICES

Consolidated procurement of end-user device hardware and software

Objective: *Consolidate procurement of end-user devices & related software*

DATA CENTRE

A government-wide footprint of 7 data centres

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

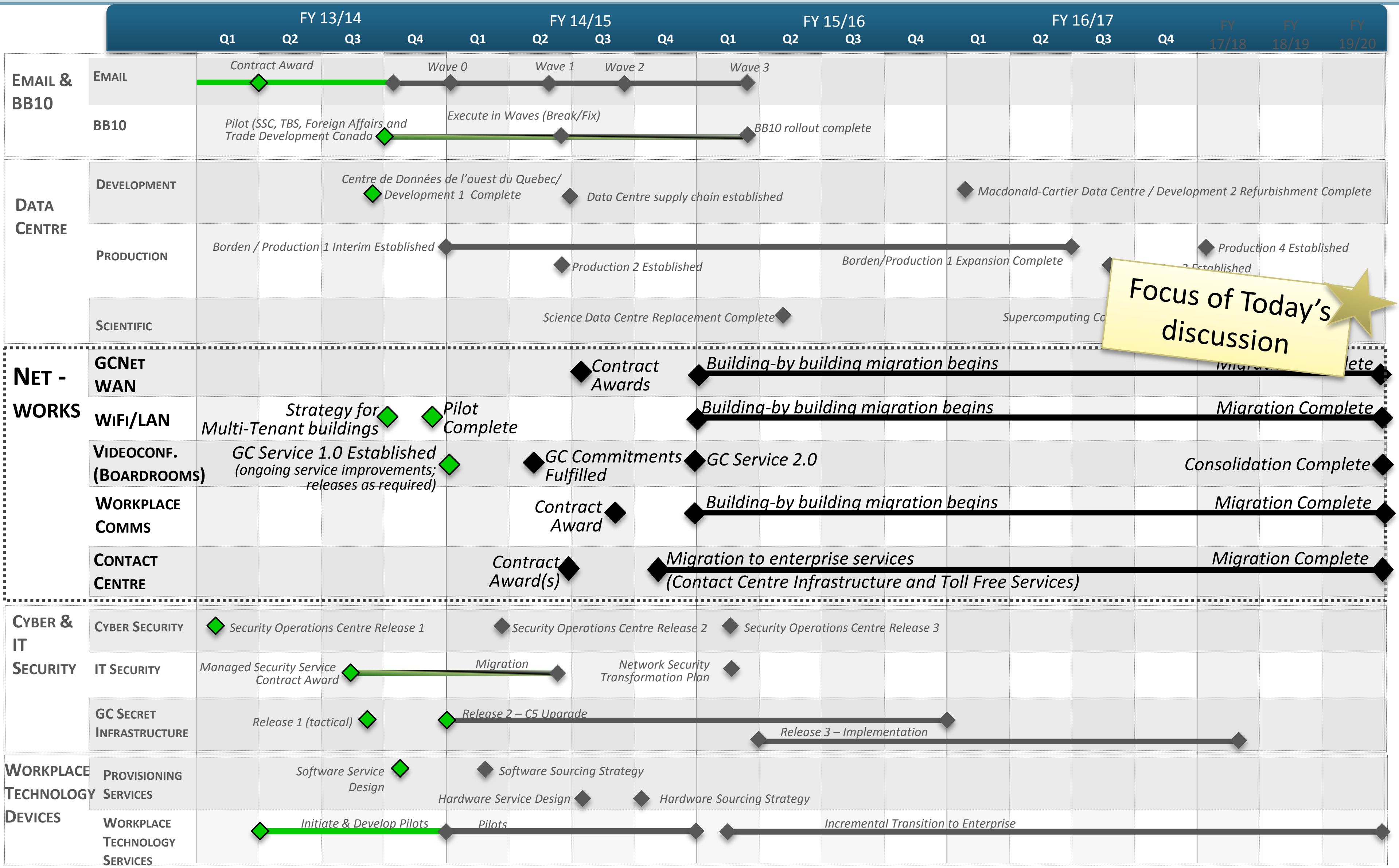
NETWORK

A single government-wide telecommunications network

Objective: *Streamline and modernize the GC's telecommunications infrastructure and services*

SSC Transformation Overview

Timeline



FY 13/14: Q1, Q2, Q3, Q4 | FY 14/15: Q1, Q2, Q3, Q4 | FY 15/16: Q1, Q2, Q3, Q4 | FY 16/17: Q1, Q2, Q3, Q4 | FY 17/18 | FY 18/19 | FY 19/20

Email & BB10

- **Email**: Contract Award; Wave 0; Wave 1; Wave 2; Wave 3
- **BB10**: Pilot (SSC, TBS, Foreign Affairs and Trade Development Canada; Execute in Waves (Break/Fix); BB10 rollout complete

Data Centre

- **Development**: Centre de Données de l'ouest du Quebec/ Development 1 Complete; Data Centre supply chain established; Macdonald-Cartier Data Centre / Development 2 Refurbishment Complete
- **Production**: Borden / Production 1 Interim Established; Production 2 Established; Borden/Production 1 Expansion Complete; …3 Established; Production 4 Established
- **Scientific**: Science Data Centre Replacement Complete; Supercomputing Co…

Focus of Today's discussion

Net - works

- **GCNet WAN**: Contract Awards; Building-by building migration begins; Migra… …lete
- **WiFi/LAN**: Strategy for Multi-Tenant buildings; Pilot Complete; Building-by building migration begins; Migration Complete
- **Videoconf. (Boardrooms)**: GC Service 1.0 Established (ongoing service improvements; releases as required); GC Commitments Fulfilled; GC Service 2.0; Consolidation Complete
- **Workplace Comms**: Contract Award; Building-by building migration begins; Migration Complete
- **Contact Centre**: Contract Award(s); Migration to enterprise services (Contact Centre Infrastructure and Toll Free Services); Migration Complete

Cyber & IT Security

- **Cyber Security**: Security Operations Centre Release 1; Security Operations Centre Release 2; Security Operations Centre Release 3
- **IT Security**: Managed Security Service Contract Award; Migration; Network Security Transformation Plan
- **GC Secret Infrastructure**: Release 1 (tactical); Release 2 – C5 Upgrade; Release 3 – Implementation

Workplace Technology Devices

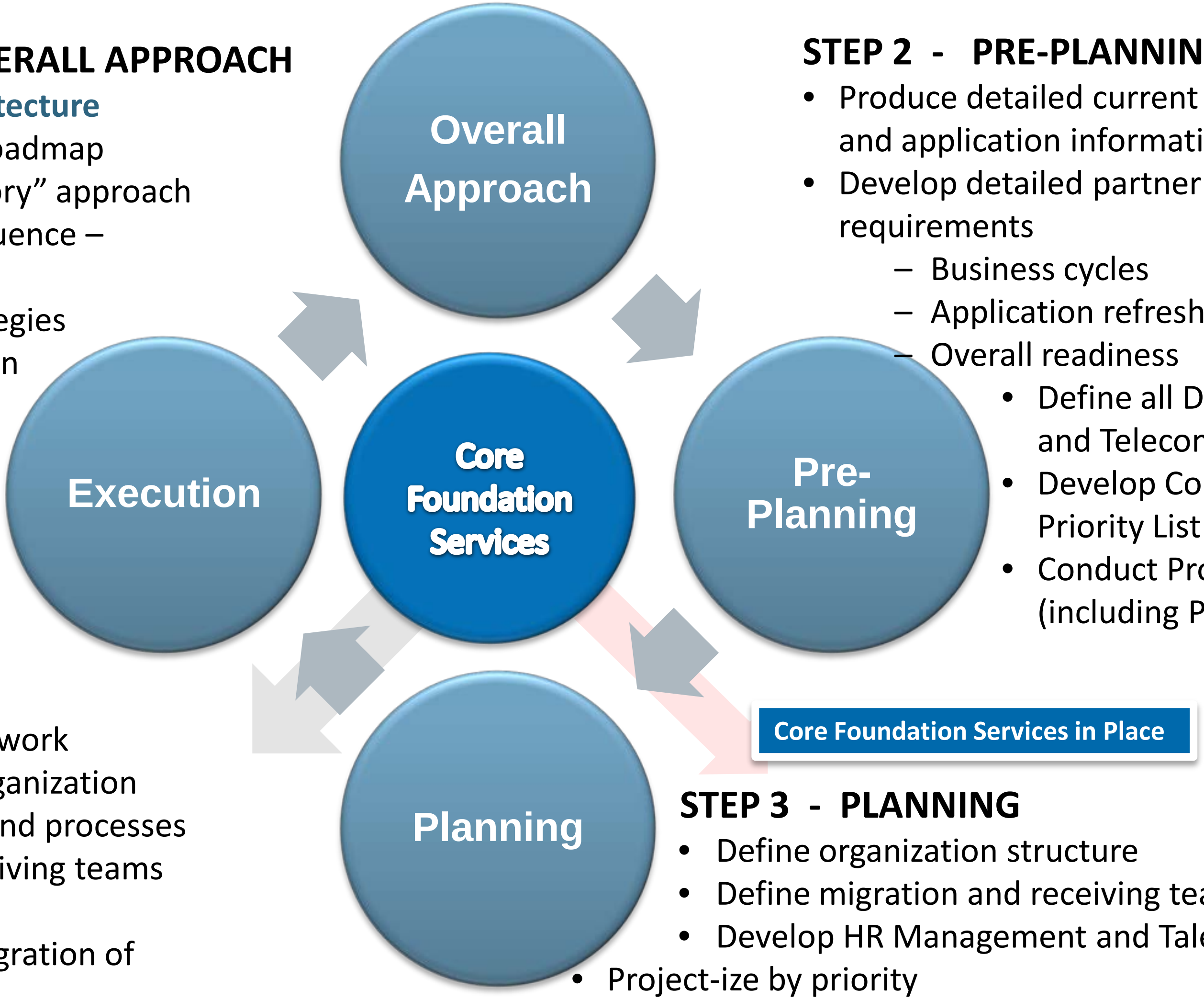
- **Provisioning Services**: Software Service Design; Software Sourcing Strategy; Hardware Service Design; Hardware Sourcing Strategy
- **Workplace Technology Services**: Initiate & Develop Pilots; Pilots; Incremental Transition to Enterprise

SSC Transformation Overview

Transformation Phased Approach

STEP 1 - ESTABLISH OVERALL APPROACH

- Produce **Reference Architecture**
- Establish **Core Services** roadmap
- Develop “Migration Factory” approach
- Define consolidation sequence – Competing factors
- Determine sourcing strategies
- Develop security by design



STEP 2 - PRE-PLANNING

- Produce detailed current state / asset and application information
- Develop detailed partner requirements
  - Business cycles
  - Application refresh plans
  - Overall readiness
    - Define all Data Centre and Telecom Services
    - Develop Consolidation Priority List (CPL)
    - Conduct Procurement (including P3, etc.)

