



# Shared Services Canada

## Procurement and Vendor Relationships Network & End User Branch

# Network Solutions Supply Chain (NSSC) Vendor Engagement Webinar

Opening Remarks and Objectives

Jason Weatherbie  
Director  
Transformation Initiatives Procurement

July 14, 2015



# Agenda

Time	Presenter	Description
1:00 – 1:10 PM	<b>Jason Weatherbie</b> Director, Transformation Initiatives Procurement, Shared Services Canada	Opening Remarks and Vendor Engagement Webinar Objectives
1:10 – 1:25 PM	<b>Jason Weatherbie</b> Director, Transformation Initiatives Procurement, Shared Services Canada	Collaborative Procurement Solutions Approach
1:25 – 1:35 PM	<b>Alexandre Dorion</b> Manager, Supply Chain Integrity Shared Services Canada	Supply Chain Integrity (SCI) Process
1:35 – 1:45 PM	<b>Jerome Tremblay</b> Security Strategic Relationships Office, Communications Security Establishment Canada	Cyber & Supply Chain Threats to the Government of Canada (GC)
1:45 – 2:40 PM	<b>Tom Brandt</b> Senior Director, Intra-Building Networks Sector Shared Services Canada <b>Jason Weatherbie</b> Director, Transformation Initiatives Procurement, Shared Services Canada	Present SSC Way Forward and NSSC Presentation
2:40 – 3:00 PM	<b>Jason Weatherbie</b> Director, Transformation Initiatives Procurement, Shared Services Canada	Overview of Questions to Vendors, Recap / Closing Remarks. Questions and Answers.

# Vendor Engagement Webinar Objectives

1. SSC is re-engaging with Industry to solicit their feedback.
2. Share Network and End User Branch's (NEUB) plans with Industry vendors and engage in a dialogue regarding the strategy for the Network Solutions Supply Chain (NSSC).
3. Explain the proposed "Collaborative Procurement Solutions" approach.
4. Address the Cyber Security Supply Chain Threat.
5. Solicit written feedback from vendors based on these presentations.



Service | Innovation | Value

# Shared Services Canada

## Procurement and Vendor Relationships

# Network Solutions Supply Chain (NSSC)

## Vendor Engagement Webinar

Collaborative Procurement Solutions Approach

Jason Weatherbie  
Director  
Transformation Initiatives Procurement

July 14, 2015



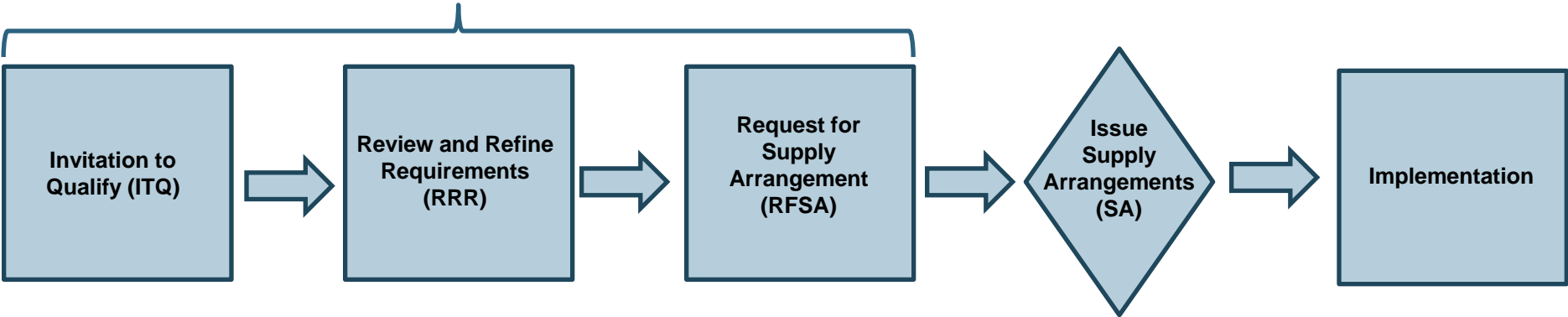
Shared Services  
Canada

Services partagés  
Canada

Canada 

# Collaborative Procurement Solutions

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



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

- The purpose is to qualify suppliers who have demonstrated and proven skills and experience in implementing network solutions.
- Evaluation criteria will focus on the supplier's capabilities and experience to deliver network solutions.
- Suppliers who meet the mandatory ITQ evaluation criteria will be deemed successful "Qualified Respondents" (QRs) and will proceed to the RRR phase.

