Service | Innovation | Value

Shared Services Canada (SSC)
GCNet WAN Services

Industry Day

July 9, 2013

EDRM # 1807240

Shared Services Canada | Services partagés Canada

Canada

GCNet Industry Day

Industry Day Objectives

- Share plans with industry suppliers and engage in a dialogue regarding GCNet Wide Area Network services and Service Delivery Options
- Explain the proposed “Collaborative Procurement Solutions” approach
- Address the Cyber Security Supply Chain Threat
- Elicit feedback from industry on the Service Delivery, High Availability, Contract Period and Pricing Options

GCNet WAN Services Industry Day

Agenda

TIME	PRESENTER	DESCRIPTION
1:00 - 1:05 pm	**Jean-François Lymburner** *DG Service Strategies and Transformation*	Opening Remarks & Industry day Objectives
1:05 – 1:45 pm	**Benoît Long** *SADM, Transformation, Service Strategy & Design, SSC*	SSC Transformation Overview
1:45 - 2:45 pm	**Michel Fortin** *DG, Telecommunications Transformation Program, SSC*	GCNet - Wide Area Network Overview
2:45 - 3:00 pm	***Break***	
3:00 - 4:00 pm	**Patrick Mountford** *Director, Cyber Security Strategy, Cyber and IT Security Transformation Program, SSC* **Carey Frey** *Director, IT Security Strategic Relationships Office, Communications Security Establishment Canada*	Supply Chain Integrity
4:00 - 4:30 pm	**Stéphane Richard** *Senior Director, Information Technology Procurement, SSC*	Collaborative Procurement Solutions Approach
4:30 – 4:45 pm	**Jean-François Lymburner** *DG Service Strategies and Transformation, SSC*	Questions and Answers
4:45 – 5:00 pm	**Jean-François Lymburner** *DG Service Strategies and Transformation, SSC*	Recap / Closing Remarks

Service | Innovation | Value

GCNet WAN Services Industry Day

Shared Services Canada (SSC) Transformation Overview

Benoît Long

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

July 9, 2013

EDRM # 1805230

SSC Transformation Overview

Agenda

- Industry Day Objectives / Key Messages
- SSC Background, Strategic Vision & Principles
- Transformation Objectives & Background
- Transformation Timeline & Approach
- Stakeholder Engagement
- Wrap up

SSC Transformation Overview

Industry Day Objectives / Key Messages

*" Engaging with others outside our institution—other levels of government, **industry**, academia, non-governmental organizations, and individual citizens—is also essential to our work. These diverse partners can **help to identify and implement practical, effective solutions that get results**. We need to develop our policies, programs and services with people, not just for them."*

Source: *Twentieth Annual Report to the Prime Minister on the Public Service of Canada*

- The strategic outcomes for Shared Services Canada (SSC) are to *generate savings, increase security*, and *improve service*
- Strategies to achieve these outcomes include *consolidation, standardization*, and *transformation*, including development of *sourcing strategies* and incorporating *security by design* strategies
- With regard to sourcing strategies, SSC Transformation needs to engage industry in exploring options to implement these strategies and achieve its desired outcomes

SSC Transformation Overview

Background / Context

2011 Budget

A New Organization with an IT Focus

STANDARDIZE

CONSOLIDATE

RE-ENGINEER

Raison d'être

- ✓ Reduce costs
- ✓ Improve Security
- ✓ Maximize Efficiencies
- ✓ Minimize Risks

SSC Transformation Overview

Strategic Vision and Principles

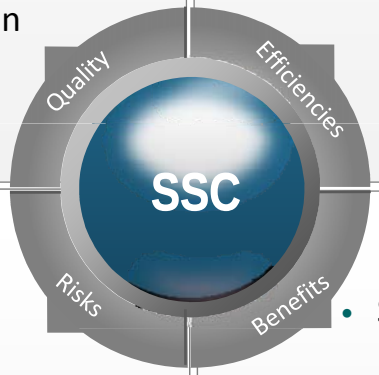
The Government of Canada will consolidate data centres and networks, transform telecommunications services, centralize their administration, and rationalize service delivery to achieve greater efficiencies, reduce costs, minimize risks, and improve security and service quality

Improve Service Quality

- Improve levels of service and security for all
- Modernize infrastructure and platforms
- Increase system availability, reliability, robustness and scalability
- Reduce dependence on physical location
- Implement ubiquitous personal mobility

Maximize Efficiencies

- Consolidate and converge to reduce duplication of infrastructure
- Standardize infrastructure and operations
  - Determine appropriate level of private sector engagement
  - Make effective use of shrinking IT labour force



Minimize Risks

- Fewer, better quality facilities
- Increase information security
- Power supply diversification
- Centralize planning and recapitalization
- Address aging IT infrastructure
- Examine industry investment and risk sharing

Additional Benefits

- Significant environmental benefits
  - Reduce power demand
  - Reduce greenhouse gas emissions (cleaner power); reduce e-waste
- Enable Workplace 2.0
- Reduce travel costs (videoconferencing)

SSC Transformation Overview

Transformation Objectives

SAVINGS

Transformation will realize material cost savings and avoid future costs.

SERVICE

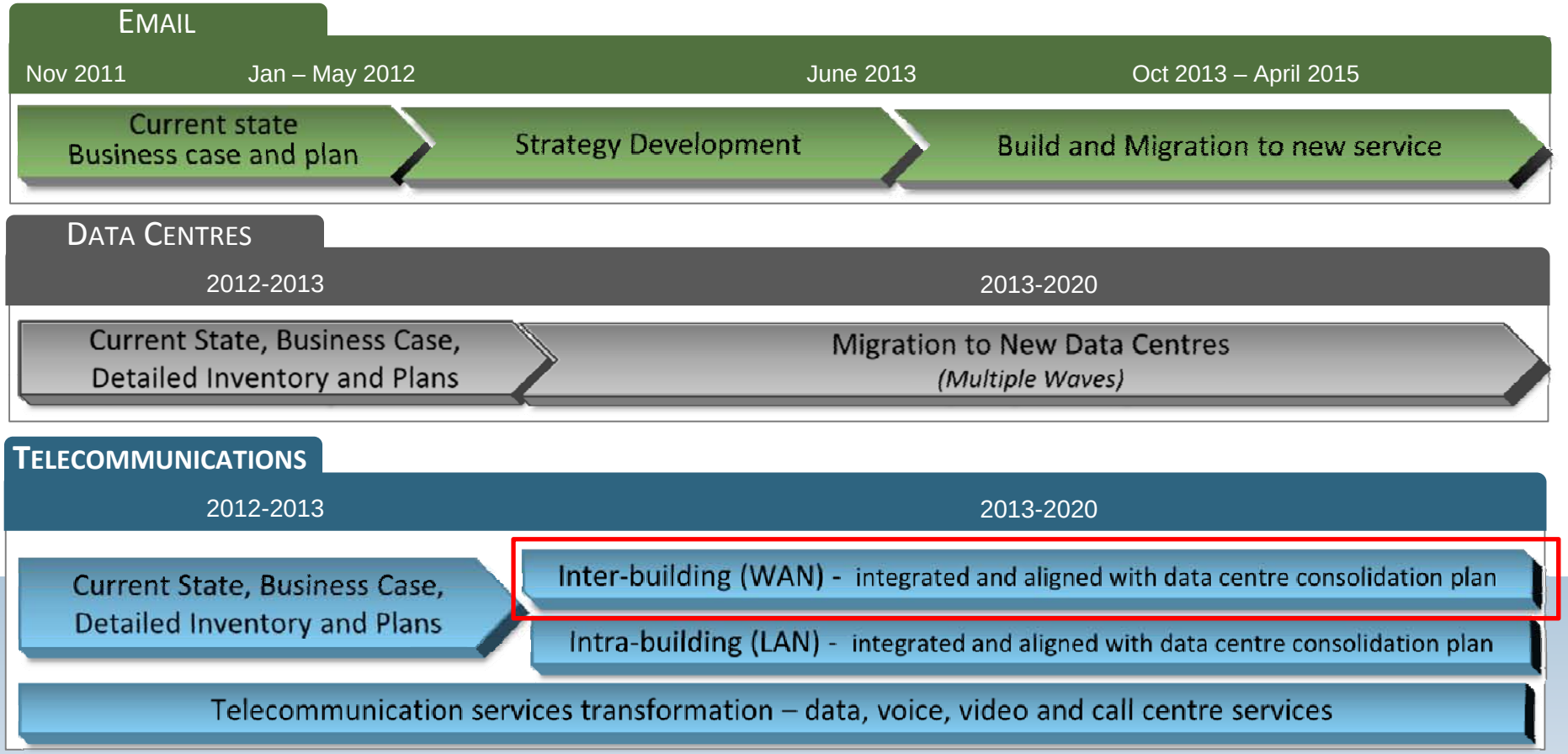
Transformation will match service levels to partner priorities.

SECURITY

Transformation will provision a secure environment to meet program needs.

SSC Transformation Overview

SSC's Transformation Initiatives



Engagement

Key Stakeholders
- Ministers
- Inter-departmental Advisory Committees (IT Business Transformation)
- CIO Council
- 43 Partner Departments
- Unions
- Industry

Inter-departmental Working Groups:
- Security
- Policy and Standards
- Functional
- Business Requirements
- Transition
- Operational & Service Mgmt
- Information Mgmt

Forums / Events
- Chief Information Officer Council (CIOC), CIO Forum
- DPI, GTEC
- Executive Summit
- Heads of IT meetings

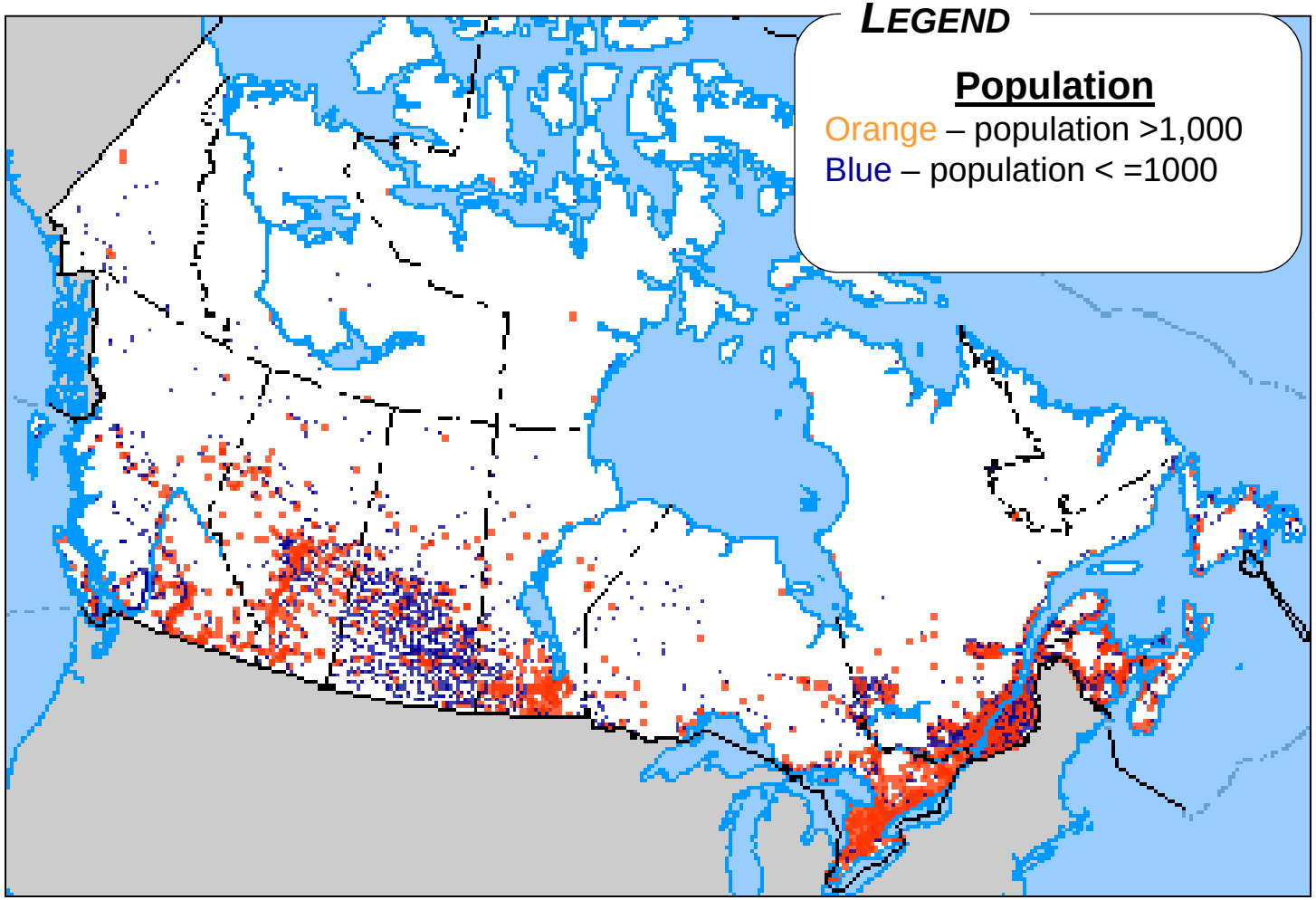
Industry – Launch and closure of procurement process; engagement of industry based on sourcing strategies