STEP 4 - EXECUTION

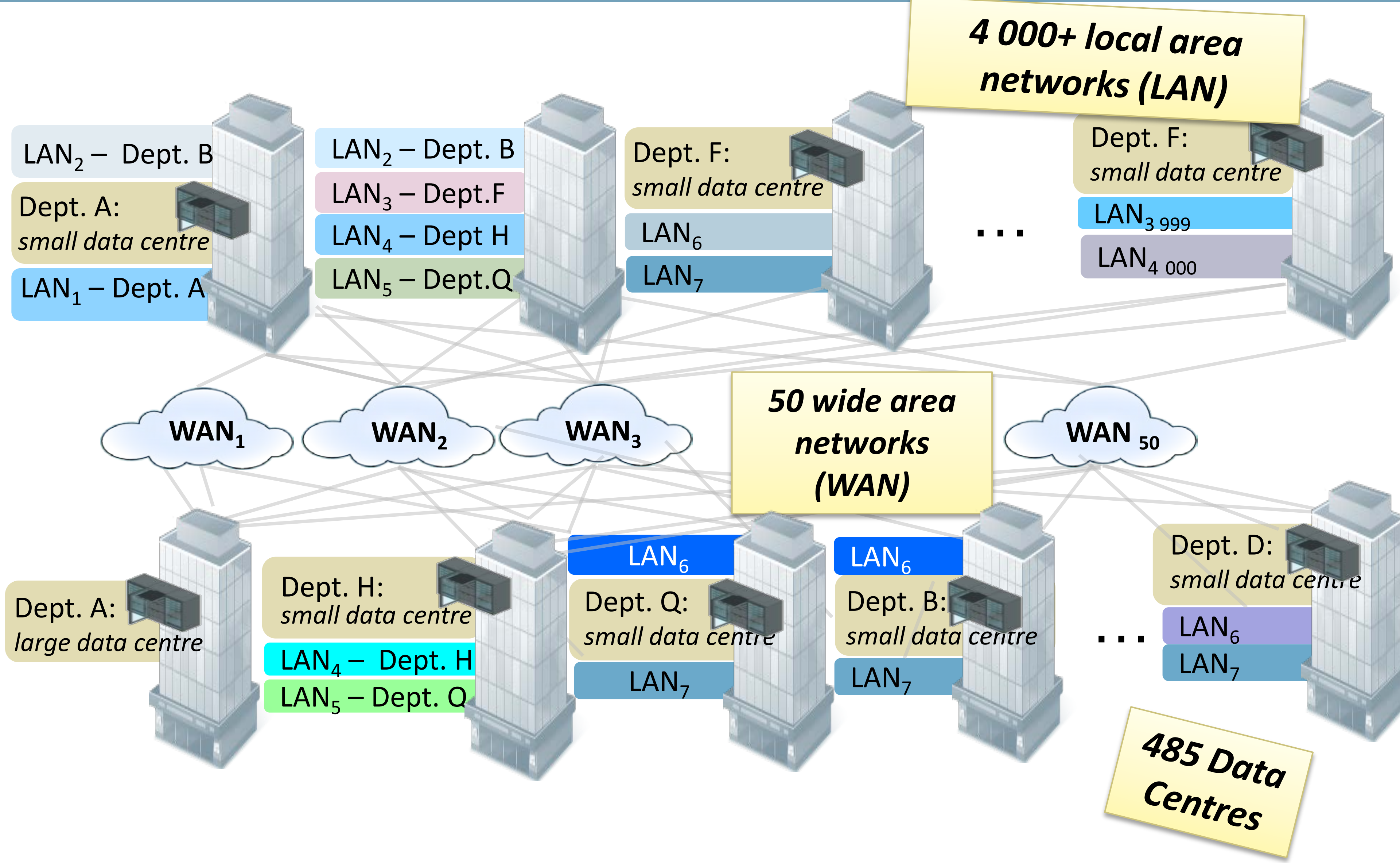
- Establish enterprise data centres and GC Network
- Build new operations organization
- Establish all ITSM tools and processes
- Build migration and receiving teams
- Perform quality control
- Assist partners in the migration of all business applications
- Install and configure new infrastructure
- Close (“shred”) data centres as they are vacated

STEP 3 - PLANNING

- Define organization structure
- Define migration and receiving teams
- Develop HR Management and Talent Plans
- Project-ize by priority
- Align network consolidation plan with data centre and application migration requirements

SSC Transformation Overview

Current State of Buildings, Networks and Data Centres



4 000+ local area networks (LAN)

LAN$_2$ – Dept. B

Dept. A:
small data centre

LAN$_1$ – Dept. A

LAN$_2$ – Dept. B

LAN$_3$ – Dept.F

LAN$_4$ – Dept H

LAN$_5$ – Dept.Q

Dept. F:
small data centre

LAN$_6$

LAN$_7$

. . .

Dept. F:
small data centre

LAN$_{3\ 999}$

LAN$_{4\ 000}$

WAN$_1$

WAN$_2$

WAN$_3$

50 wide area networks (WAN)

WAN $_{50}$

Dept. A:
large data centre

Dept. H:
small data centre

LAN$_4$ – Dept. H

LAN$_5$ – Dept. Q

LAN$_6$

Dept. Q:
small data centre

LAN$_7$

LAN$_6$

Dept. B:
small data centre

LAN$_7$

. . .

Dept. D:
small data centre

LAN$_6$

LAN$_7$

485 Data Centres

SSC Transformation Overview

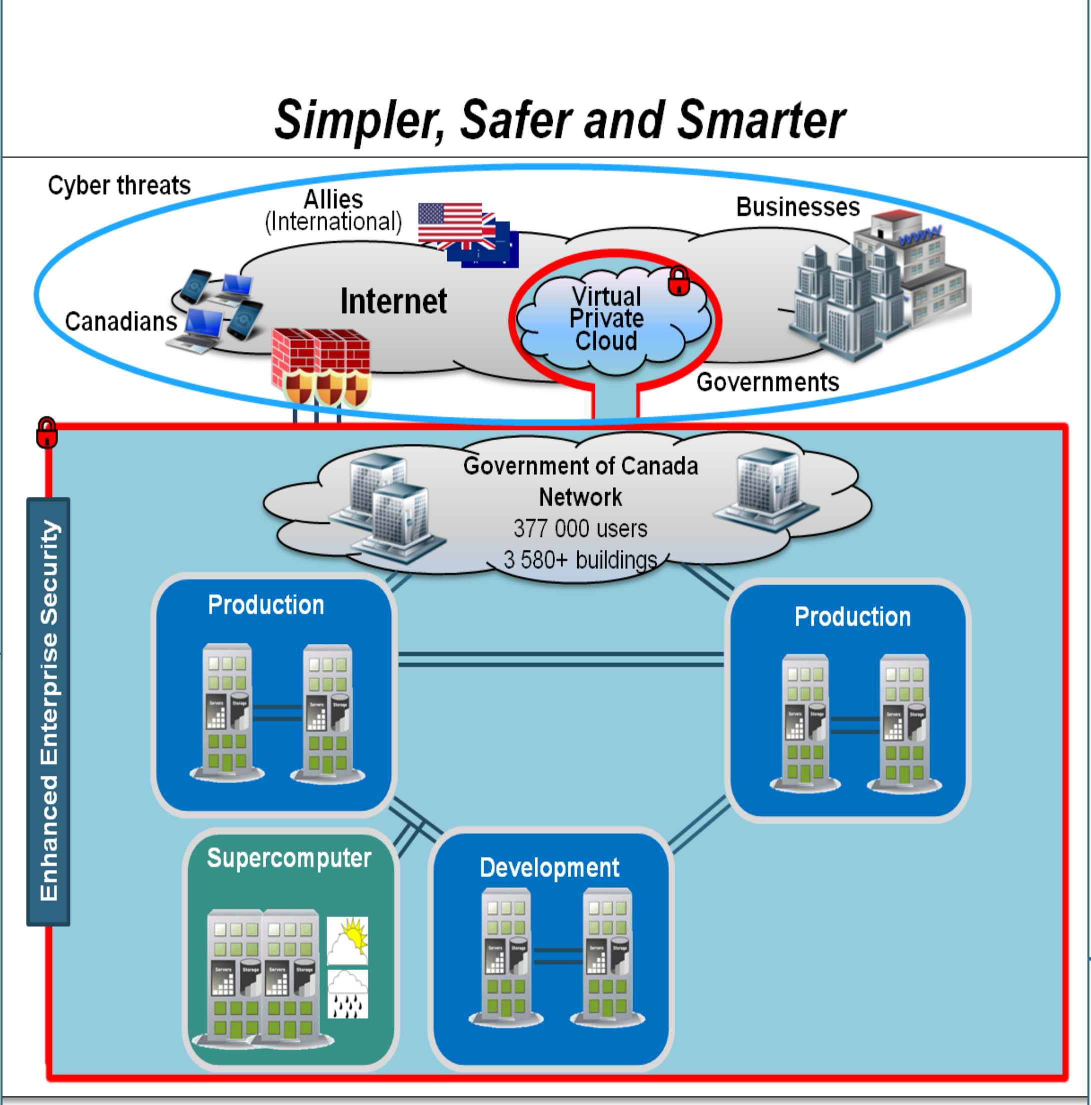
Target End State

Security

- All departments share one enterprise/common zone
- Access to sensitive departmental data is secured through restricted zones
- Developers do not have access to production infrastructure
- Classified information below Top Secret
- Consolidated, controlled, secure perimeters
- Balance security and consolidation
- Certified and Accredited infrastructure