# Review and Refine Requirement (RRR) Phase

- Qualified Respondents will be provided with a draft Request for Supply Arrangement (RFSA) and Statement of Work (SOW).
- Canada will collaborate with Qualified Respondents to seek feedback and clarification on Canada's requirements to refine the draft Request for Supply Arrangement (RFSA) and Statement of Work (SOW).
- RRR sessions will have various formats (e.g. workshops, one-on-one sessions, Q and A documents, etc).

- Canada may issue one or more formal Request for Supply Arrangements(s) (RFSA(s)) directly to the Qualified Respondents who have participated in the RRR phase.
- Each Qualified Respondent will be permitted to formally bid on the requirements set out in the RFSA(s).



- Supply Arrangement issuance will occur after completion of the RFSA Phase.
- One or more agreements may be awarded depending on the Request for Supply Arrangements.



# Shared Services Canada Cyber and IT Security Branch

## Network Solutions Supply Chain (NSSC) Vendor Engagement Webinar

Supply Chain Integrity (SCI)  
Process Overview

Alex Dorion  
Manager  
Supply Chain Integrity

July 14, 2015



# Agenda

- ✓ Supply Chain Integrity (SCI) Process
- ✓ Supply Chain Security Information (SCSI)
- ✓ Scope & Templates
- ✓ Assessment
- ✓ Outcome

# Supply Chain Integrity (SCI) Process

- ✓ The purpose of the Supply Chain Integrity (SCI) process is to ensure that no un-trusted equipment, software or services are procured by SSC and are used in the delivery and/or support of Government of Canada (GC) services.
  - Verify integrity of origin, elements, operation and route of travel.
- ✓ **SCI process can be applied to any phase of procurement, but the RFSA stage is preferred due to a clearer set of requirements.**
- ✓ Qualified Respondents or Bidders must successfully pass the SCI process in order to be able to continue to participate in the procurement process.\*
- ✓ SCI clauses and requirements are integrated into the terms and conditions of the solicitation.
- ✓ SSC competitive procurements are covered by the National Security Exception (NSE), which removes the trade agreement obligations related to national security.

\*Flexibility to be pre- or post- SA issuance:

Timing of SCI may be during the RFSA phase and/or issuing of SAs phase.

# Supply Chain Security Information (SCSI)

- ✓ Qualified Respondents (QRs) will be required to submit their SCSI package to the Contracting Authority before the required deadline as set out by the procurement schedule.
- ✓ The mandatory SCSI elements are:

## **IT Product List:**

- 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 (including Workplace Technology Devices) that operates at the data link layer of the OSI Model (i.e. Layer-2) and above, and related software.
- Products used by both the primary Bidder and by each of their proposed subcontractors in any context (installation, testing, production, delivery, support, maintenance, etc.) .