SSC Transformation Overview

Background - Current State

- Canada population = 33.4M
- 13 largest cities (metro areas) total population > 18M
- Canada has 230 cities with a population of > 15,000
- Important to factor in population distribution in network architecture to provide best service to citizen

Canadians population distribution

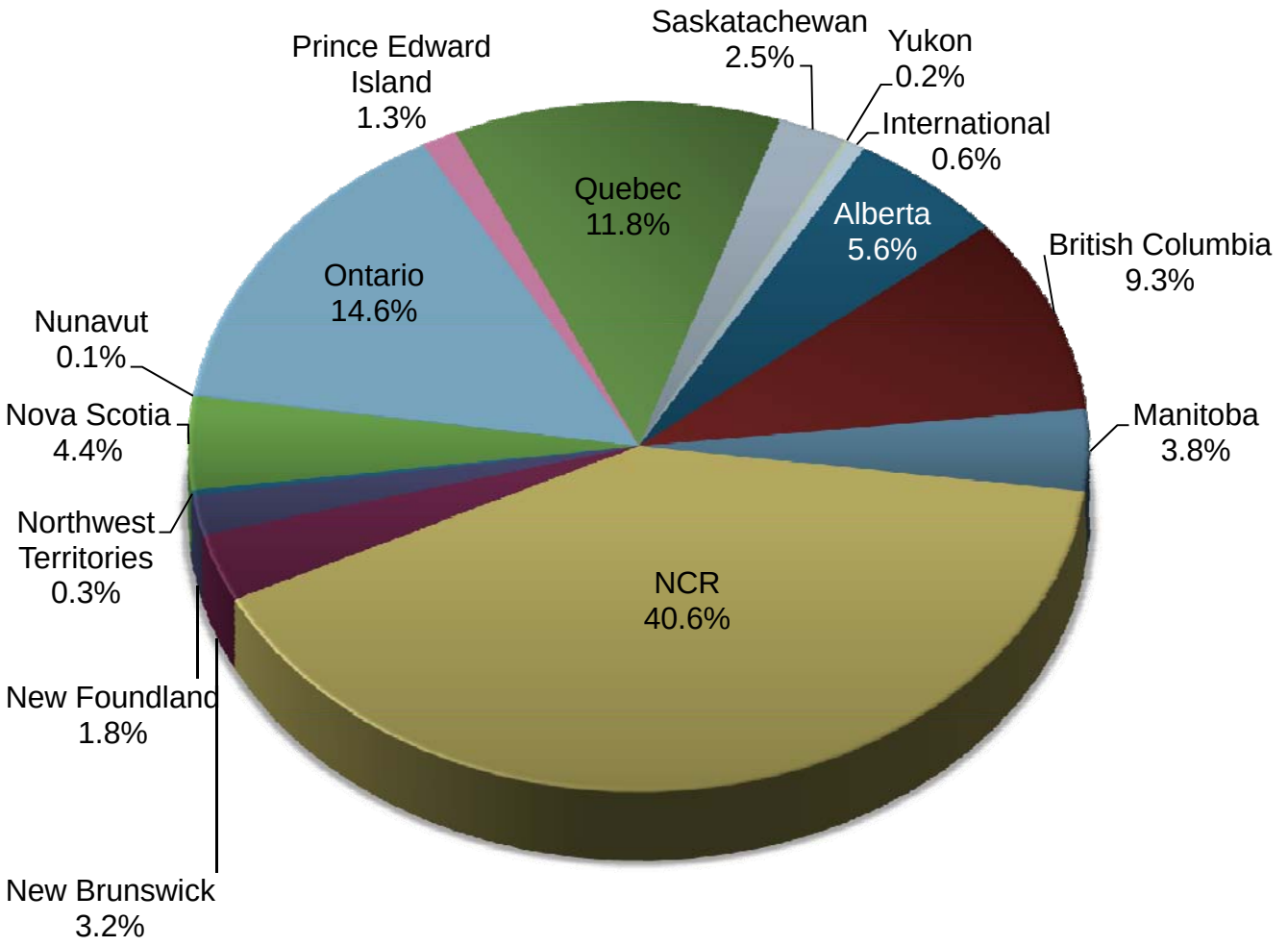


SSC Transformation Overview

Background - Current State

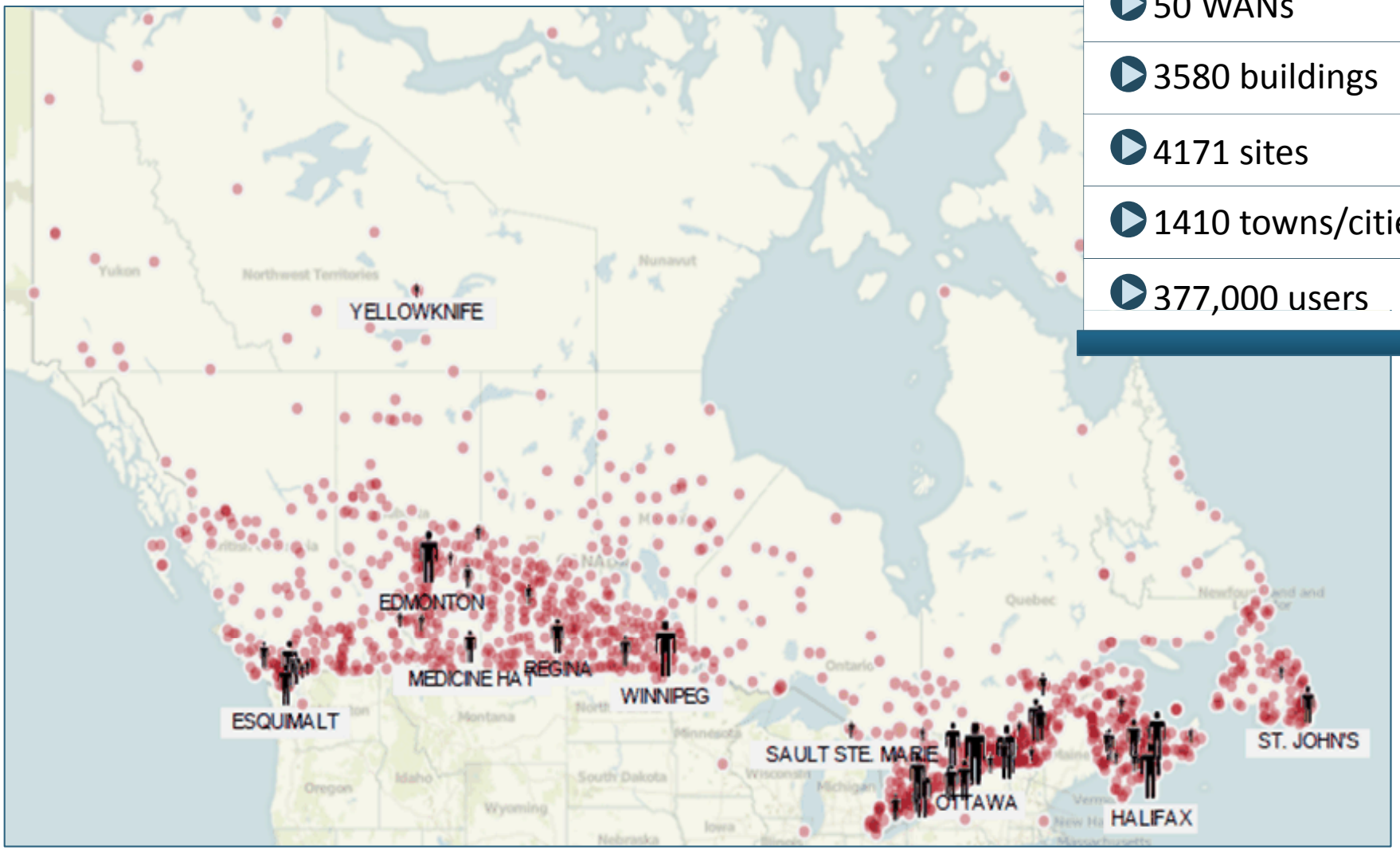
- Total of approximately 255,000 public servants (excluding military members of the Canadian Forces and RCMP officers)
- Over two thirds of public servant employees are located in Ontario and Quebec

GC employee distribution by province + NCR



SSC Transformation Overview

Background - Current State Complexity Across Canada



- 50 WANs
- 3580 buildings
- 4171 sites
- 1410 towns/cities
- 377,000 users

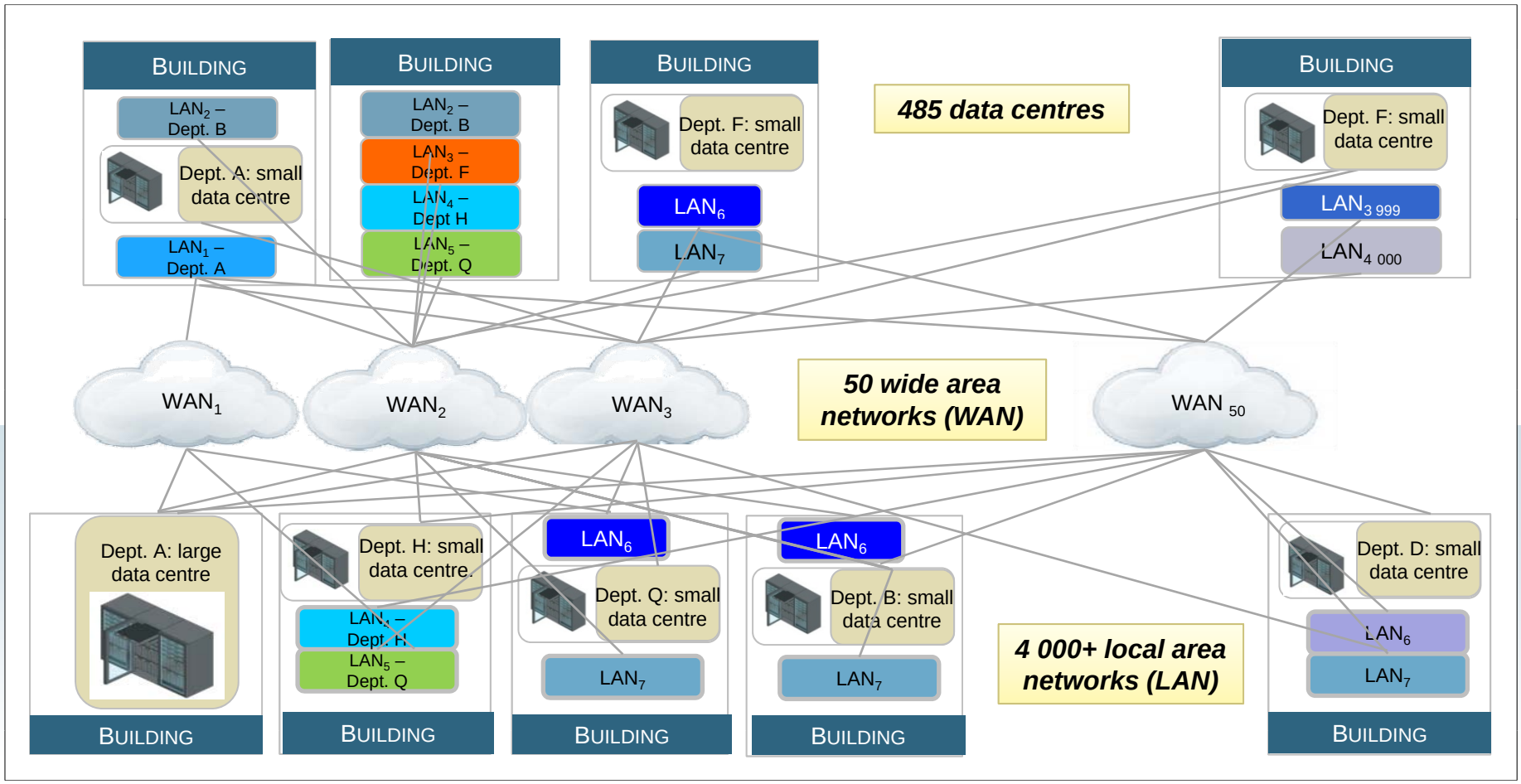
Note: Red dots indicate locations which need to be supported