Characteristics

- Integrated (single, common, secure GC network will link all service delivery points)
- High performance
- Secure
- Cost-effective
- Standardized (based on open standards, modularized design)
- Mobile (wireless technology will be maximized where cost-effective)
- Responsive and resilient



Consolidation Principles

1. As few wide area networks as possible
2. All departments share network access in multi-tenant buildings
3. Network equipment is shared
4. Telecom hubs (call managers, VC bridges) located in enterprise data centres or common points of presence
5. Inter-data centre connections should be diverse and fully redundant
6. Scalable and flexible infrastructure
7. Performance levels should be similar wherever possible
8. Contracts/services will be consolidated

Business Intent

- Business to Government
- Government to Government
- Citizens to Government

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)

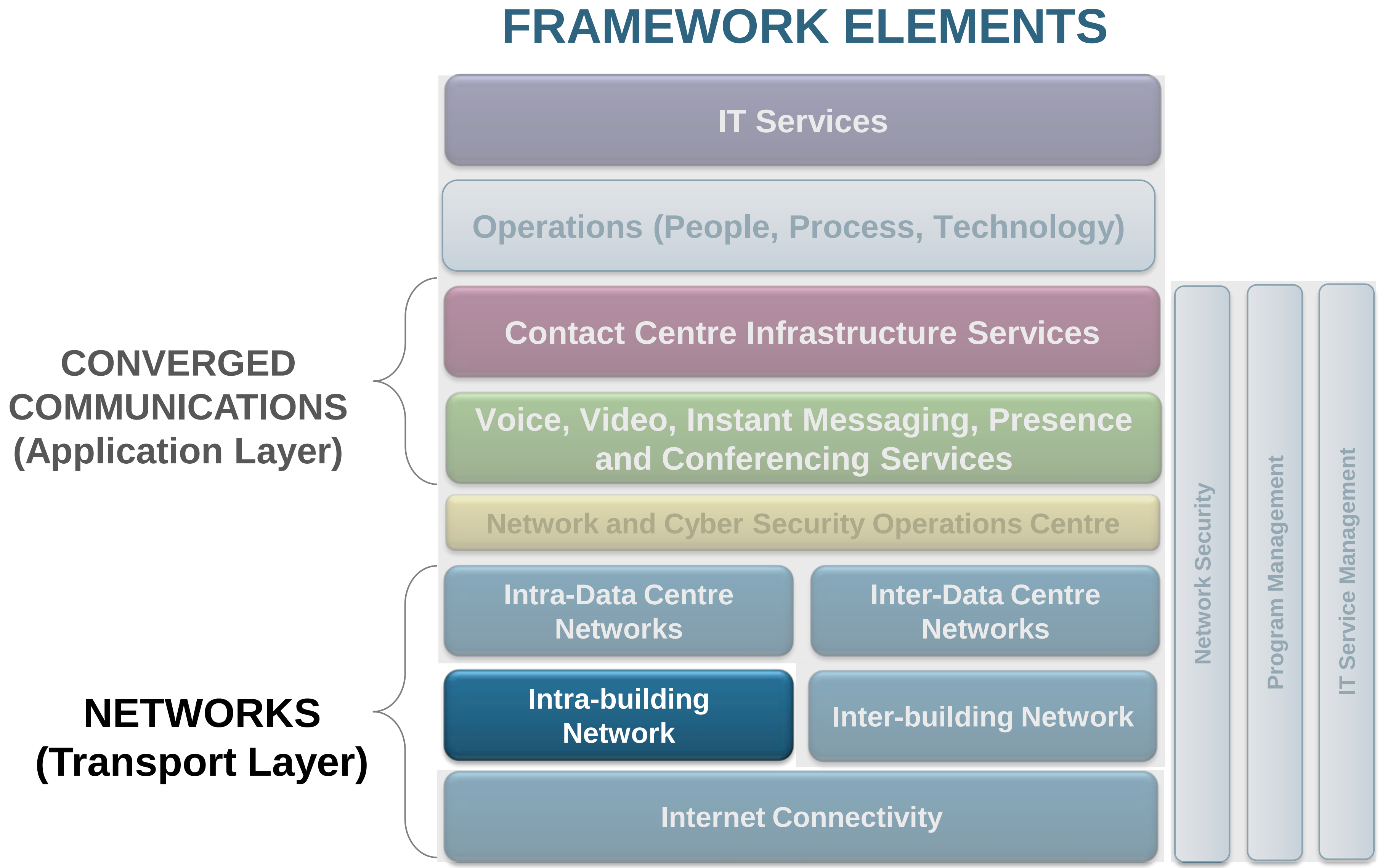
SSC Transformation Overview

Functional Requirements

- **Supplier diversity for Local Area Networks**
- **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)

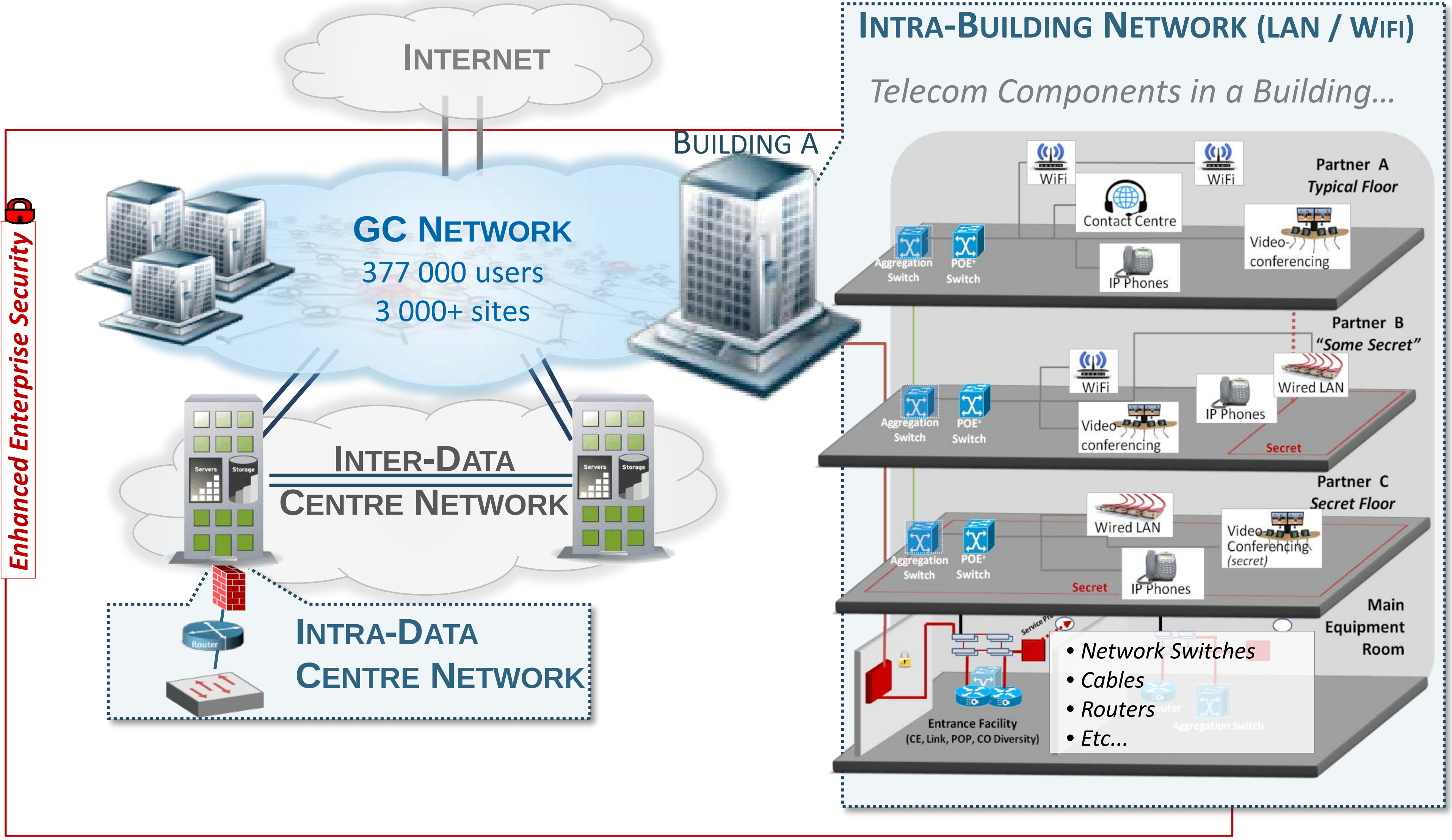
SSC Transformation Overview

Telecom Transformation Program Conceptual Framework


FRAMEWORK ELEMENTS
IT Services
Operations (People, Process, Technology)
CONVERGED COMMUNICATIONS (Application Layer)
Contact Centre Infrastructure Services
Voice, Video, Instant Messaging, Presence and Conferencing Services
Network and Cyber Security Operations Centre
NETWORKS (Transport Layer)
Intra-Data Centre Networks
Inter-Data Centre Networks
Intra-building Network
Inter-building Network
Internet Connectivity
Network Security
Program Management
IT Service Management