SSC Transformation Overview

Background - Current State is Complex, Costly and Vulnerable

The Government's current IT infrastructure is complex, costly and vulnerable

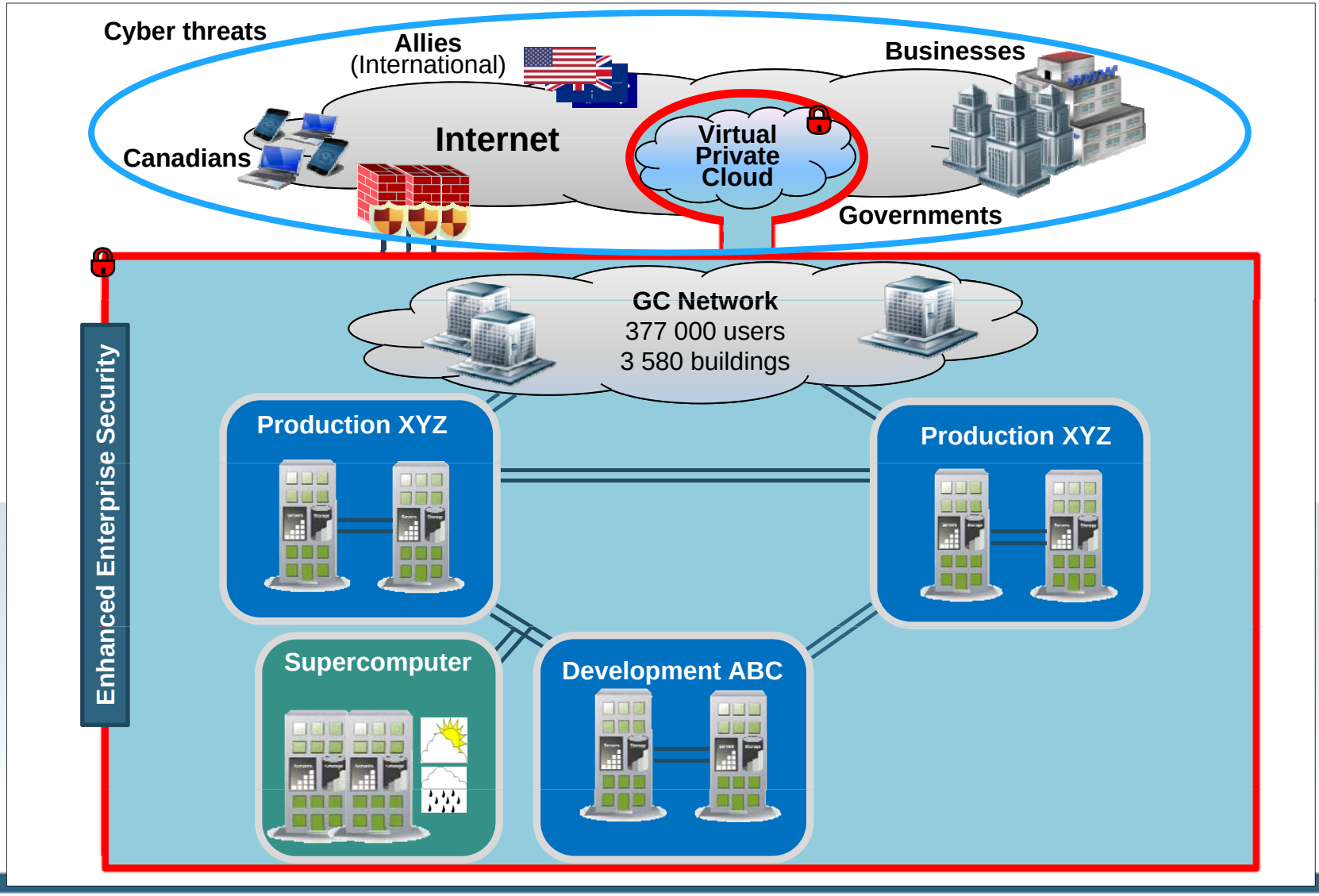
Built and managed in silos, the existing web of infrastructure is unreliable, inefficient and difficult to maintain.



SSC Transformation Overview

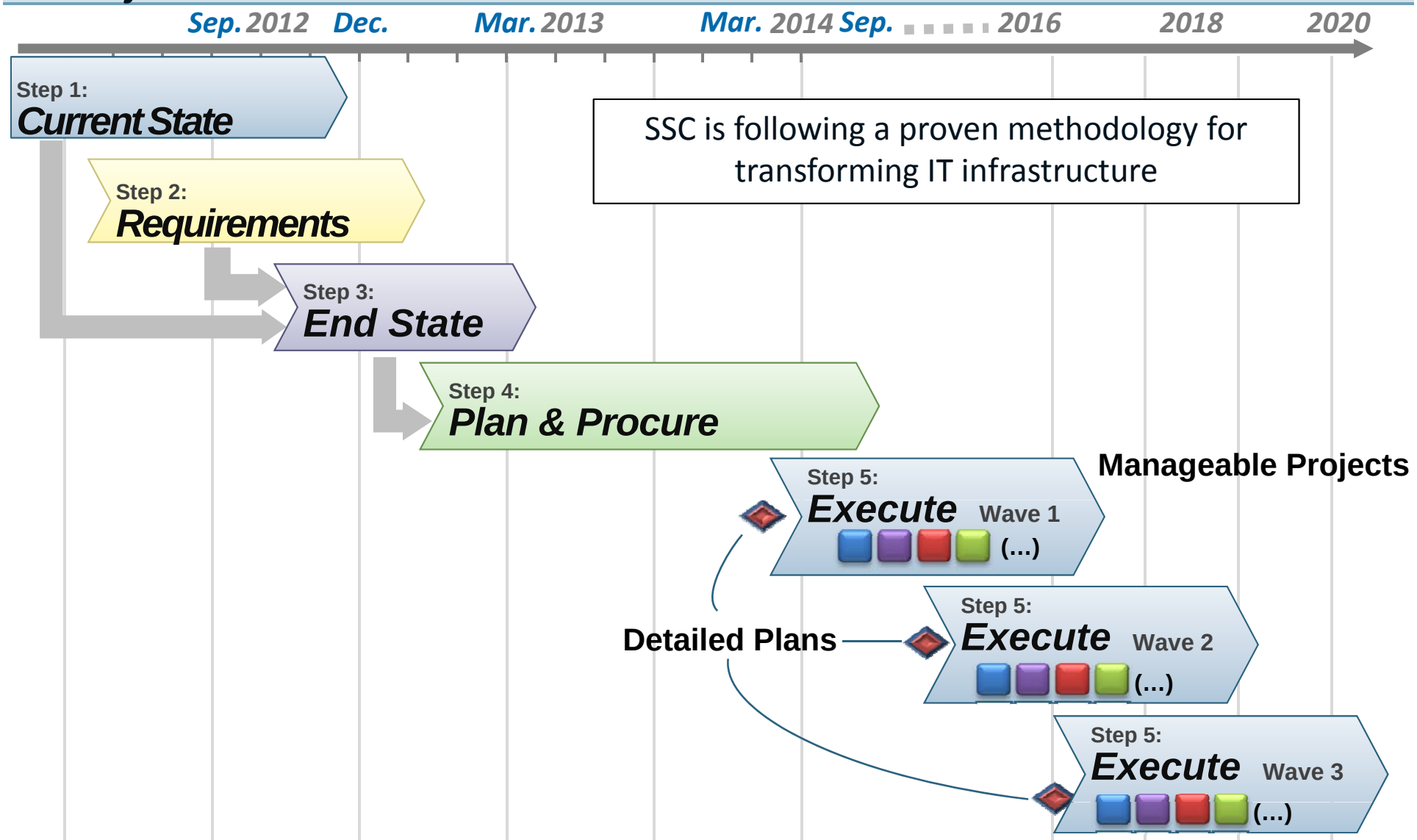
Background - Conceptual End State

Simpler, Safer and Smarter



SSC Transformation Overview

Transformation Schedule



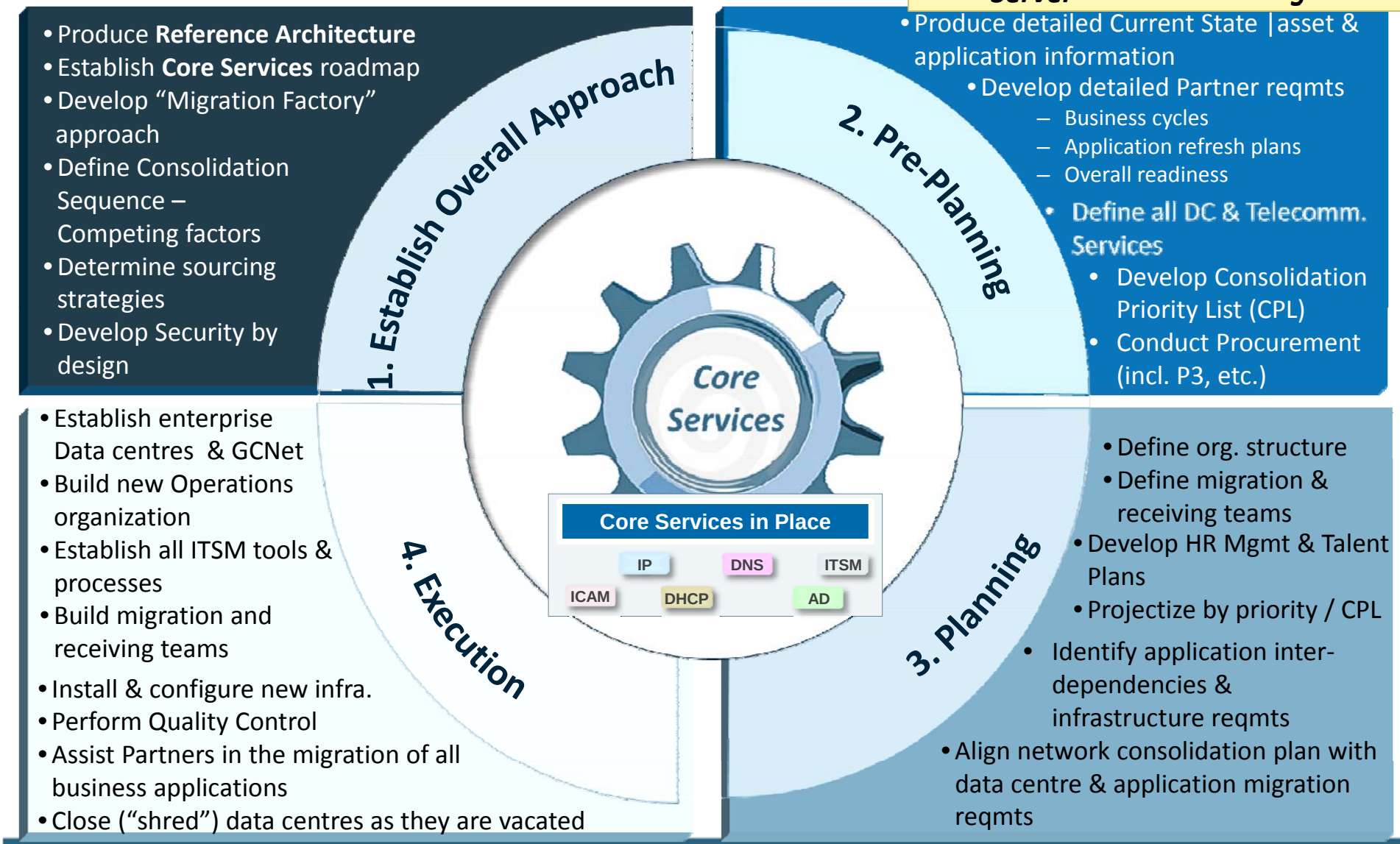
Program Management: Project Management, Reporting, Communications, Governance, Stakeholder Engagement, Finance

SSC Transformation Overview

Transformation Phased Approach

UNIT OF TRANSFORMATION WORK:

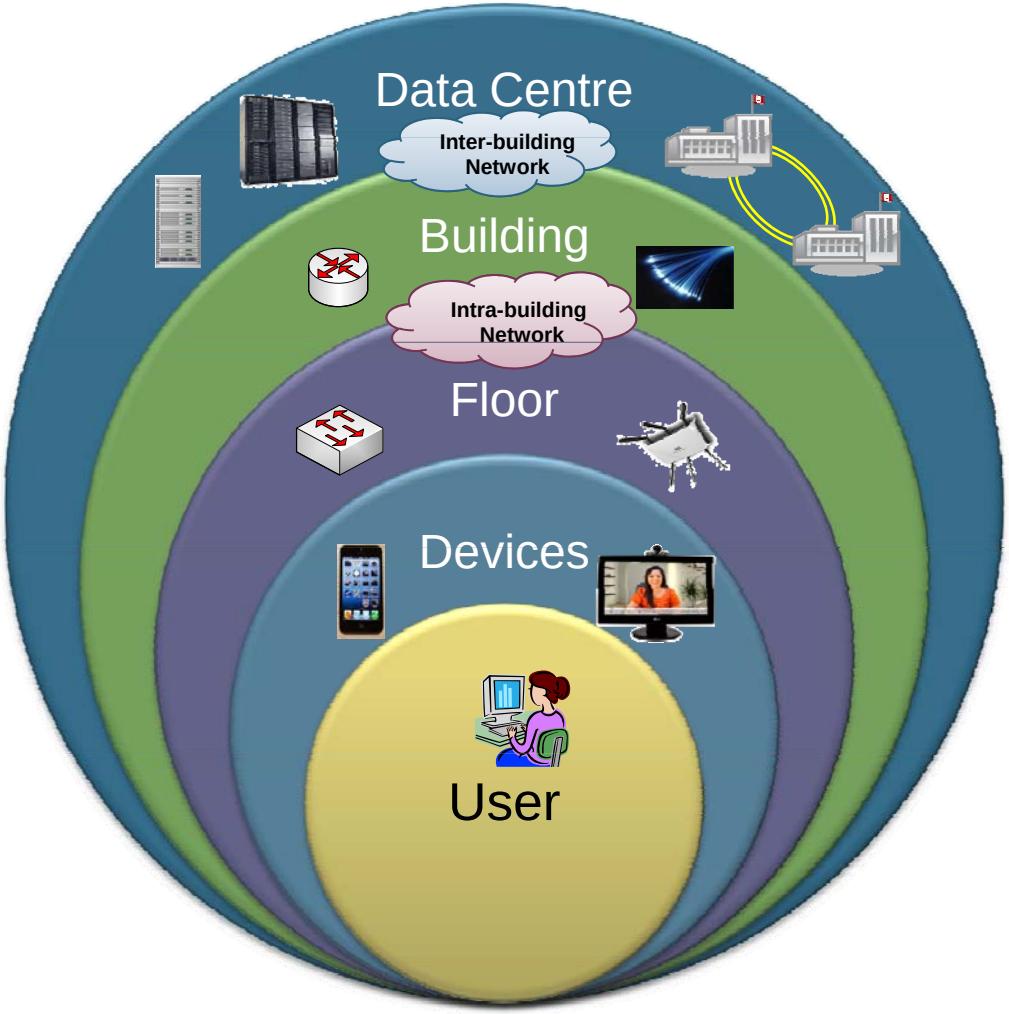
DCC:	*TTP:*
Server	***Building***



SSC Transformation Overview

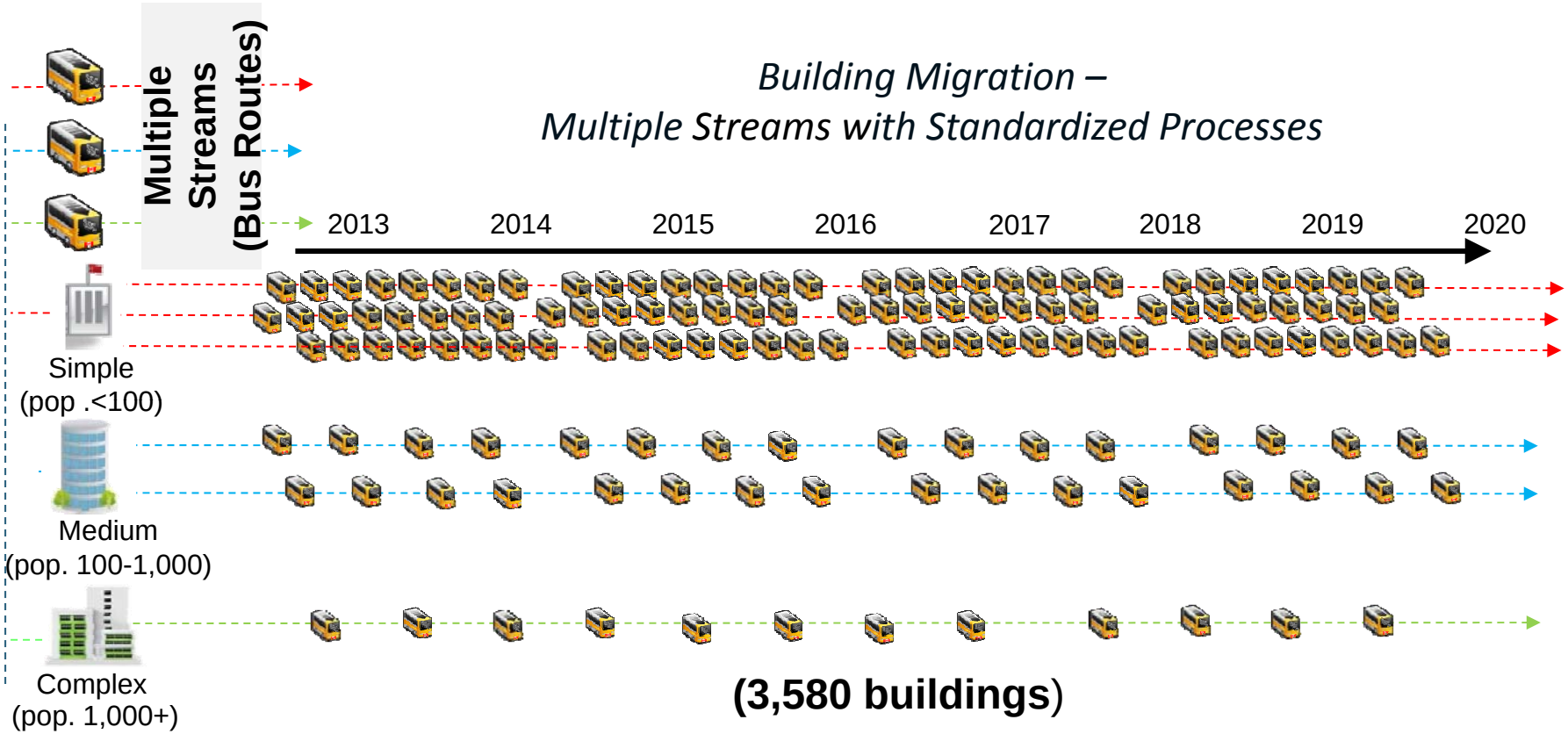
User-centric Approach to Planning / Execution

- Overall planning and execution framework is based on user-centric approach
- Project for each of the 3 580 buildings
- 377 000+ users located in 1 400+ different cities/towns



SSC Transformation Overview

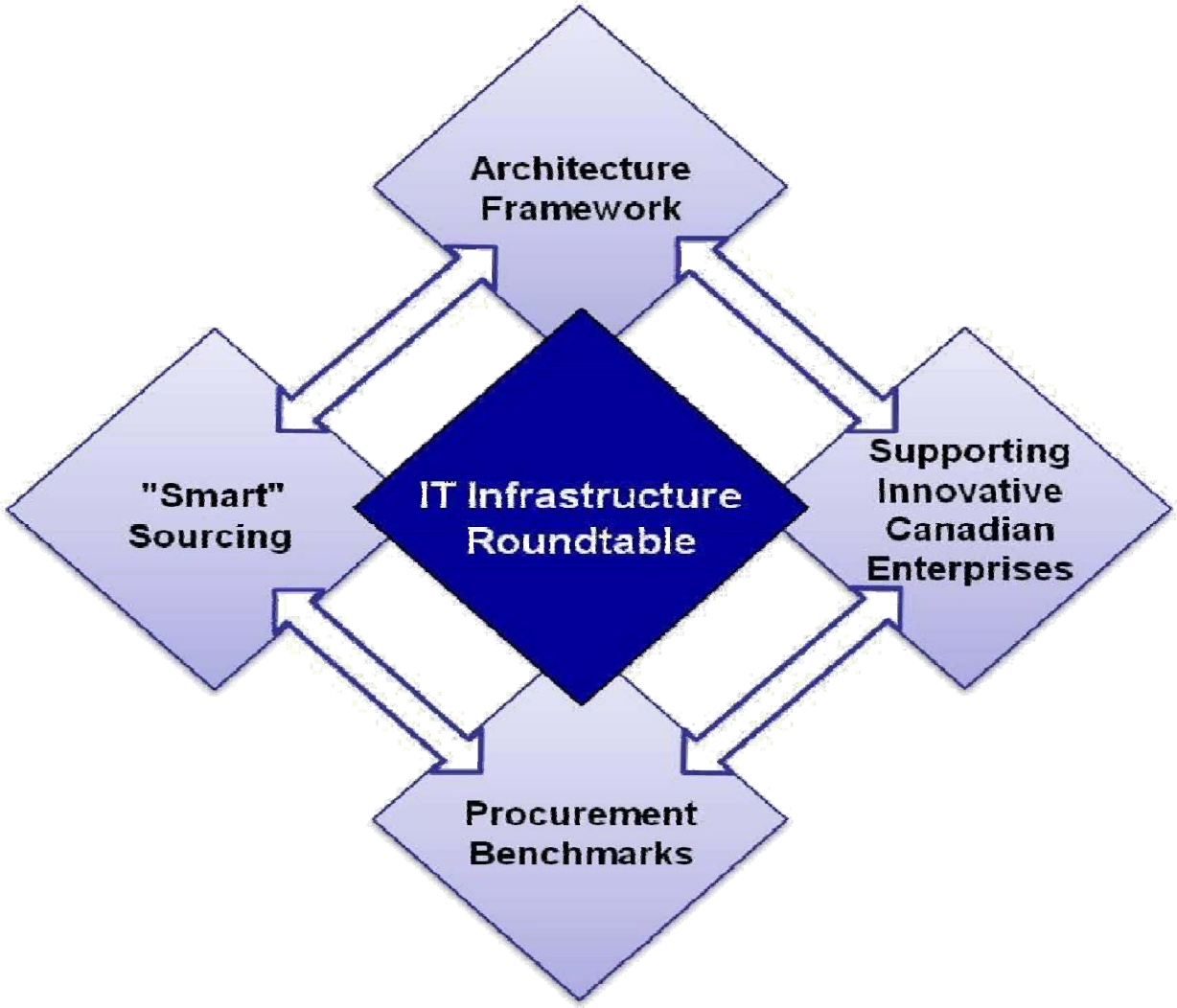
Overall Transformation Approach



Bus routes in the context of buildings mean multiple teams transforming different types of buildings. Buildings will be migrated to consolidated infrastructure which includes wireless LAN and VoIP services.

SSC Transformation Overview

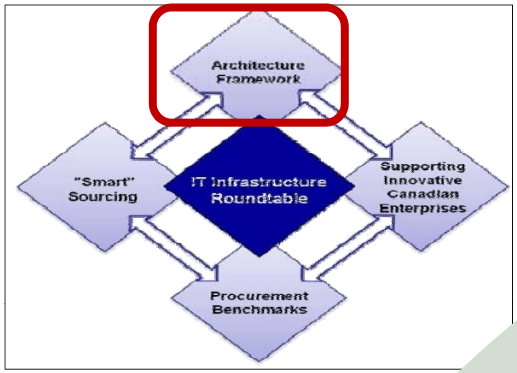
Stakeholder Engagement - IT Infrastructure Roundtable and Advisory Committees



SSC Transformation Overview

Stakeholder Engagement - Architecture Framework Advisory Committee (AFAC)

AFAC was launched in Oct 2012 and includes a core group of members from ICT Industry and SSC



Oct. 11, 2012

Launch of AFAC

Transformation Overview

Cloud Computing/ Platforms

Converged Communications

Sample Feedback from AFAC

"SDN is absolutely real. Multi-vendor interoperability around SDN is a generational change at the network layer. No one is implementing Spanning Tree anymore. You can do very fine bandwidth management higher in the stack w/o being connected to the network."

"...Architecturally trying to separate into LAN, WAN, and then PSTN, Internet etc. We don't look at them together because we want competition and flexibility. Also important for bargaining power. You can have multi-vendor applications managed.

"Bandwidth is a commodity that is going down in price. You don't want to bundle bandwidth with suppliers. There are few SPs that can go all across Canada."

SSC Transformation Overview

Wrap Up & Questions

Questions?

(for Suppliers only)

Service | Innovation | Value

GCNet WAN Services Industry Day

GCNET – WAN Services Overview

Michel Fortin
DG, Telecommunications Transformation Program
Transformation, Service Strategy & Design
Shared Services Canada

July 9, 2013

EDRM # 1805227

Shared Services Canada | Services partagés Canada

Canada

Telecommunications Transformation Program (TTP) Overview

Purpose

To provide background and obtain industry input on the proposed approach for GCNet Wide Area Network service delivery options and procurement process

- Obtain industry input on the strategy
  - ✓ National or regional model ?
  - ✓ High availability approach
  - ✓ Length of contract
  - ✓ Pricing Model
- Advice that could lead to better pricing (based on past experience)
- Explain the revised procurement process to address supply chain integrity
- Address questions regarding process
- Set the stage for the one-on-one engagements

"Early, ongoing and honest discussion with Industry Leaders and other stakeholders is critical to our Government's commitment to achieve the best possible results for Canadians. This roundtable provides us with the a new opportunity – a chance to receive valuable feedback on how to improve our processes, increase our efficiencies and reduce costs to Canadian taxpayers"

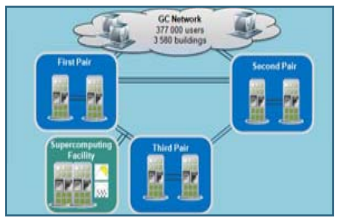
Source: The Honourable Rona Ambrose

Telecommunications Transformation Program (TTP) Overview

Growing Bandwidth Requirements for the Government of Canada

ULTRA HIGH BANDWIDTH SERVICE REQUIREMENTS

- Growing delivery of applications in the cloud (e.g. e-mail)
- Virtual Desktop Hosting



- Consolidation and centralization of data (Data Center Consolidation)

- Fully interactive
- Telepresence
- Unified Communications

- Growing use of Social Media-like apps (eg. Facebook, Twitter, GCPedia)

…UBIQUITOUS FOR ANY LOCATION…

Growing Mobility Requirements

Seamless work/home environment (remote access)

Requires End-to-end security

Must be available in Remote Locations

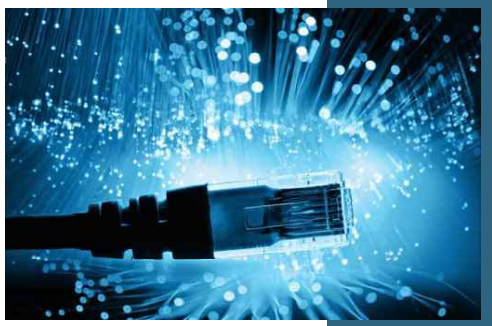
Telecommunications Transformation Program (TTP) Overview

What is the Telecommunications Transformation Program?

- Telecommunications Transformations Program is comprised of 6 elements with the principle services being **inter-building (WAN)**, **local area network (LAN) & voice services**

- One of the main objectives of the TTP is to design and build an integrated telecommunications network to support Government of Canada operations. The Government of Canada Network (GCNet) will be the future integrated network.

- The scope of the GCNet WAN is currently planned to exclude inter-data centre connectivity (will be the subject of a separate procurement process). Scope in other areas may be modified based on industry feedback.