SSC Transformation Overview

Telecom Transformation Program Components

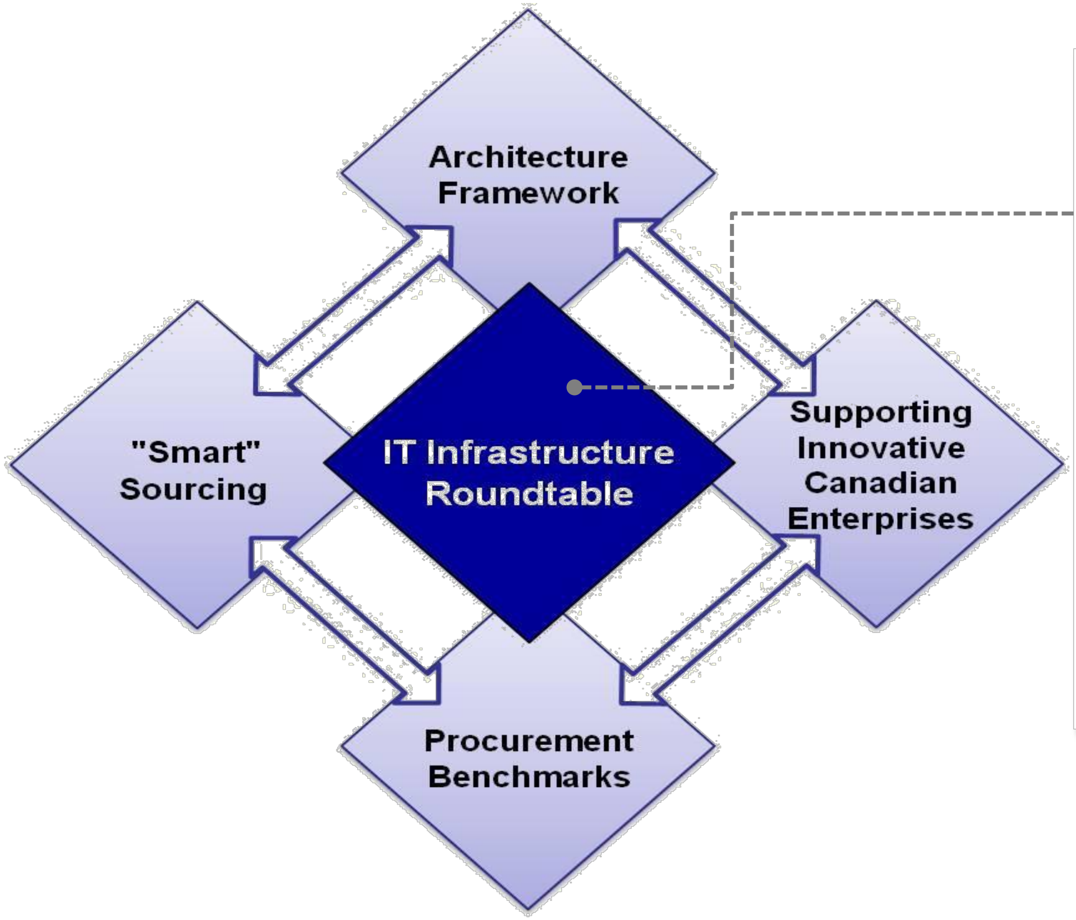


- *Network Switches*
- *Cables*
- *Routers*
- *Etc…*

SSC Transformation Overview

Engagement - IT Infrastructure Roundtable and Advisory Committees

- SSC recognizes the value and contribution of the Information and Communications Technology (ICT) sector, and the important role that sector can play in the transformation of the Government of Canada's IT infrastructure


Architecture Framework
"Smart" Sourcing
IT Infrastructure Roundtable
Supporting Innovative Canadian Enterprises
Procurement Benchmarks

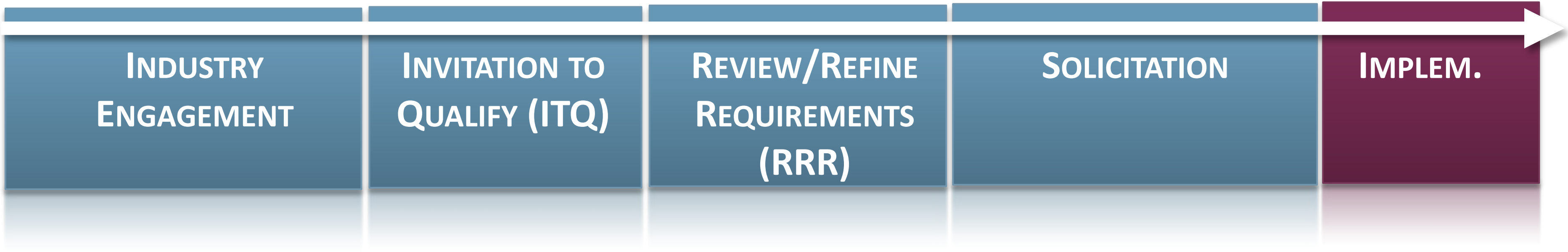
- *The ITIR is a forum that SSC uses to harness the benefits of a diverse and innovative supplier community to build a secure, lower-cost, more effective technology platform for the Government of Canada*
- *ITIR discussions focus on the government's long term IT transformation agenda, emerging technologies in the marketplace, and first-use technologies*

SSC Transformation Overview

Network Solutions Supply Chain - Engaging Industry for Feedback

- SSC also engages industry for feedback throughout the collaborative procurement process, which will result in:
  - A balance of industry capability with cost effectiveness
  - Provide suppliers with the opportunity to share their knowledge with the Government of Canada on key discussion topics
  - Allow for an exchange of information through written response with telecommunications experts that will ultimately inform telecommunications transformation strategies and procurement planning

PHASES OF THE COLLABORATIVE PROCUREMENT PROCESS



INDUSTRY ENGAGEMENT

INVITATION TO QUALIFY (ITQ)

REVIEW/REFINE REQUIREMENTS (RRR)

SOLICITATION

IMPLEM.

SSC Transformation Overview

Wrap Up and Questions

Questions?

(for suppliers only)

Service | Innovation | Value

TELECOMMUNICATIONS TRANSFORMATION PROGRAM
Network Solutions Supply Chain (NSSC) Industry Day

Overview

Michel Fortin

Director General

Telecommunications Transformation Program

Transformation, Service Strategy and Design

May 28 2014

Shared Services Canada Services partagés Canada

Canada

Objectives of Industry Engagement

- Determine the best strategy / approach to :

1. Support intra-building network transformation of wired and wireless (Wi-Fi) infrastructure and services

2. Maintain the existing network equipment and services as transformation proceeds

- Highlight strategies and considerations for future service provision of these services
  - Strategies for Procurement Vehicles (sourcing and supply methods)
  - Consolidation and Migration Strategies
  - Bundling of products/solutions/services
  - Consideration for including additional services

- Solicit input and feedback on key questions

1 Transforming Intra-Building Network Services

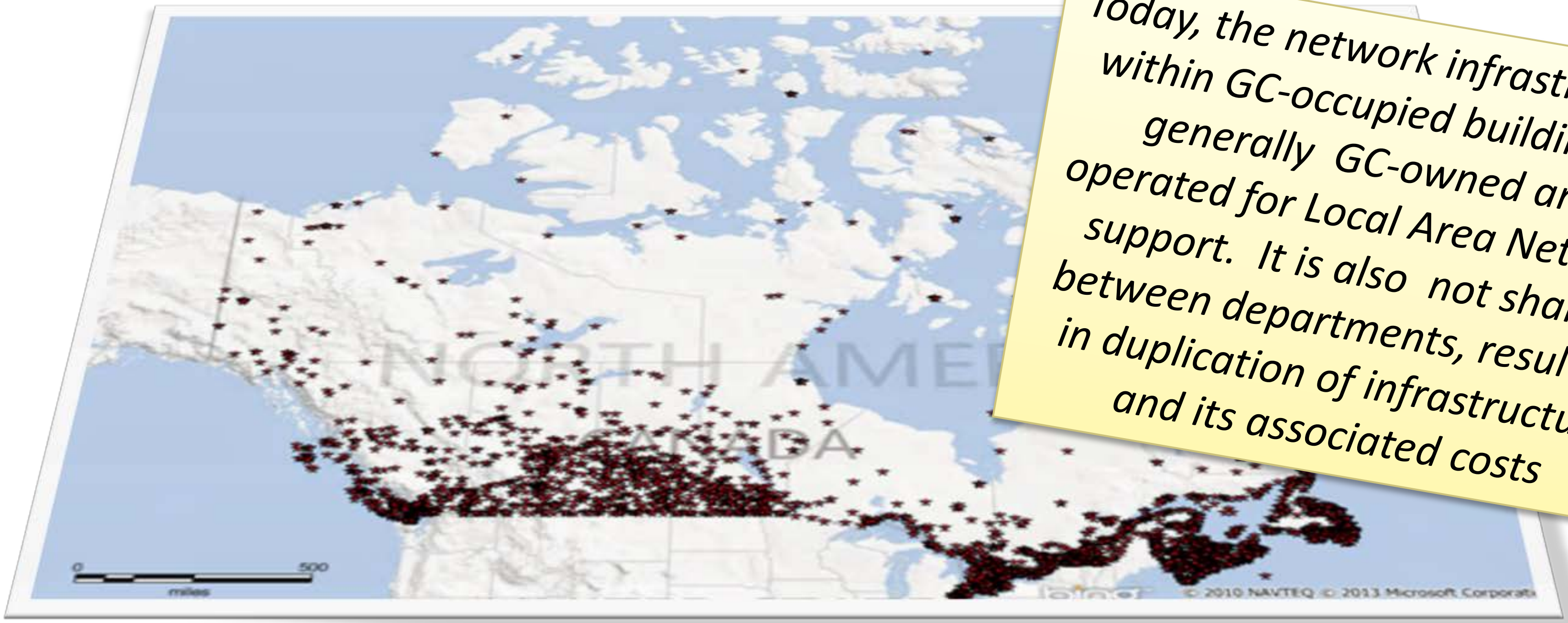
Strategic Context

- SSC will be transforming network infrastructure in buildings at more than 3,580 sites nationally and internationally

INTRA-BUILDING CURRENT STATE

▶ **3580+ Sites** ▶ **495 multi-tenant buildings** ▶ **4000+ Local Area Networks**

(61 "large" buildings (1000+ pop))