Telecommunications Transformation Program (TTP) Overview

6 Element Framework – Focus on Inter-Building Network / GCNet WAN

#3 – Voice/Video/Conferencing Services

- IP-based voice, video and conferencing services over converged network
- Migration from wired to wireless devices

#2 – Network and Cyber-security Operations Centre

- Consolidated 24/7/365
- Co-located NOC/CSOC in DC

#1 – Network Services

a. **Internet** - High-speed, dual ring backbone between data centers with very high availability

b. Inter-building - Consolidated and converged network with shared inter-building access

c. **Intra-building** - Shared infrastructure in multi-tenant buildings with wireless

d. **Inter-data centre** - High-speed, fully redundant through rings

e. **Intra-data centre** - Shared infrastructure

#4 – Contact Center Services

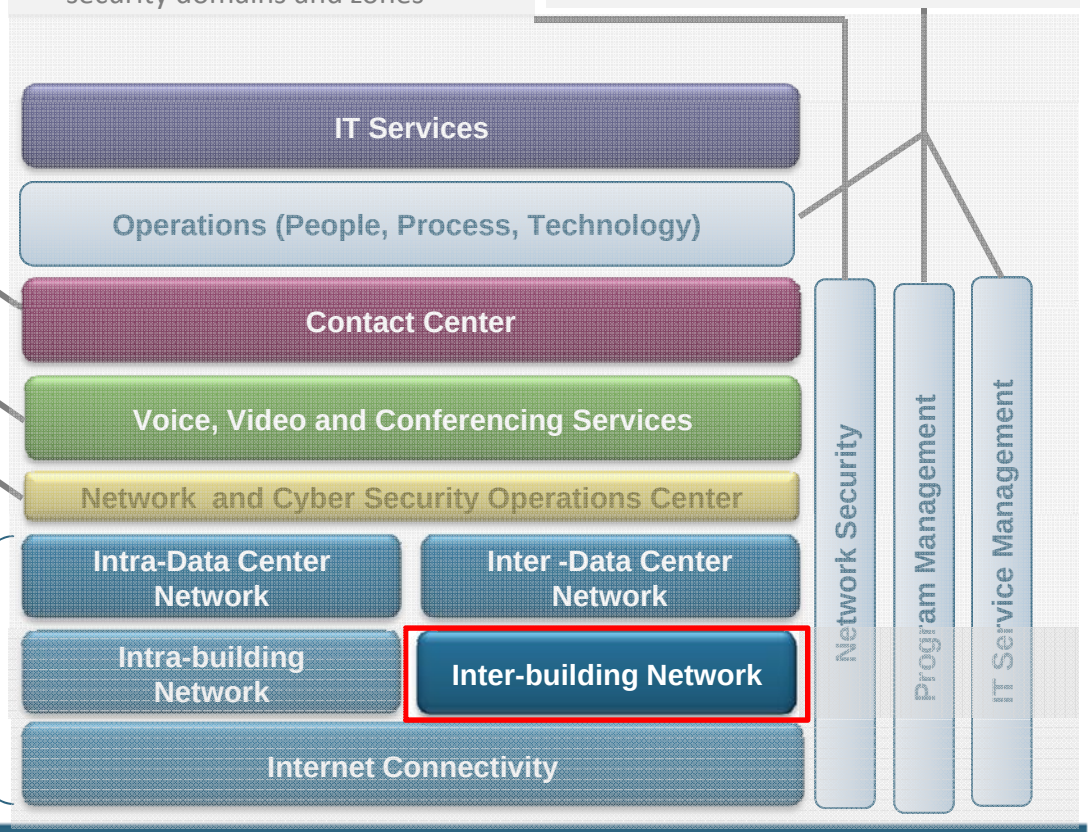
- Migrate from legacy to IP-based infrastructure for contact centres

#5 – Network Security

- Network security based on security domains and zones

#6 – Management and Operations

- Management and Administration
- IT Service Management
- Service Strategy and Transformation



Telecommunications Transformation Program (TTP) Overview

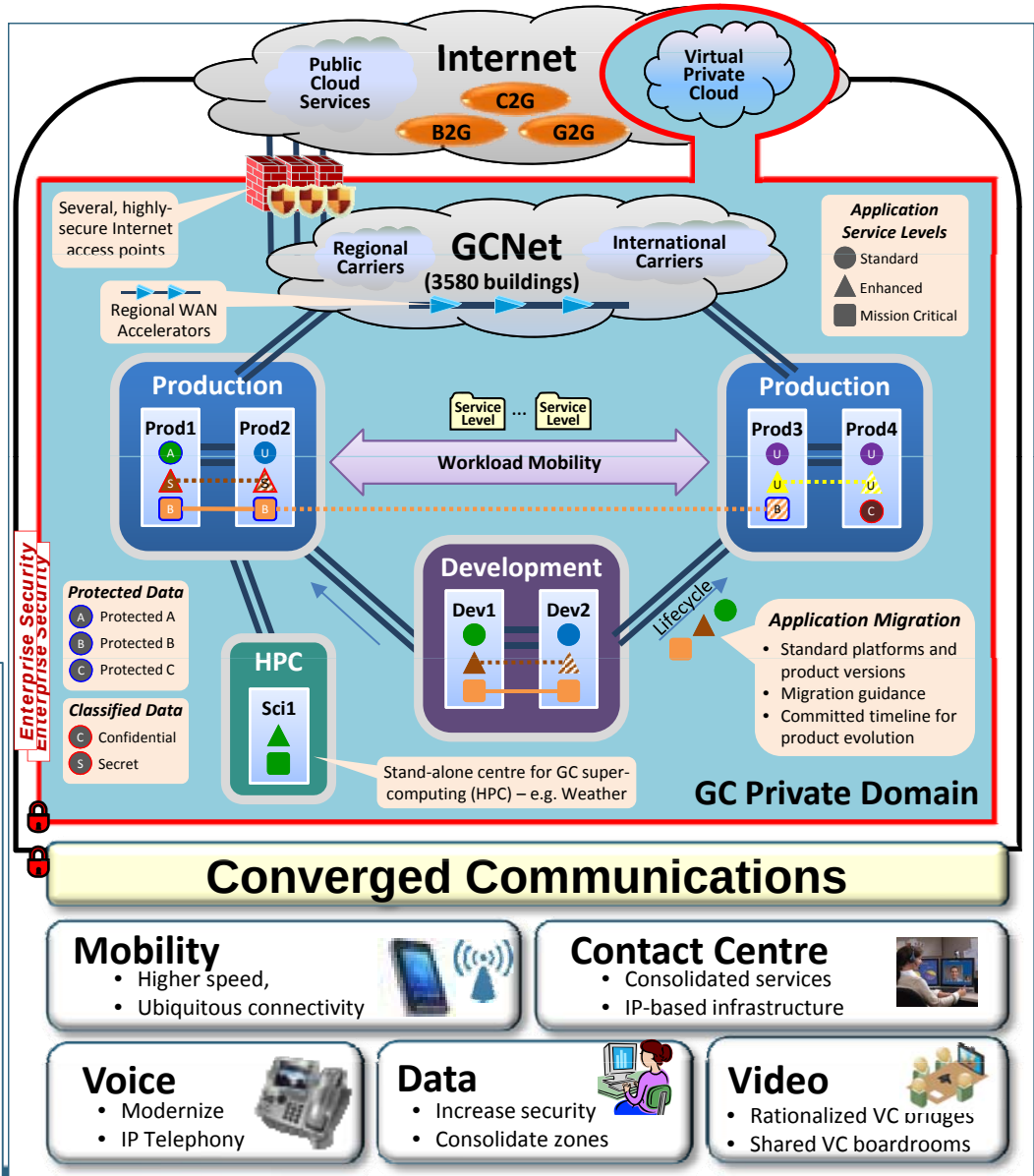
TTP Conceptual End State

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

GCNet WAN Services Overview

GCNet Business Objectives

- Establish a new contract for Wide Area Network (WAN) services to be provided to SSC and its 43 Partner departments and agencies at approximately 3,580 locations nationally

SAVINGS

Reduced IT complexity and overall cost

- Consolidate and standardize the IT infrastructure for delivery of WAN transport services for SSC partners, Canadian and international locations
- Converge network services supporting legacy Voice and Video services onto the consolidated and standardized WAN services
- Facilitate interoperability across departments and agencies

SERVICE

Standardize and Simplify Service Management

- Standardize service levels to ensure a consistent delivery and availability of WAN services

SECURITY

Enhance WAN Security

- Implement standard WAN security measures and controls to ensure robust protection against threats
- Continue to deliver services securely and reliably to Canadians

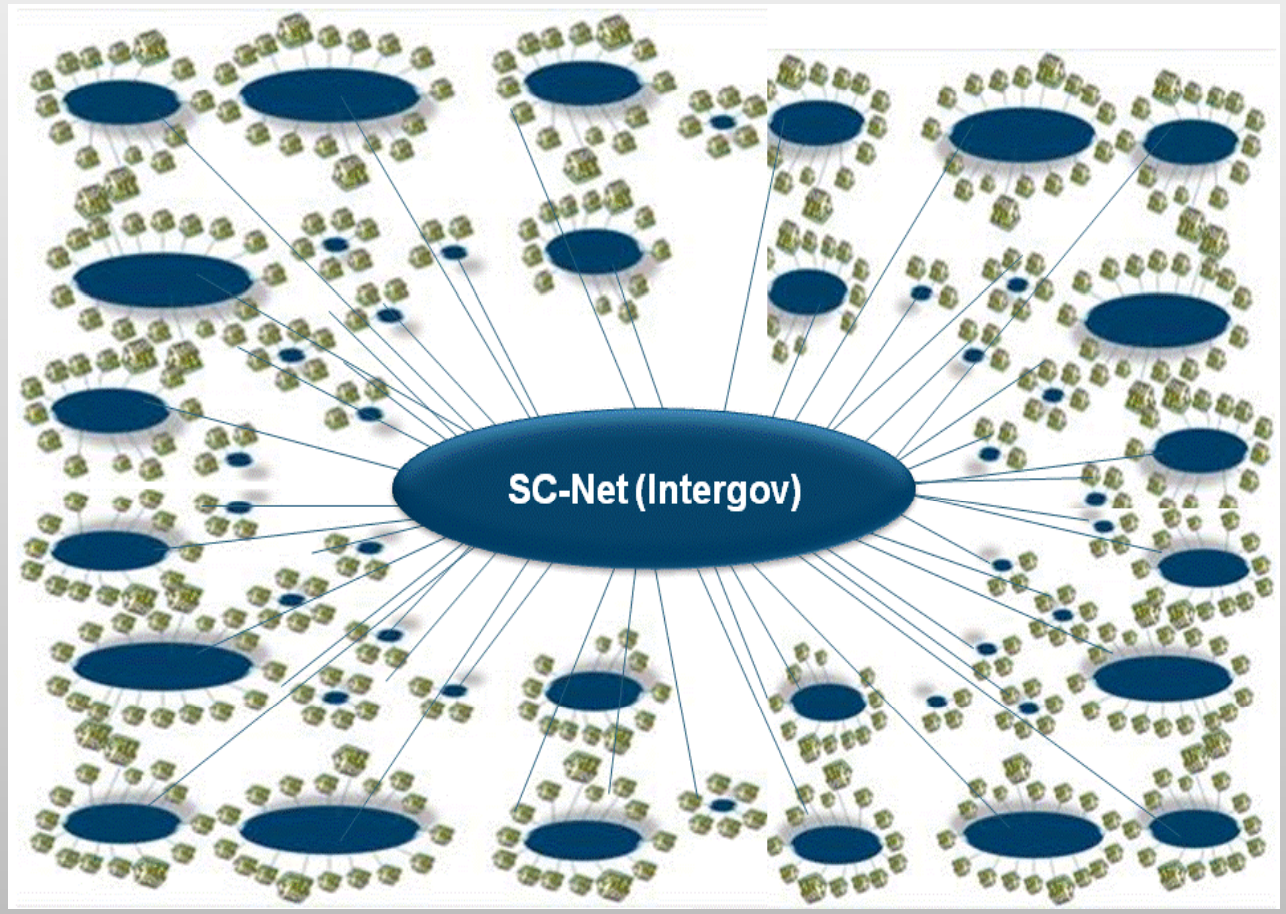
GCNet WAN Services Overview

Current State – Departmental "Siloes"

Current State:

- Departmental-based Wide Area Networks
- Various service levels and management oversight
- Separate access charges for each department in multi-tenant buildings
- Requires a separate network just to interconnect departments

50 Wide Area Networks interconnecting 485+ Data centres

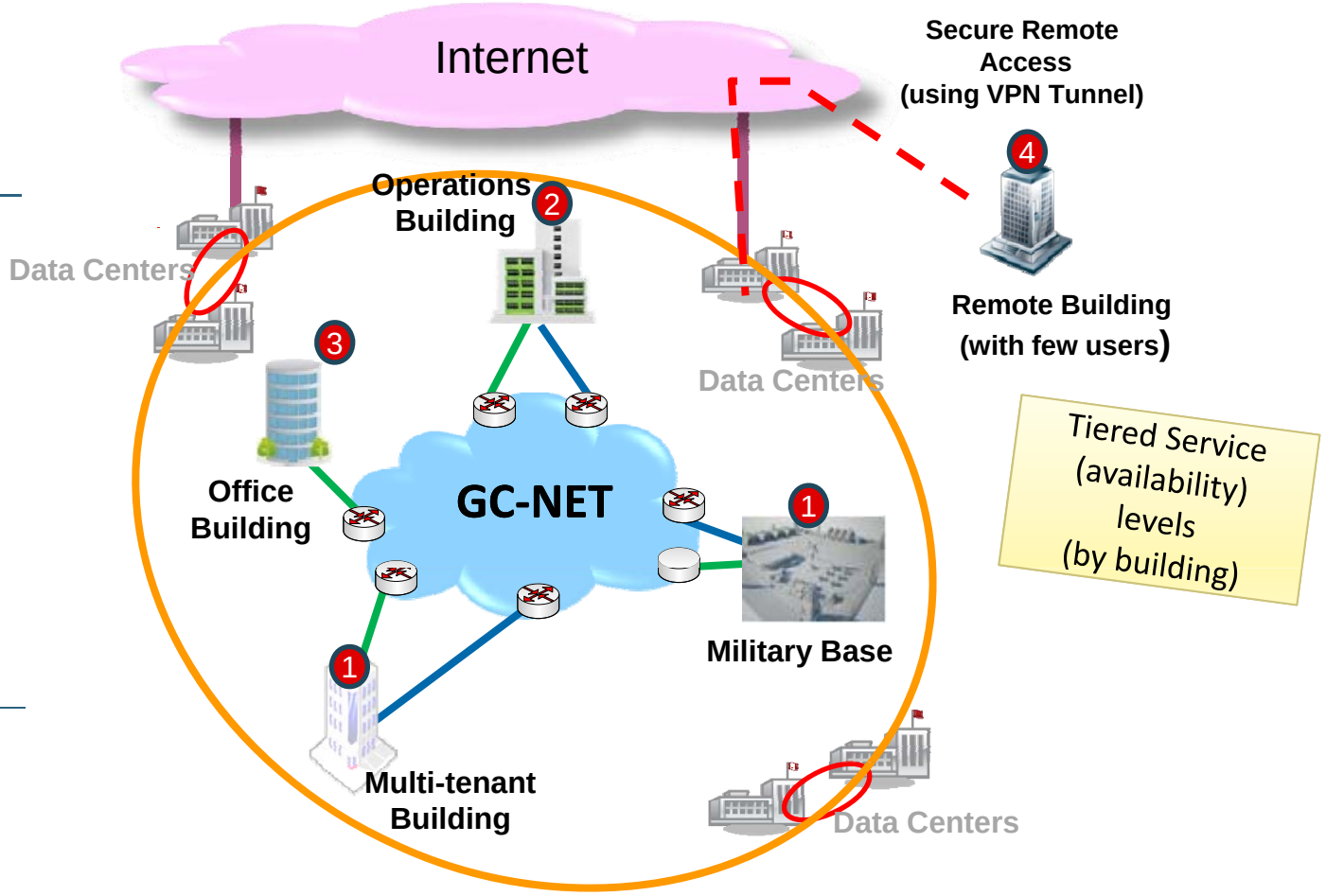


GCNet WAN Services Overview

Detailed End State – Services View

Enterprise Converged and Consolidated Networks

Provide greater network capacity, reliability and security to enable partners to deliver optimum support service to Canadians

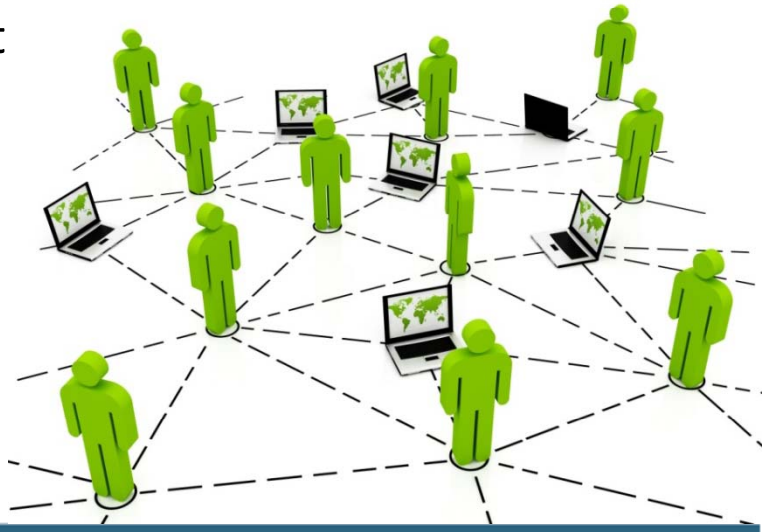


- Transform from 50 “siloed” networks to a shared, more secure enterprise network
- Much greater bandwidth to support increased centralized services (e.g. Consolidated data centers and e-mail) and videoconferencing
- Expected increase in bandwidth usage is projected at 22% annually

GCNet WAN Services Overview

Requirements: Business

- **Support a wide variety of federal government programs** and applications ranging from corporate email and routine data exchanges, to real-time government wide mission critical military, policy, health and public safety information
- **Consolidate** the management of networks to eliminate silos and **facilitate interoperability** across departments and agencies
- **Reduce duplication** and inefficiencies
- **Ensure high availability** for mission critical sites
- **Standardize service levels** to ensure a consistent delivery and availability of WAN services across all SSC partners and agencies
- **Minimize cost** to manage service
- **Security**: Supply must meet the **trusted Supply Chain requirements** (identified in the "Supply Chain Integrity" presentation to follow)



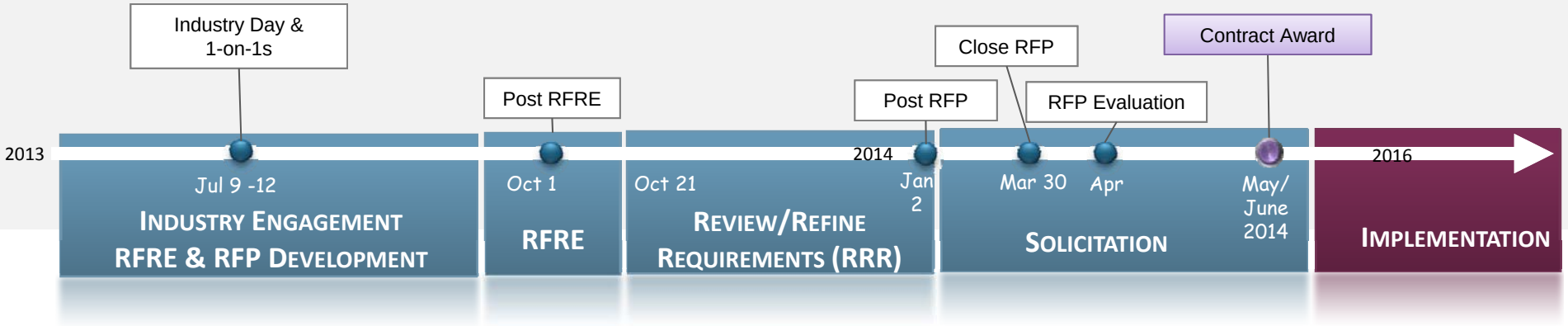
GCNet WAN Services Overview

Requirements: Functional

- The ability to provide **inter-building Layer 3 connectivity** to all buildings where the GC or one of its partners is a tenant
- The ability to **support data and real time traffic** such as voice and video
- The ability to support network performance service levels using **Quality of Service (QoS) /Class of Service (CoS)** to enable the convergence of data, voice and video onto IP network services
- The ability to **support a variety of multiple virtual private networks**
- **Consolidated network access** to each building for all departmental WAN requirements at a site
- **High availability** at buildings (through **diverse physical routing** and /or **multiple carriers) at** sites with **mission critical business functions**
- **Service options** with **scalable bandwidth levels** to meet the different service requirements
- **Connectivity to existing networks** to ease the transition to the new GCNet
- Support for **Legacy applications** until they can be converted onto an MPLS network

GCNet WAN Services Overview

Procurement Timeline to Contract Award



- The Collaborative Procurement process (identified above) will be explained further in the following “Collaborative Procurement Solutions Approach” presentation
- Supply Chain Integrity (SCI) verification will be conducted during the RRR to ensure all IT Products meet Canada’s security and supply chain standards; more detail will be provided in the following “Supply Chain Integrity” presentation

Objective:

- Allow for an exchange of information through discussion (during one-on-one sessions) with Telecommunication Experts that will ultimately inform telecommunications transformation strategies and procurement planning
- Provide Suppliers with the opportunity to share their knowledge with the GC on the following discussion topics (detailed slides to follow):

    1. Service Delivery Models
    2. High Availability
    3. Contract(s) Period
    4. Pricing Models

GCNet WAN Services Overview

Service Delivery Models – Options

Discussi
Topi

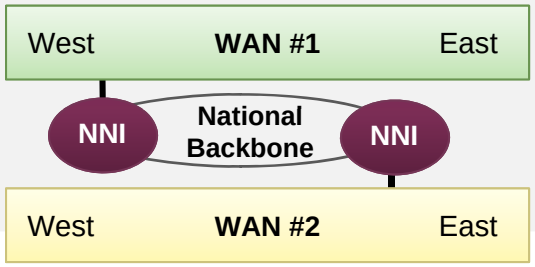
1

Option #1

Pros
- Efficient to operate & manage
- Economies of scale
- Single supplier to manage
- End to end SLA
- No NNIs

Cons
- Business is not shared
- No supplier diversity

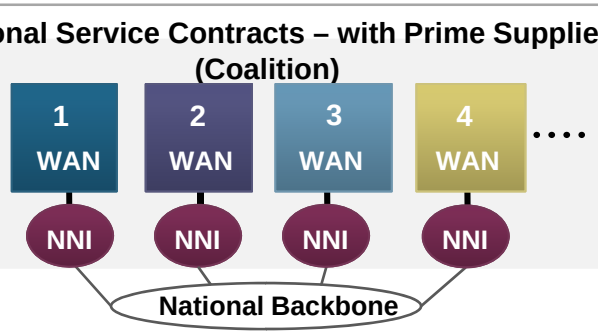
Option #2



Pros
- Pricing may be more competitive
- Business shared
- Supplier diversity

Cons
- No single point for end-to-end accountability
- Challenging to guarantee support for latency sensitive applications end-to-end
- Complex to operate, manage & integrate
- Increased costs due to GC NNI & backbone
- Different pricing per supplier

Option #3



Pros
- Pricing may be more competitive for regional services
- Business extensively shared across Industry
- Improved performance with regional Supplier Central Office (CO) presence

NNI Network to Network Interface

GCNet WAN Services Overview

Service Delivery Models – Options (continued)

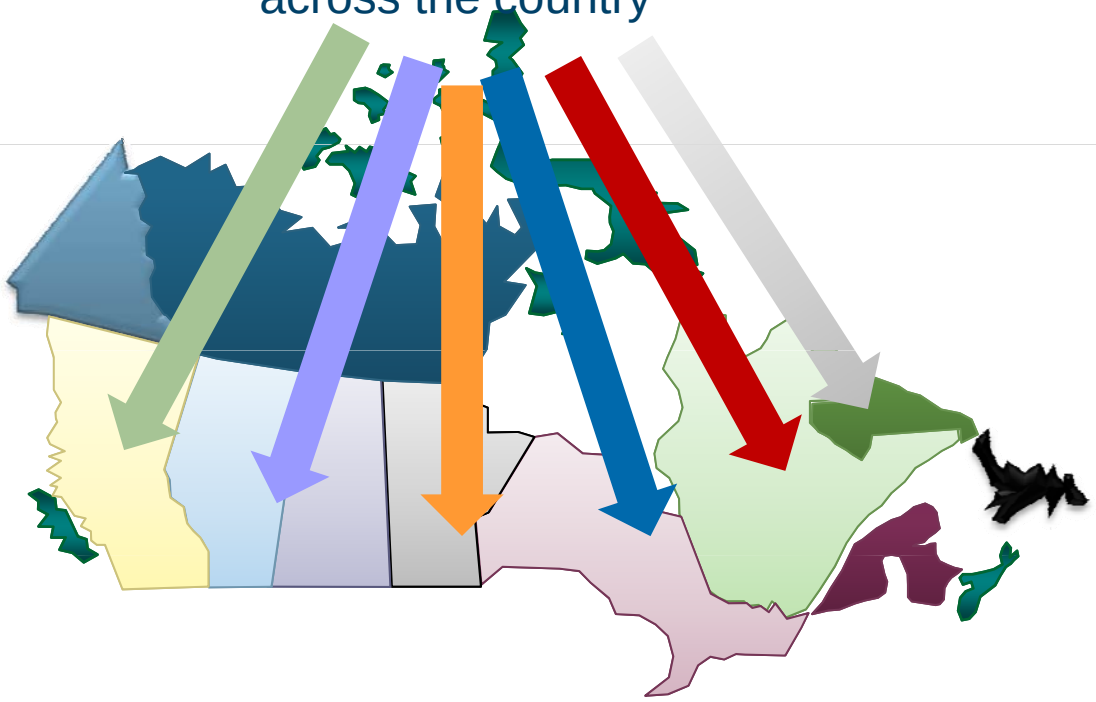
Discussi
Topi
1

Preference:

- Deal with one Primary Service Provider or Integrator to provide end-to-end WAN service
  (but not if cost-prohibitive)
- Primary service provider will deal with various carriers for "off-net" connectivity requirements
- Coalition of ILECs/CLECs* is option with Prime Service Provider/Integrator