Today, the network infrastructure within GC-occupied buildings is generally GC-owned and operated for Local Area Network support. It is also not shared between departments, resulting in duplication of infrastructure and its associated costs

Intra-building Network Components

The components of the Intra-building network transformation are:

Wired LAN Service

- Shared and modernized infrastructure at 495 multi-tenant buildings will be consolidated
- Simplified support and management

WiFi Network & Service

- Improved employee mobility / productivity & supports Blueprint 2020
- Supports voice, video and data
- 80% of user will have WiFi access by 2020

Cabling Service

- Wired infrastructure – will continue to be required for vertical cabling, data centres, wireless access points and connections requiring wiring

In scope for Network Solutions Supply Chain (NSSC)

Out of scope for NSSC

Current State – Network Equipment Support Services

The Network Equipment Support Services (NESS) standing offer is used to procure **new network equipment and support services** (including a one-year warranty and optional installation) from qualified offerors for the following classes of equipment:

Each “call up” against NESS is on a per category basis

1.0	**LAN Switches**
2.0	**Routers**
3.0	**Layer 4-7 Devices** (application switches)
5.0	**Intrusion Detection Systems**
6.0	**VPN Appliances**
7.0	**Optical Networking Devices**
8.0	**Multi Class Equipment** (unified threat management network equipment)
9.0	**Wireless Systems**
10.0	**Intrusion Prevention System**
11.0	**Uninterruptible Power Supply**
12.0	**Common Requirements** (across all classes)

Note: Class 4.0 Firewall was deleted and is incorporated within 8

Current State – Network Infrastructure Management Services

- Network Infrastructure Management Services (NIMS) standing offer is used to procure the **maintenance of network hardware and software** in the following areas:
  - Network Equipment
  - Multi-Functional Devices
  - IT Security Equipment
  - Application / Software
  - Specialized Device

All classes of NESS are included within NIMS, but NIMS is limited by the subset of OEMs that are qualified offerors

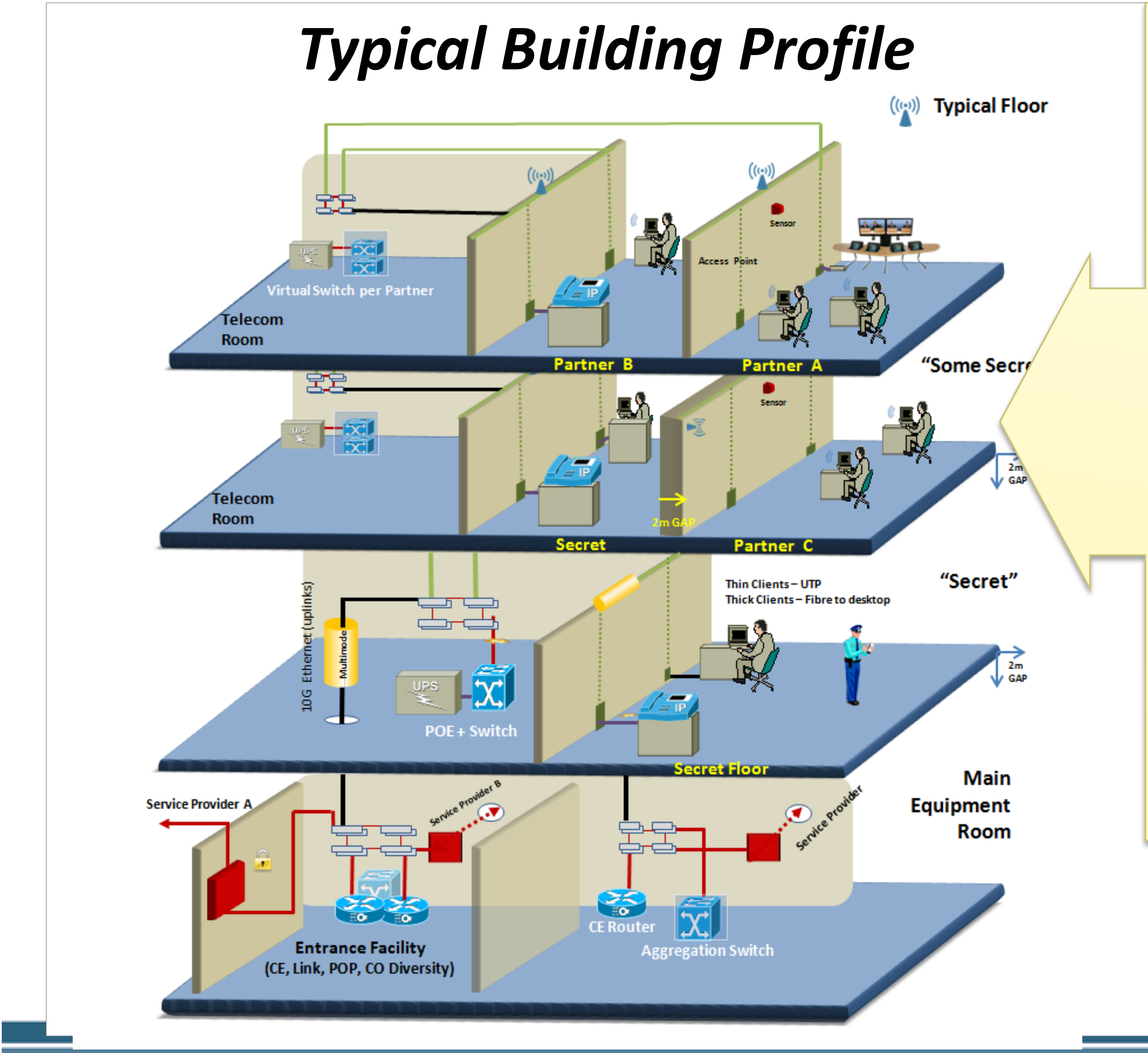
- Maintenance services include the necessary hardware, software and resource support for the **fault restoration, ongoing functional operation and preventative maintenance** of products; 3 types of maintenance plans:

1 REPLACEMENT:
Offeror is required to **acquire and deliver the replacement component** to a technical contact in an identified timeframe

2 ON-SITE REPLACEMENT:
Offeror is required to **acquire / deliver and install the replacement component on-site or undertake whatever maintenance** and repair service that is necessary to restore the product to operational service

3 RETURN TO DEPOT:
Offeror is required to **receive** the faulty product, **repair or replace** the product and **ship** the repaired or replaced product back to the site

Target State - Building View



Typical Building Profile

General profile

- Combination of wireless and wired infrastructure
- Some buildings will have SECRET systems (require more cabling and limit WiFi)
- Multi-tenant buildings will share network equipment
- VoIP (hard and soft phones) and/or cellular/smartphones
- Desktop videoconferencing
- Sharable VC rooms

Key Challenges – Network Solutions

KEY CHALLENGES

- Existing NESS does not support transformation well because it is equipment-specific as opposed to solutions oriented
- Too many different items in the catalogue
- Interoperability is challenging between multiple OEMs (ie. OEMs implement customized “open standards” which are not always interoperable with other OEMs without loss of functionality)
- Standards are used differently across many networks
- Consolidation of partner / business domains with differing security and privacy considerations
- Support to remote and international locations
- Executing transformation while maintaining the existing infrastructure and services

Guiding Principles – Network Solutions

Guiding Principles

- Technology based **open architecture** and **industry standards** to ensure **flexibility and interoperability** between existing and future services
- Must be **scalable** and **future-proof** (e.g. support Software Defined Network framework)
- Must support **multi-tenancy** (traffic isolation differentiated by partner) and secure, controlled access to data
- Must support **centralized management**, **configuration** and **reporting**
- Must ensure information is handled using the appropriate controls, protocols and infrastructure to support the **required level of security**
- Network must support a **self-serve model** for data centre services
- Provide **best value** and **total cost of ownership (TCO)** for the operations and management of services

2 Maintaining Existing Network Services and Equipment

Maintaining Existing Network Services and Equipment

CURRENT STATE

- To ensure ongoing support of GC Department and agencies, the existing network infrastructure must be maintained during transformation
- Existing supply arrangements (e.g. NESS) are used to maintain existing network and IT security infrastructure (including Top Secret)
- Supply arrangements support all of Government of Canada
- Ongoing requirement to procure network and IT security products and services
- NESS and NIMS will be replaced with procurement vehicles which will support transformation

High Level Requirements

- Provide the ability to procure the following classes of network products/components and/or services:
  - Wired Switches
  - Wireless Networking
  - Routers
  - Application Delivery Networking Products
  - Optical Networking Devices
  - Network Monitoring and Management
  - Specialized Networking
  - Firewalls, *including Deep Packet Inspection*
  - Forward and Reverse Proxy
  - Intrusion Detection and Prevention, *including network, host & wireless*
  - URL and Content Filtering, *including whitelisting, blacklisting*
  - Anti-Virus / Malware / Spyware
  - Anti-Spam / Anti-Phishing
  - Link Layer Security/VPN (IPSec, SSL, TLS)
  - Data Loss Prevention
  - Vulnerability Assessments
  - Network Forensics & Analysis

Considerations

CONSIDERATIONS

Ensure support for:

- Varying service levels across SSC partners and clients
- Partner and client specific Security Requirements (e.g. Public Safety, Correctional Services, National Security)
- High availability and fault tolerant standards must be maintained, with minimal downtime for maintenance schedules, to ensure continuous levels of service for mission critical applications
- Network Access Control, Network Encryption Layers, Network Policy Management
- Virtualized environments
- Malware execution in Advanced Persistent Threat Detection (APTD),including detection of DNS-based malware

KEY DISCUSSION TOPICS AND QUESTIONS FOR INDUSTRY FEEDBACK

Strategies for Procurement Vehicle

Discussion Topic 1

SSC is trying to determine the **strategy** that will provide the **best value** and **lowest total cost of ownership** (TCO) for the GC to deliver transformed Intra-Building network services while maintaining existing network services and providing standard levels of service.