End-to-end WAN Service managed by Primary Service Provider

Various carriers (providing "last-mile") across the country



Note:* ILEC is Incumbent Local Exchange Carrier; CLEC is Competitive Local Exchange Carrier

GCNet WAN Services Overview

High Availability

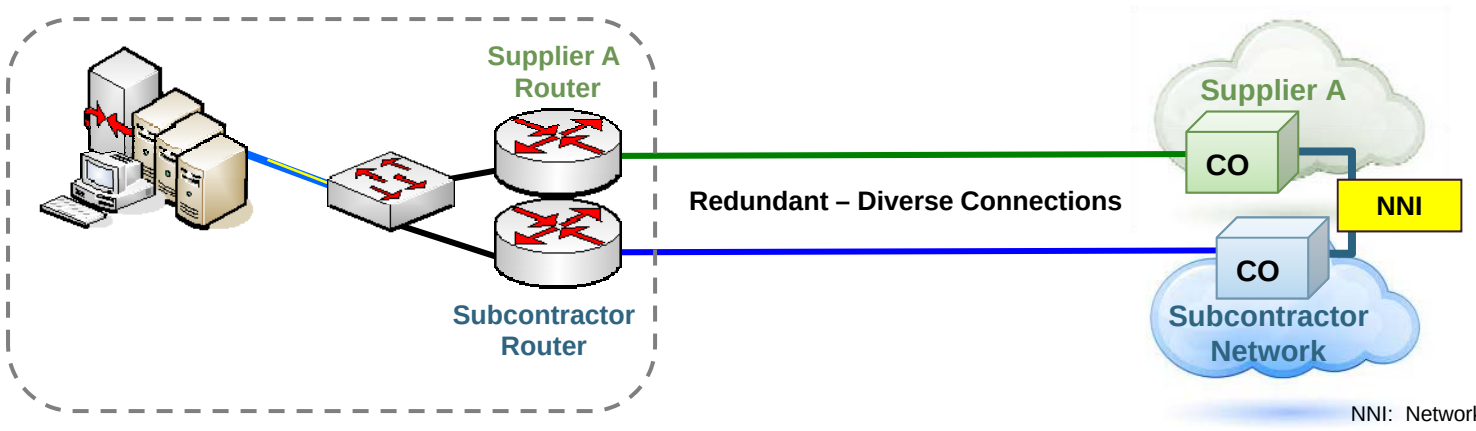
Discussi
Topi
2

Objective:

The Requirement is to provide high availability to critical building/data centres

- The most vulnerable part of site connectivity is the “last-mile”
- HA can be provided by redundancy, diverse routing, diverse Central Offices, and diverse carriers
- Requirement is for 99.9+% availability – guaranteed
- Consideration for a multiple/diverse carrier approach: traffic routing, network interconnectivity, performance for time sensitive applications, accountability

High Availability Models (various) 99.9+%



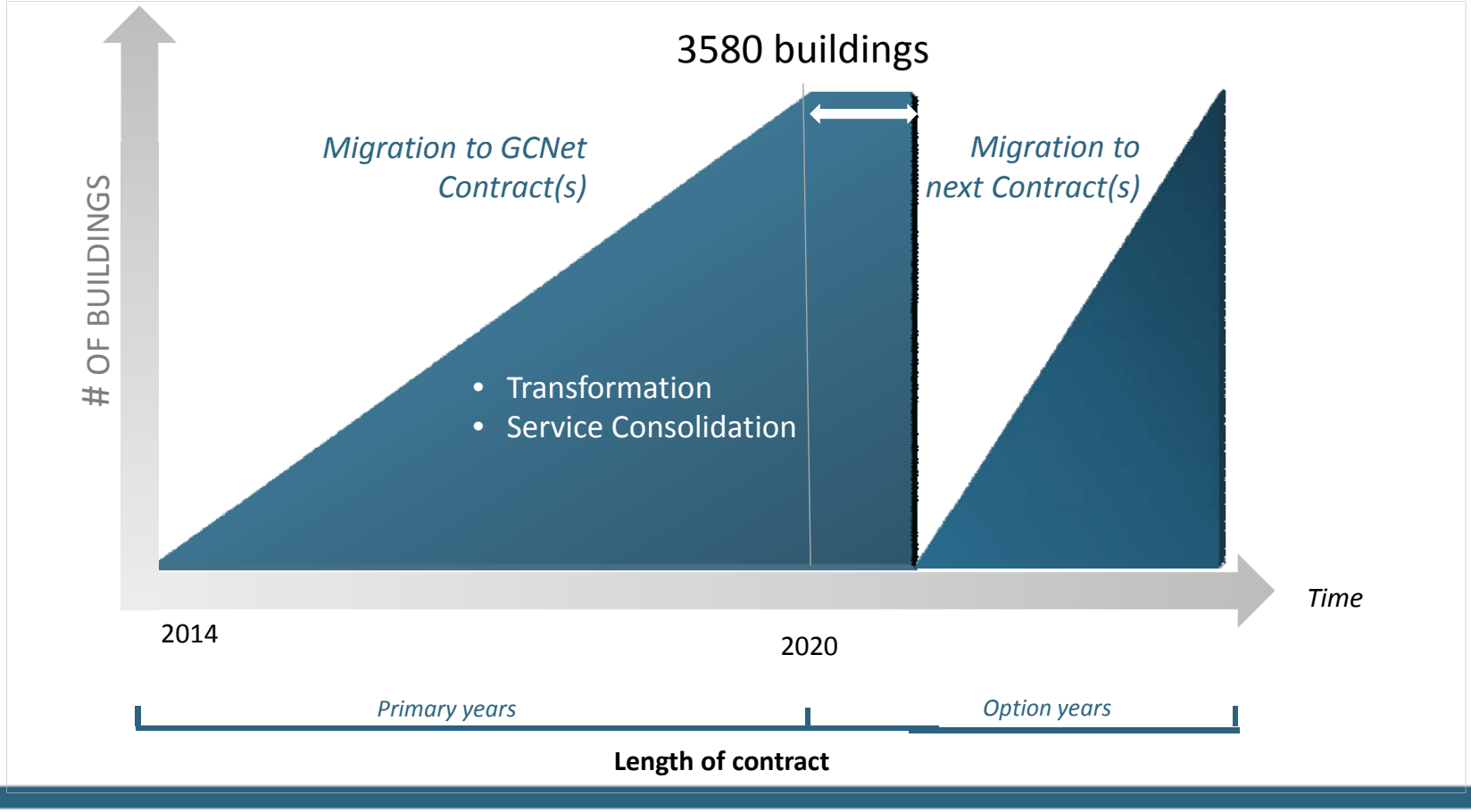
NNI: Network-to-Network Interface

GCNet WAN Services Overview

Contract Period

Discussi
Topi
3

- Recommended contract length (including option years) ?
- Is model which implements regular cost reviews (based on industry benchmarks) feasible ? (eg. every 3 years)

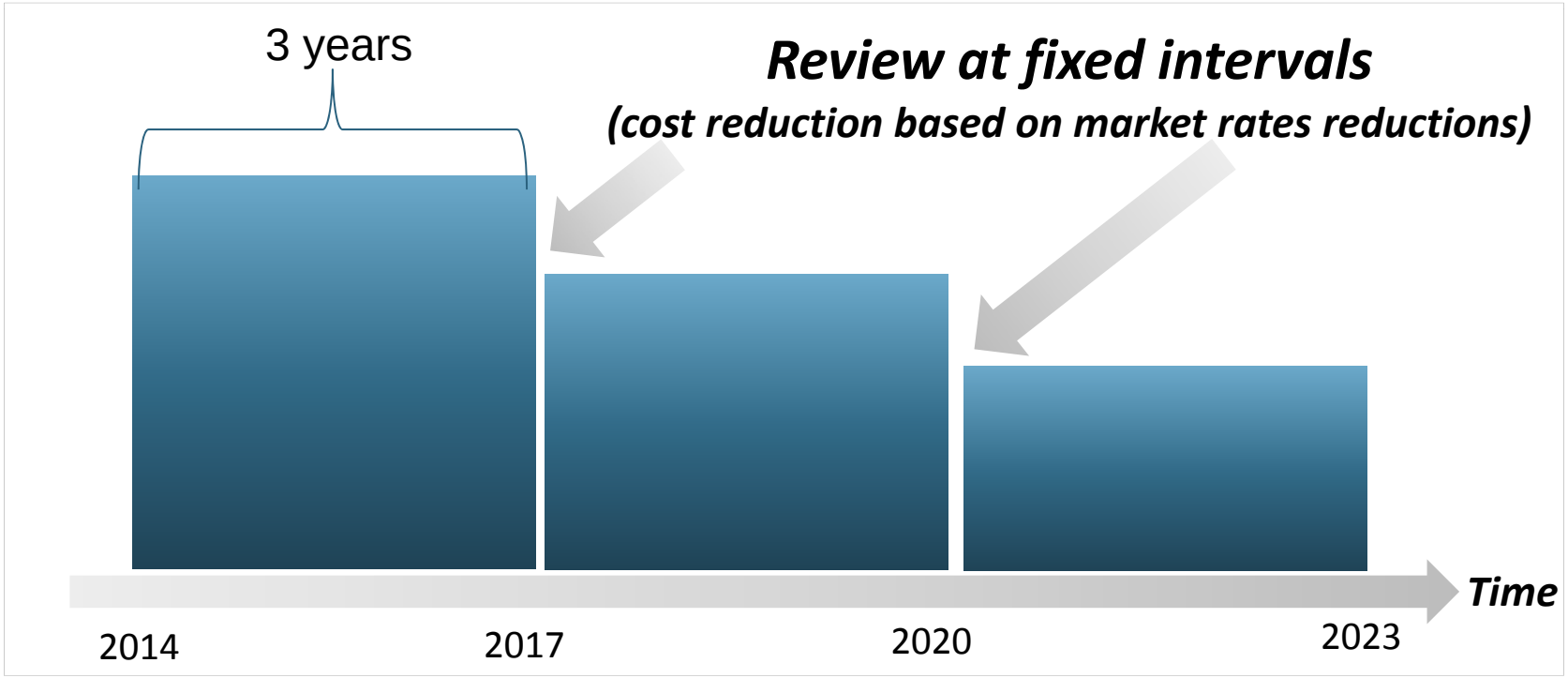


GCNet WAN Services Overview

Pricing Model Options

Discussi
Topi
4

- Numerous pricing model options possible (fixed, variable, etc)
- Pricing reviews at fixed intervals (based on market benchmarks) over the period of contract(s) advisable?
- What are the factors that drive the rates up?



GCNet WAN Services Overview

Questions for Industry Feedback

OPERATIONAL/TECHNICAL:

1. Feedback on National and Regional approach to providers
   - Technical and operational considerations
   - Procurement considerations
2. What are the considerations related to facilitating Real-Time applications (video, voice, etc.) in a multi-supplier arrangement ?
3. What are the pros and cons with dual-supplier connections at critical sites ?
   - Technical and operational considerations (NNIs and backbone)
   - Procurement considerations
4. Identify possible technology enhancements for WAN services over the next 10 years that we may need to consider in our requirements
5. Comment on the integration/peering of the new GCNet WAN services with the existing GC WAN environment (e.g. GC Data Centre internetwork)
6. Do you offer MPLS(TP) or similar services ?
7. Can GCNet traffic completely remain in Canada ?
8. Advice on methods to increase WAN security

GCNet WAN Services Overview

Questions for Industry Feedback (continued)

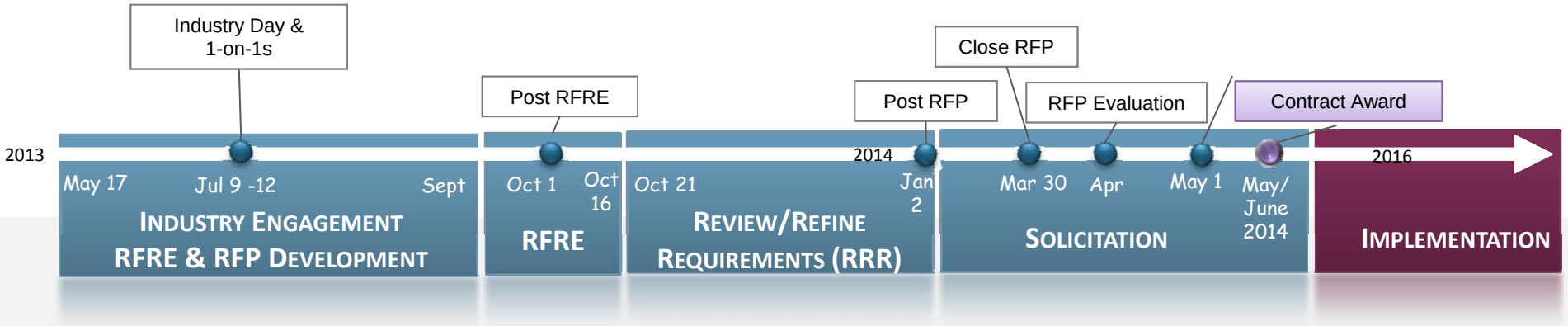
PROCUREMENT:

1. What Pricing Model would be most beneficial to Canada ?
   (Are regular pricing reviews at fixed intervals over the period of contract(s) advisable?
2. What should length be contract length (including option years) ?
3. Provide recommendations on the approach for the technical evaluation of Supplier proposals
4. Provide recommendations for requirements to maximize competitiveness and minimize costs . What are the factors that drive rates up ?
5. Are coalitions of regional providers feasible to create a national service ?
6. What requirements (in SOW) should SSC be considering to increase migration speed on WAN services ?
7. Feedback on proposed procurement timelines
8. Can RFP contain requirement to route traffic only in Canada (for intra-Canadian traffic) ? If so, would this impact costs?
9. Should GCNet contract(s) include International locations

GCNet WAN Services Overview

Next Steps

- Industry one-on-one engagements* (45 min each) to be held for the next 3 days to obtain feedback on the discussion topics
  - Industry feedback will be incorporated into the statement of work
- Initiate next phase of the procurement process (RFRE)



*Note: Suppliers must have pre-registered for the one-on-one sessions; registration is now closed

GCNet WAN Services Overview

Wrap Up & Questions

Questions?