Factors to consider for Procurement Vehicles:

A Sourcing Strategy:

- Out-source *(fully managed)*
- Hybrid
- In-Source

B Supply Method:

- Supply Arrangement (SA)
- Standing Offer (SO)
- Contract

C Supplier Strategy:

- Worldwide
- By region
- Varies by site

D Product (HW/SW) Sourcing Method:

- Buy
- Lease
- Bundled with services

E Procurement Considerations

Variation by OEM ?

- One for all categories
- One per category *(LAN, WiFI, etc.)*

Variation by Geography?

- Nationally/ Worldwide
- By region
- Varies by site

A Sourcing Strategy

Discussion Topic 1

1. What are the **benefits, technical challenges**, **requirements** and **recommended pricing model** for successful deployment and ongoing support of each deployment model?

2. Which sourcing strategy would you recommend?

Outsourced / Fully Managed

Third parties design, provide and operate the solution(s) through a managed service

EXAMPLE:
Vendor provides the end-to-end network solution based on the requirements provided

Co-Managed / Hybrid

SSC in-house resources deliver parts of the service on GC-owned infrastructure while the remainder is delivered by a third party vendor

EXAMPLE:
Vendor A provides the design, Vendor B provides the equipment / infrastructure and SSC in-house resources operate

In-sourced / In-House

Design and deliver the solution by in-house SSC resources using SSC acquired infrastructure components

EXAMPLE:
Buy the equipment / infrastructure, and SSC in-house resources build and operate solutions

B Supply Method

Discussion Topic 1

1. What supply methods would you recommend to support intra-building network transformation, and why?
2. If contract, what contract period would you recommend ?

Contract

- **A voluntary, deliberate, and legally enforceable agreement** between two or more competent parties
- Each party to a contract acquires rights and duties relative to the rights and duties of the other parties

Standing Offer

- **An offer from a potential supplier to provide 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" against the standing offer.
- The government is under no actual obligation to purchase until that time

Supply Arrangement

- **A method of supply to procure goods and services**
- Not a contract and neither party is legally bound as a result of signing a supply arrangement alone
- Includes a set of predetermined conditions that will apply to bid solicitations and resulting contracts
- Allows government to solicit bids from a pool of pre-qualified suppliers for specific requirements

Source: "An Introduction to procurement "manual and *https://buyandsell.gc.ca/*

C

Supplier Strategy

Discussion Topic 1

1. Which supplier strategy would you recommend?: (ie. a single supplier nationally, by region or by site? or continuation of a model with potentially varying resellers/OEMs for each procurement of products?
2. What are the pros and cons of each option?

WORLDWIDE/NATIONAL

One prime supplier to transform all sites worldwide

SUPPLIER BY REGION

Suppliers will transform the sites within respective regions

SUPPLIER BY SITE

A site could be:

- *Campus*
- *Military base*
- *DCN*
- *Remote sites*
- *Etc.*

Allows suppliers to vary by site based on site requirements and complexity (e.g. small, medium, large sites)

D Sourcing Method

Discussion Topic 1

There are various sourcing methods available including leasing/procuring managed services, buying or leasing products with in-house services:

1. Which categories do you recommend that we lease services rather than buy/lease products and perform services in-house?

2. In the case that products are acquired do you recommend that they be bought or leased? Why?

3. What are the pros and cons of each option: **buy** vs. lease vs. bundle with services?

LEASE SERVICES VS BUY PRODUCTS ? VS LEASE PRODUCTS? VS BUNDLE PRODUCTS WITH SERVICES? *(BUY ENTIRE SOLUTIONS)*

E

Procurement – OEM Considerations

Discussion
Topic
1

Products/solutions can be procured or leased from a single or multiple OEMs:

1. For each service category (eg. Wired LAN, WiFi, etc), do you recommend that products/solution sets be procured entirely from the same original equipment manufacturer(OEM)?
2. In the case of multiple OEMs, which types of solutions/products (eg. LAN switches, routers, etc) will be easy/challenging to integrate between various manufacturers' products? Which industry standards should be adopted to improve interoperability?

Single Original Equipment Manufacturer (OEM)
("Uniform")
by Service Category

VS

Multiple Original Equipment Manufacturers (OEMs)
("Best in Class")
by Service Category

E

Procurement – Geographical Considerations

Discussion Topic 1

Products, solutions and services can be procured for all locations, by region or even by site:

1. For each solution/service type, which model would you recommend (i.e. procure the same solution set/service provider for all locations, for each region or for every site? Why ?
2. Should products and/or services international locations be procured separately?

Options	Region X		Region Y		Etc…
	Building 1	Building 2	Building 3	Building 4	Building X
All locations	OEM **A**	OEM **A**	OEM **A**	OEM **A**	OEM **A**
Supplier by Region	OEM **A**	OEM **A**	OEM **B**	OEM **B**	OEM **X**
Supplier by Site	OEM **A**	OEM **B**	OEM **B**	OEM **C**	OEM **X**

Consolidation and Migration Strategies

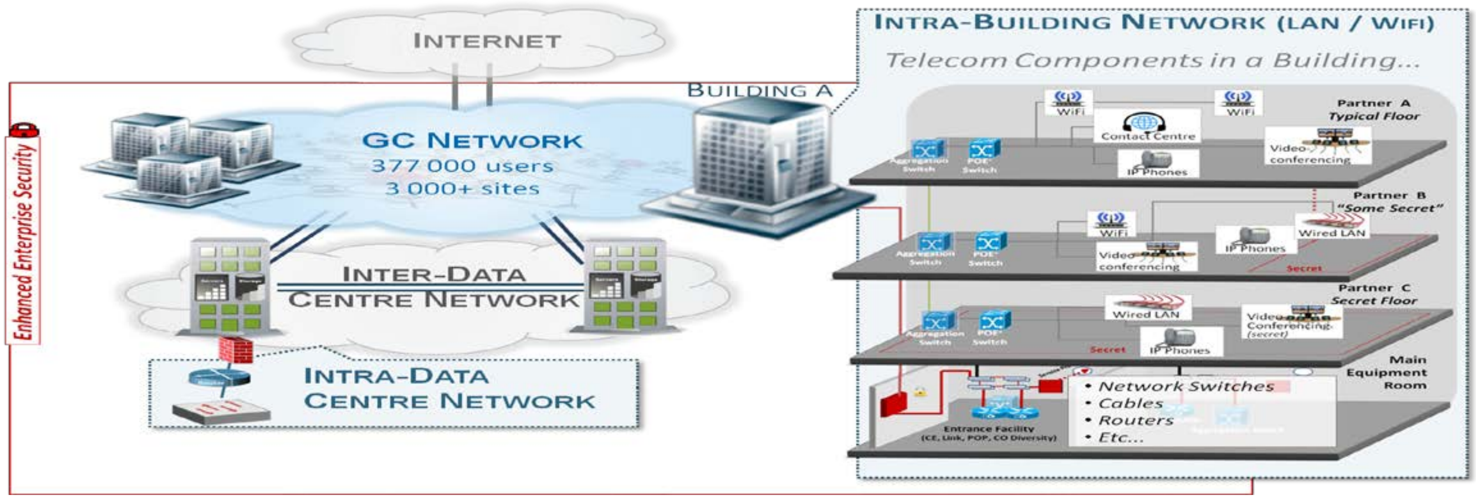
Discussion Topic 2

SSC will be using a building-by-building approach for telecommunications services delivered inside buildings (eg. network, voice and videoconferencing services)

Are there strategies that you would recommend to:

1. Minimize user disruption and maximize resource efficiency during the roll out phase of these initiatives?
2. Are there migration strategies which you would recommend to migrate and consolidate the various partner domains (workload migration, overlapping network addressing, etc.) particularly within a multi-tenant environment?

HOW THE TELECOMMUNICATIONS COMPONENTS FIT TOGETHER



Bundling of Products/Solutions/Services

Discussion Topic 3

There are many products, solution sets and/or services which could be bundled together.

1. Which products, solutions and/or services would you recommend bundling together? (e.g. should routers and firewalls be bundled together) Why ?
2. Should network and security products be procured together?
3. In the case where product/solutions are procured, should maintenance (beyond the warranty period) be bundled together or procured separately?

Considerations for including additional services

Discussion Topic 4

- Recently, SSC held an Industry Engagement on Inter and Intra Data Centre Network services, to gather valuable feedback on the approach for delivering the DCN services

- Based on the feedback received, SSC is considering the option of including the Inter and Intra DCN services within the scope of the NSSC procurement vehicle, to **enable the flexibility of defining a hybrid model**

- Should NSSC procurement vehicles include products/solutions related to Data Centre Networks or should these be procured separately ?

- Should other categories of products such as videoconferencing products be included in NSSC? If so, which ones would you recommend including ?

Health Break

Key Questions for Industry Feedback

STRATEGY

SSC is **seeking a strategy** that will enable the GC to cost-effectively deliver transformed Intra-Building network services. The following are areas of consideration:

A. **Sourcing Strategy**: What is the recommended sourcing model for intra-building network services (**Out-sourced service, Hybrid or In-sourced**)? What are the benefits, technical challenges, requirements and recommended pricing model for successful deployment and ongoing support of each deployment model?

B. **Open Standards:** Which standards should be adopted to ensure interoperability between different OEMs? Which ones should be avoided ? Are there areas where interoperability between OEM products is challenging ? Are there situations where a single OEM model would be recommended? Which type of equipment where OEM variation could be considered by region/site? What are the integration/interoperability implications of each option?

Key Questions for Industry Feedback (continued)

C. **Bundling:** Which services or group of products should be bundled together when procuring a solution? Should other areas such as videoconferencing end-points and data centre networks be bundled in or kept in separate procurement vehicles?

D. **Buy vs Lease:**
Should the products/services be procured or leased? What are the pros and cons of each option: **buy** vs. **lease** vs. bundle with services?

E. **Supplier Strategy**: What supply method would be optimal to achieve best value/lowest TCO and interoperability? Should certain products/solutions be bundled into a single contract/supplier/service provider over a long period (ie. years) ? If so, for how long? Should this be separated by region? For services, should single or multiple service providers be considered? What are the pros and cons for each option?