(for Suppliers only)

Break – 15 Minutes

Coffee & Refreshments are available in the lobby

Please return to your seat by 3:00

Service | Innovation | Value

Supply Chain Integrity

GCNet WAN Industry Day

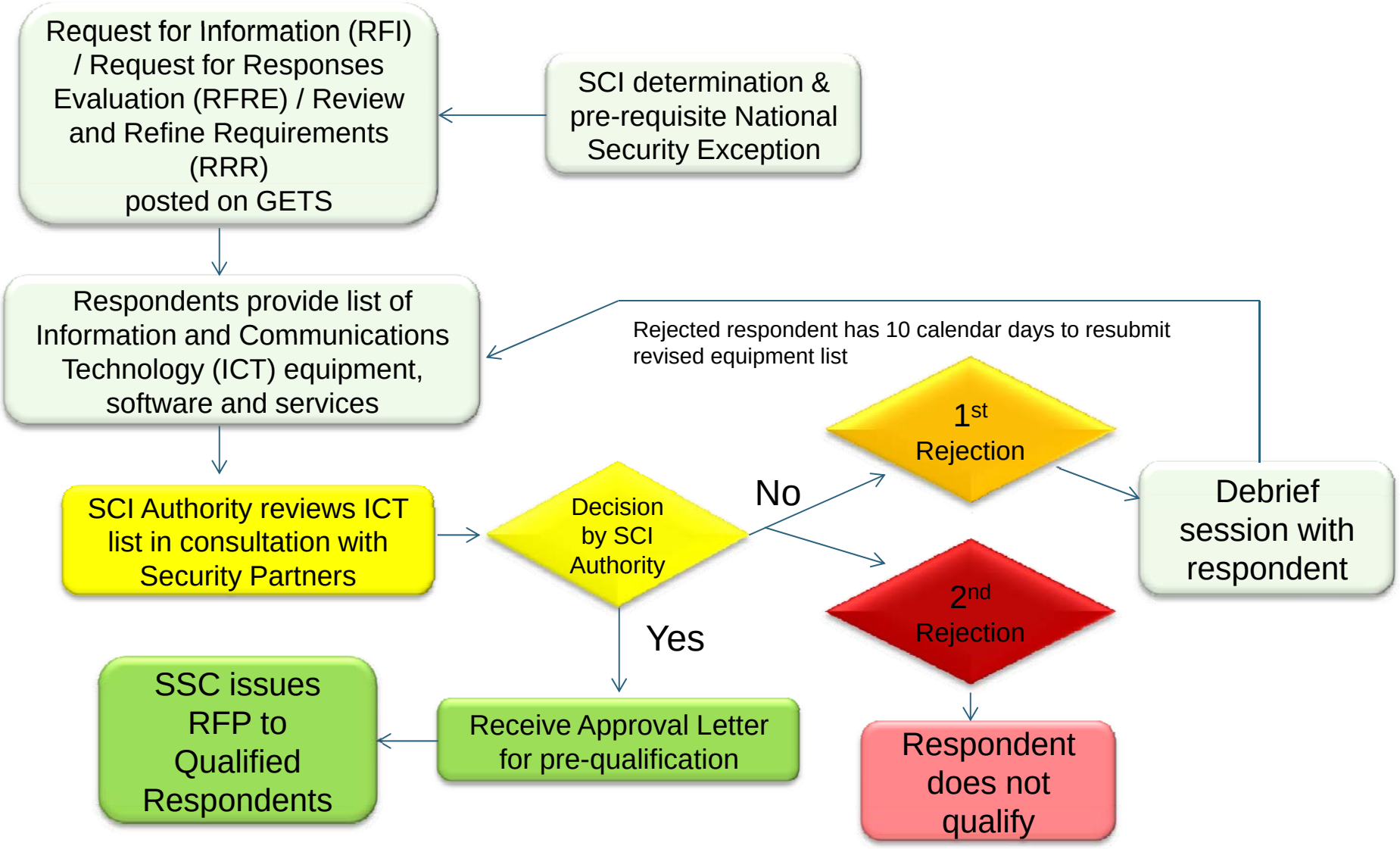
July 9th, 2013

Patrick Mountford, Director, Cyber Security Strategy
Christian Caron, A/Manager, Cyber Threat Assessment Unit

Shared Services Canada | Services partagés Canada

Canada

Two-Step Procurement Process

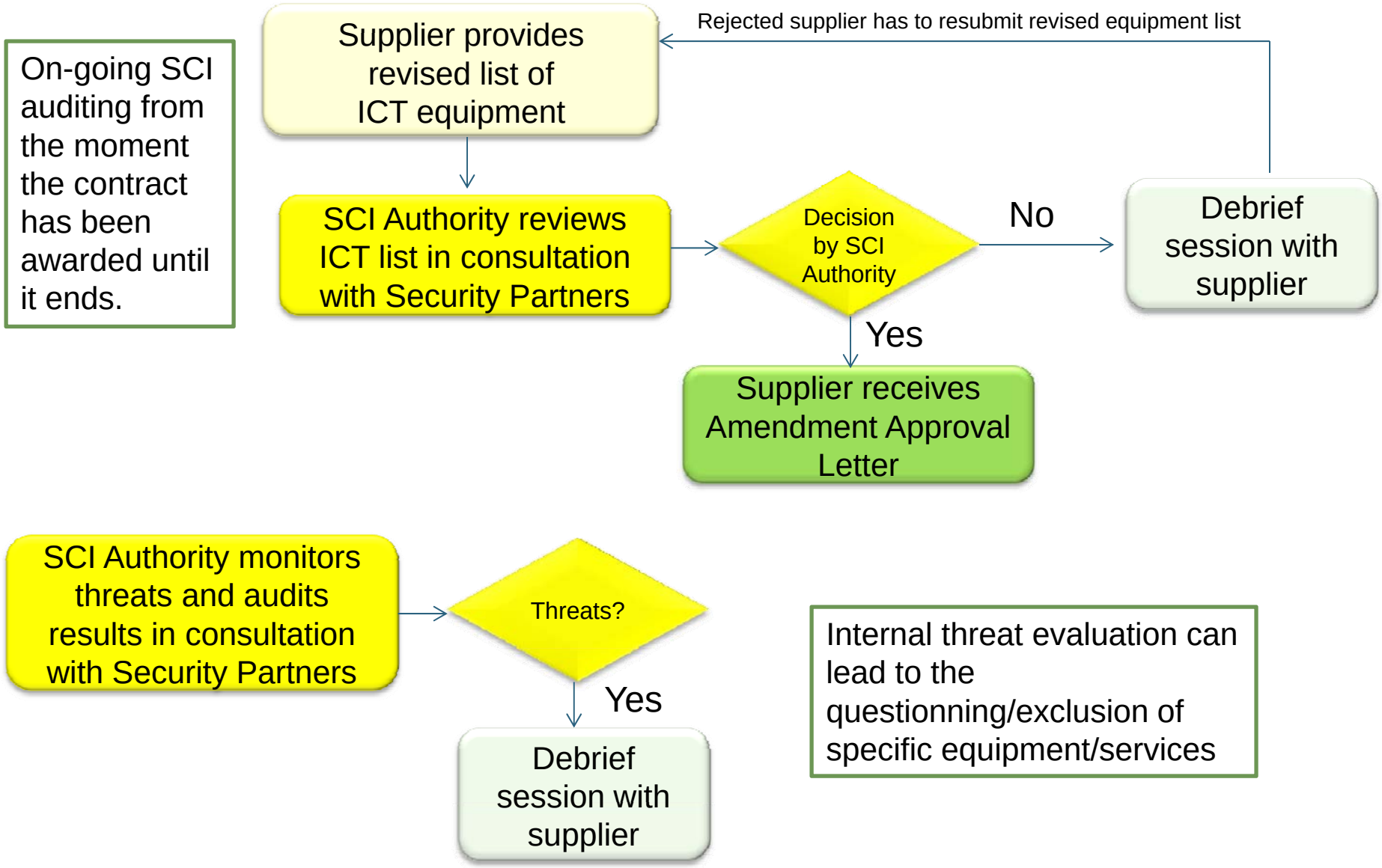


Required Information from the Respondents

- Once the SOW is finalized, GoC will request that the respondents provide their list of IT products and services. More specifically, when it applies, the GoC 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 managed services (names of companies and the location from where these services are delivered).
3. Conceptual network diagrams showing third party dependencies and interconnections (includes physical and logical network topology, depicting the nodes and connections amongst nodes in the network).
4. All of the above applies for sub-contractors and partners (sub-contractor and their own sub-contractors). This should include all companies who will be sub-contracted to provide equipment or services as part of the GCNet Wan project.

On-going Supply Chain Integrity Auditing



Cyber & Supply Chain Threats to the GC

GC WAN
Industry Day

July 9, 2013

Carey Frey, 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 telecommunications networks threatens the sovereignty of GC information and the continuity of government operations**
  - **Cyber threat actors are effective at exploiting internet-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 telecommunications services through GCNet 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 CSEC are working in partnership 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 shared services
  - Companies must be willing to sign a CSEC non-disclosure agreement to receive this information

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

Service | Innovation | Value

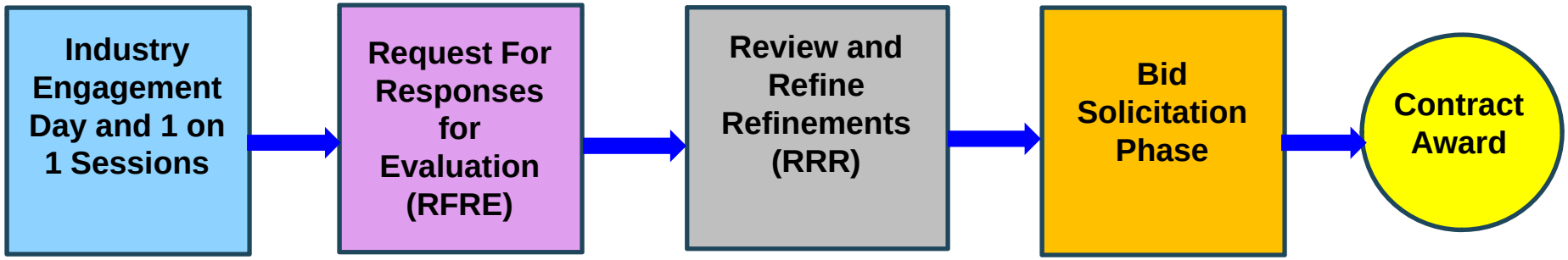
GCNet –WAN Services

Collaborative Procurement Solutions Approach

Stéphane Richard
Shared Services Canada
Senior Director
Procurement and Vendor Relationships

July 9, 2013

Collaborative Procurement Solutions Approach



Note: No Request for Information (RFI) is planned.

Request for Responses for Evaluation (RFRE) Phase

- The purpose is to qualify suppliers who have demonstrated and proven skills and experience in implementing and operating WAN services.
- Evaluation criteria will focus on the supplier's capabilities and experience to deliver WAN services.
- Suppliers who meet the mandatory RFRE evaluation criteria will be deemed Successful Respondents and will proceed to the RRR phase.
- Canada will inform Successful Respondents that, in the "Review and Refine Requirements Phase", a draft Statement of Work (SOW) will be provided to them, and once the SOW is finalized, Successful Respondents will be requested to submit their list of IT products (equipment, software, services and network diagrams) as part of Canada's Supply Chain Integrity process.

Review and Refine Requirements (RRR) Phase

- Canada will provide the Successful Respondents with a draft SOW.
- Canada will collaborate with Successful Respondents to seek feedback and clarification on Canada's requirements to refine the SOW (e.g. one-on-one sessions, Q's and A's, written submissions, etc.).
- Once the SOW is finalized, Canada will request that the Respondents provide their list of IT products.

continued

Review and Refine Requirements (RRR) Phase
(continued)

- Canada will conduct the Supply Chain Integrity (SCI) verification over a period of 10 calendar days to ensure that all IT products meet Canada's security and supply chain standards.
- Upon completion of the SCI verification process, Canada will provide Respondents with written notification informing them if their IT product list are approved.
- If a Respondent's IT products list is not approved, the Respondent will be briefed and have 10 calendar days following the receipt of Canada's written notification to resubmit their IT products list.
- If the Respondent's IT products list is rejected a second time, there will be no further opportunities to resubmit a new IT products list and the Respondent will not be qualified to proceed to the next phase in the procurement process.
- Respondents whose IT product list are approved by Canada will be deemed Qualified Respondents and will proceed to the "Bid Solicitation Phase".

Bid Solicitation Phase

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

Contract Award and Implementation

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

GCNet WAN Services Industry Day

Questions & Answers

GCNet WAN Services Industry Day

Recap / Closing Remarks