F. **Transformation Strategy**: What are some key considerations/strategies in consolidating networks? What procurement strategies were used in these cases? (i.e. integrators, service providers, buy/lease. Provide examples, use cases, white papers, etc.

Additional Questions for Industry Feedback

OPERATIONAL/TECHNICAL:

1. What support model would you propose for a site once it has been transformed, considering both the multi-tenant and single tenant site?

2. What are the strategies, technical considerations and challenges for ensuring smooth integration with Integrated Command Centre (DOC/NOC/SOC) and other enabling foundational services (DNS, DHCP, ICAM, etc.)?

3. What are the possible technology or service enhancements over the coming years that we may need to consider in our requirements? How can emerging trends/technologies be incorporated into the proposed solutions? How can we keep technologies up to date given the length of transformation? How could they contribute to the Savings, Security and Service objectives?

Additional Questions for Industry Feedback *(continued)*

OPERATIONAL/TECHNICAL:

4. What value-added services would you recommend that we should be incorporating? For example Videoconferencing services and Data Centre Network services (Inter & Intra) be bundled within the same procurement vehicles as those related to Network Solutions Supply Chain.

5. What are the perceived barriers to success and risks that require mitigation strategies?

6. Please provide strategies/input on how SSC could best achieve the use of current generation products and future generation products throughout the lifetime of the procurement vehicle(s).

Additional Questions for Industry Feedback *(continued)*

OPERATIONAL/TECHNICAL:

7. How should SSC approach product substitutions in future procurement vehicles?

8. Notwithstanding the requirements that have been identified today, please provide insight and advice on how to best ensure ongoing manufacturer supply chain integrity.

9. Please provide your views how to best integrate network security into the proposed solutions/services, while keeping aligned with technological enhancements that address the evolving threat landscape?

Additional Questions for Industry Feedback *(continued)*

PROCUREMENT:

1. What strategy would you propose to improve procurement and lower costs?

2. SSC recognizes that many different pricing models can be used to achieve value to the Crown. Given the requirements outlined, please suggest various pricing models that could be used for the different sourcing options.

3. Should future procurement vehicles include categorization as currently exists within the Network Equipment Support Services (NESS) procurement vehicle or should a solutions-based approach be pursued? What approach would you propose for future procurement vehicles?

Additional Questions for Industry Feedback *(continued)*

PROCUREMENT:

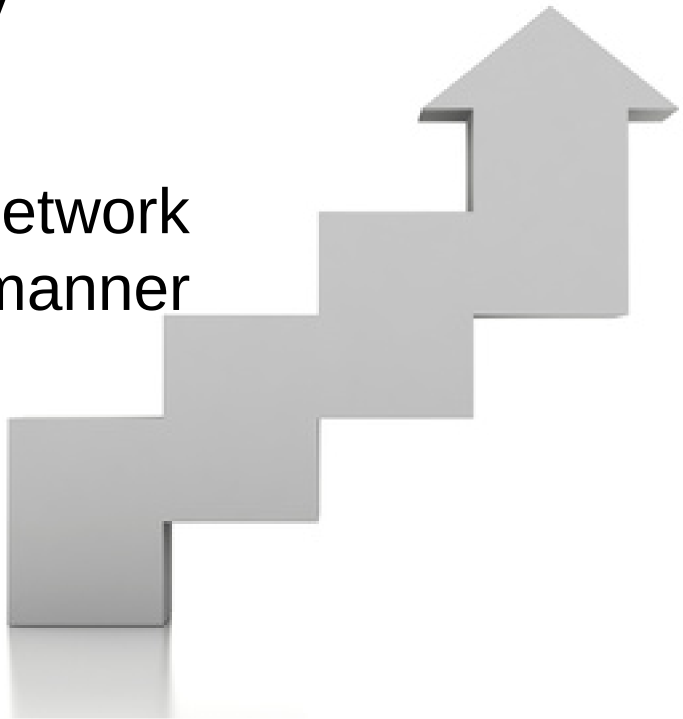
4. Provide recommendations for requirements to maximize competitiveness and reduce the TCO. What are the factors that drive rates up?

5. What are the industry standards for wired and wireless services should be included as part of requirements in future procurement vehicles?

6. Should products/services for international locations be procured separately? If so, why?

Next Steps

- Industry feedback on discussion topics and questions to be received by June 13, 2014
- Evaluate input / feedback received to refine procurement and sourcing strategy
- Proceed with the procurement of network solutions supply chain in a timely manner



Wrap Up and Questions

Questions?

(for Suppliers only)

Network Solutions Supply Chain (NSSC)

Collaborative Procurement Solutions Approach

Tom Mercer

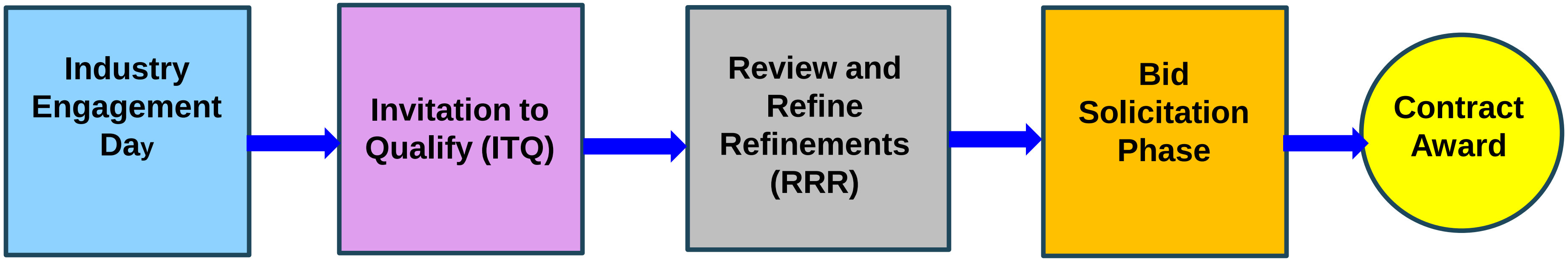
Shared Services Canada

Manager

Procurement and Vendor Relationships Directorate

May 28, 2014

Collaborative Procurement Solutions Approach


Industry Engagement Day
Invitation to Qualify (ITQ)
Review and Refine Refinements (RRR)
Bid Solicitation Phase
Contract Award

Invitation to Qualify (ITQ)

Invitation to Qualify (ITQ) Phase

- The purpose is to qualify suppliers who have demonstrated and proven skills and experience in implementing and providing network solutions that will support the transformation and maintenance of wired local area networks (LANs) and wireless LANs (Wi-Fi) and other supporting telecommunications equipment and services.
- Evaluation criteria will focus on the supplier’s capabilities and experience to deliver NSSC services.
- Suppliers who meet the mandatory ITQ evaluation criteria will be deemed successful “Qualified Respondents” (QRs) and will proceed to the RRR phase.
- Canada will inform Qualified Respondents that, in the “Review and Refine Requirements Phase”, a draft Statement of Work (SOW) will be provided to them and at that time.

Review and Refine Requirements (RRR)

Review and Refine Requirements (RRR) Phase

- Canada will provide the Qualified Respondents with a draft RFP(s).
- Canada will interact with Qualified Respondents to seek feedback and clarification on Canada’s requirements to refine the RFP(s) (e.g. workshops, one-on-one sessions, Q’s and A’s).
- A Supply Chain Security Information (SCSI) assessment will also be started during this stage.

Bid Solicitation Phase

Bid Solicitation Phase

- Canada may issue one or more formal Request for Proposal(s) (RFP(s)) to the Qualified Respondents who have participated in the ITQ and RRR Phases
- Each Qualified Respondent will be permitted to formally bid on the requirements set out in the RFP(s).

Contract Award

Contract Award and Implementation

- Contract Award will occur after completion of the Bid Solicitation Phase
- One or more contracts may be awarded depending on the Request for Proposal(s)

Cyber & Supply Chain Threats to the GC

Network Solutions Supply Chain
Industry Day

May 28, 2014

Brad McInnis

Communications Security Establishment

CSE: What We Do

- CSE: 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

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 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 GC departmental networks threatens the sovereignty of GC information and the continuity of government operations
  - Cyber threat actors are effective at exploiting inter-connected network element technologies and management systems used to administer and operate network infrastructures (i.e. Mandiant APT1 Report)
- **Risks from an overly complex and decentralized threat surface**
  - Consolidation of GC networks 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

Service | Innovation | Value

Supply Chain Integrity (SCI)

Network Solutions Supply Chain
Industry Engagement Day

May 28th, 2014

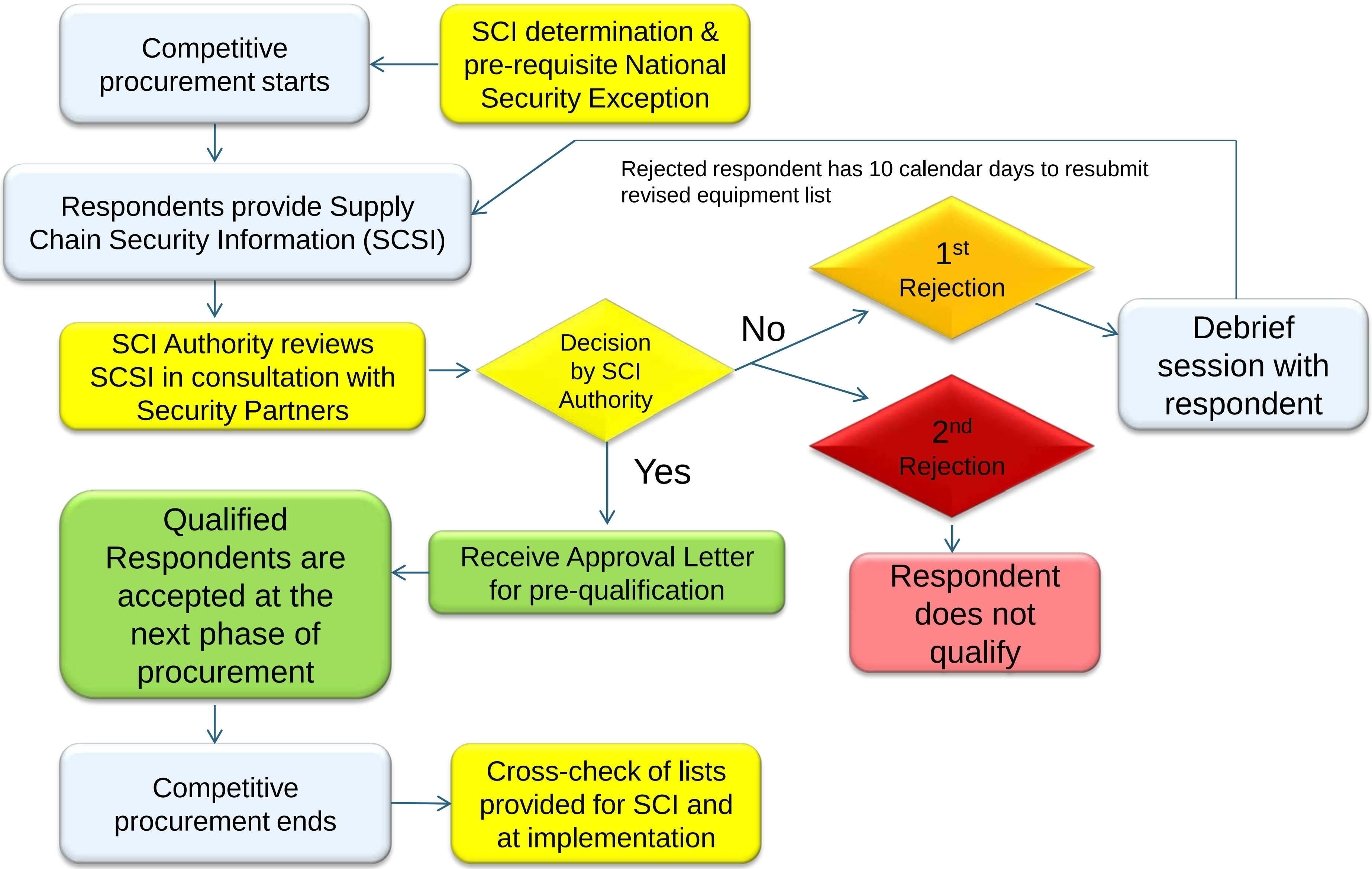
Simon Levesque
Sr. Director Planning and Design, Cyber and IT Security Transformation Program

Nature of the SCI

- ✓ The purpose of the Supply Chain Security Information (SCSI) assessment process is to ensure that no un-trusted equipment, software or services, procured by SSC, are used to deliver and/or support GC services.
- ✓ Respondents must successfully pass the SCSI assessment process in order to remain Qualified Respondents.

SCSI assessments are being applied consistently to SSC procurement activities; as a result, we can count some of these recent contracts as having verified Supply Chains: *Email Transformation Initiative, Managed Security Services, Data Centre Consolidation, and others.*

SCI in Competitive Procurement



Competitive procurement starts

SCI determination & pre-requisite National Security Exception

Respondents provide Supply Chain Security Information (SCSI)

Rejected respondent has 10 calendar days to resubmit revised equipment list

SCI Authority reviews SCSI in consultation with Security Partners

Decision by SCI Authority

No

1st Rejection

Debrief session with respondent

2nd Rejection

Yes

Qualified Respondents are accepted at the next phase of procurement

Receive Approval Letter for pre-qualification

Respondent does not qualify

Competitive procurement ends

Cross-check of lists provided for SCI and at implementation

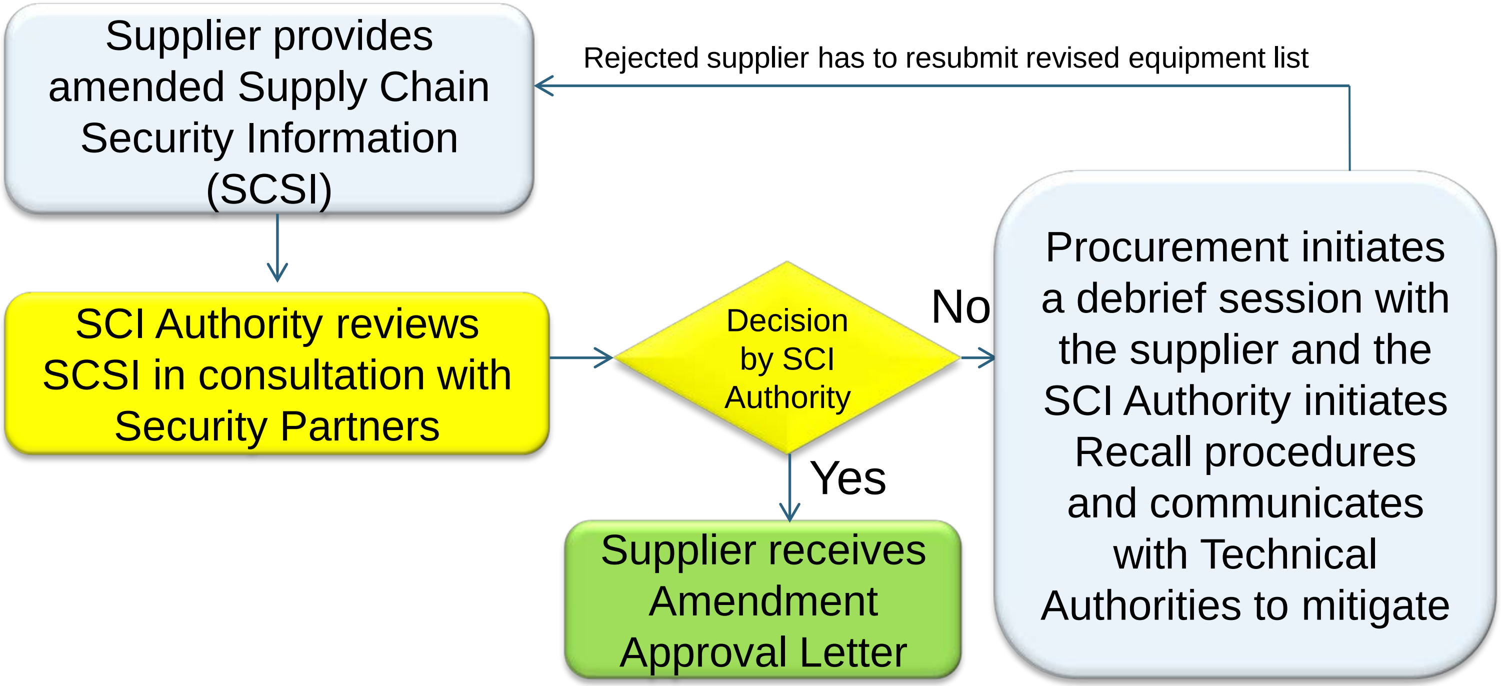
Required Information from the Respondents

- Once the SOW is finalized, GC will request that the respondents provide their Supply Chain Security Information. More specifically, when it applies, the GC will be requesting the following detailed information:

1. List of equipment used to deliver the service (vendor, manufacturer, model number, software load version).
2. List of subcontractors (names of companies and the location from where these services are delivered).
3. Network diagram.
4. All of the above applies for sub-contractors and partners (sub-contractors and their own sub-contractors). This should include all companies who will be sub-contracted to provide equipment or services as part of the project.

On-going Supply Chain Integrity Auditing

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



Supplier provides amended Supply Chain Security Information (SCSI)

Rejected supplier has to resubmit revised equipment list

SCI Authority reviews SCSI in consultation with Security Partners

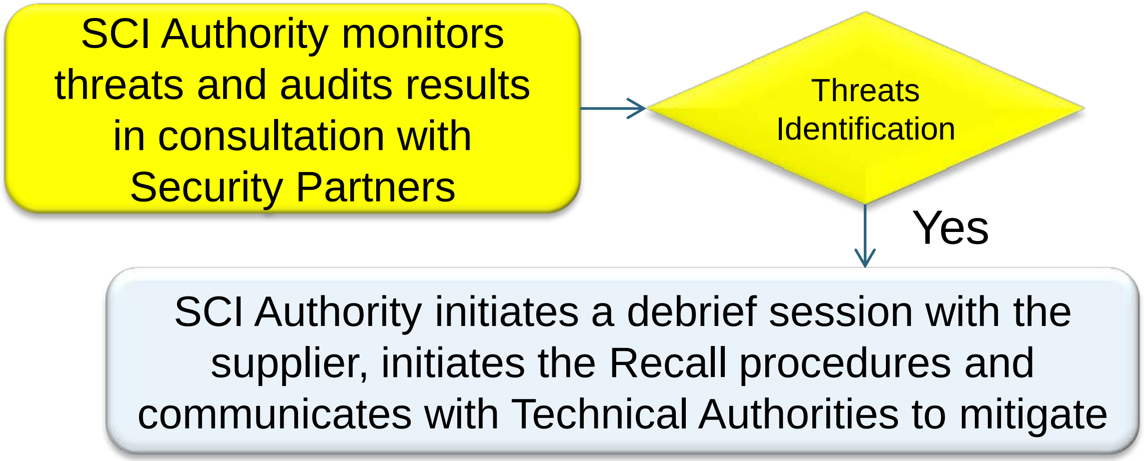
Decision by SCI Authority

No

Procurement initiates a debrief session with the supplier and the SCI Authority initiates Recall procedures and communicates with Technical Authorities to mitigate

Yes

Supplier receives Amendment Approval Letter



SCI Authority monitors threats and audits results in consultation with Security Partners

Threats Identification

Yes

SCI Authority initiates a debrief session with the supplier, initiates the Recall procedures and communicates with Technical Authorities to mitigate

Internal threat evaluation can lead to the questionning/exclusion of specific equipment/services

Networks Solutions Supply Chain Industry Day

Questions & Answers

Networks Solutions Supply Chain Industry Day

Recap / Closing Remarks