## **Network Diagrams:**

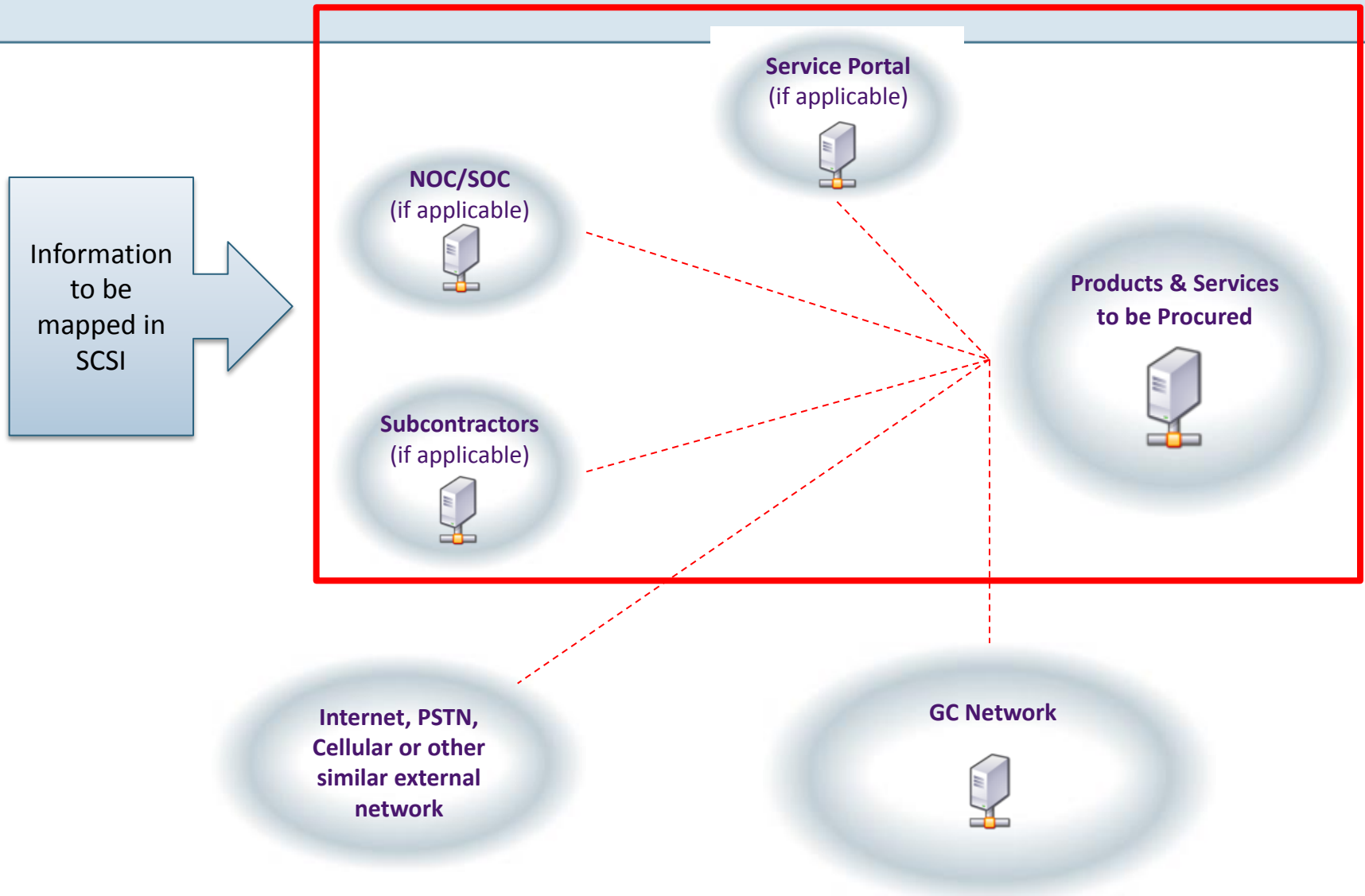
- Conceptual architecture diagrams\* indicating location of IT Products so as to provide context for usage .

## **List of Subcontractors:**

- All subcontractors that could be used to perform any part of the Work pursuant to the resulting contract (including subcontractors that are affiliated or otherwise related to the Bidder).

\*Dependent on a per solution basis. Example: no diagram required for one box solution.

# SCSI Scope



# SCSI Templates

- ✓ Spreadsheet templates will be provided to the Bidders as part of the solicitation.

FORM B - IT Product List							
Line Item #	Location (a)	Product Type (b)	IT Component (c)	Model Name/ Number (d)	Description and Purpose (e)	Product Manufacturer and/or Software Publisher (f)	Name of subcontractor (g)

FORM B - Subcontractor List			
Name of the Subcontractor (a)	Address of the Subcontractor's headquarters (b)	Portion of the Work that would be performed by the Subcontractor (c)	Location(s) where the Subcontractor would perform the Work (d)

- ✓ Bidders are requested not to repeat multiple iterations of the same Product (e.g. if the serial number, location and/or color is the only difference between two products, they are considered the same Product).
- ✓ Assessment of the SCSI requires that a complete package be submitted before the established deadline.

# Supply Chain Assessment

- ✓ SSC/CITS provides the Supply Chain Security Information (SCSI) to Communications Security Establishment (CSE) for assessment, as received from prospective Bidders.
- ✓ CSE assesses the SCSI, provides recommendations and mitigation measures regarding potential risks to national security from a confidentiality, integrity and availability point of view.
- ✓ Based on the supply chain risks, recommendations and the potential mitigation measures, SSC makes a business decision on how to address any concerns.
- ✓ Bidders will be notified in a formal letter of any items of concern, the required mitigation measures and a timeline for implementation.
  - Making the needed changes in time will ensure your SCSI gets approved.
  - If required, SSC may choose to conduct a debrief session to further clarify any aspect of the assessment.

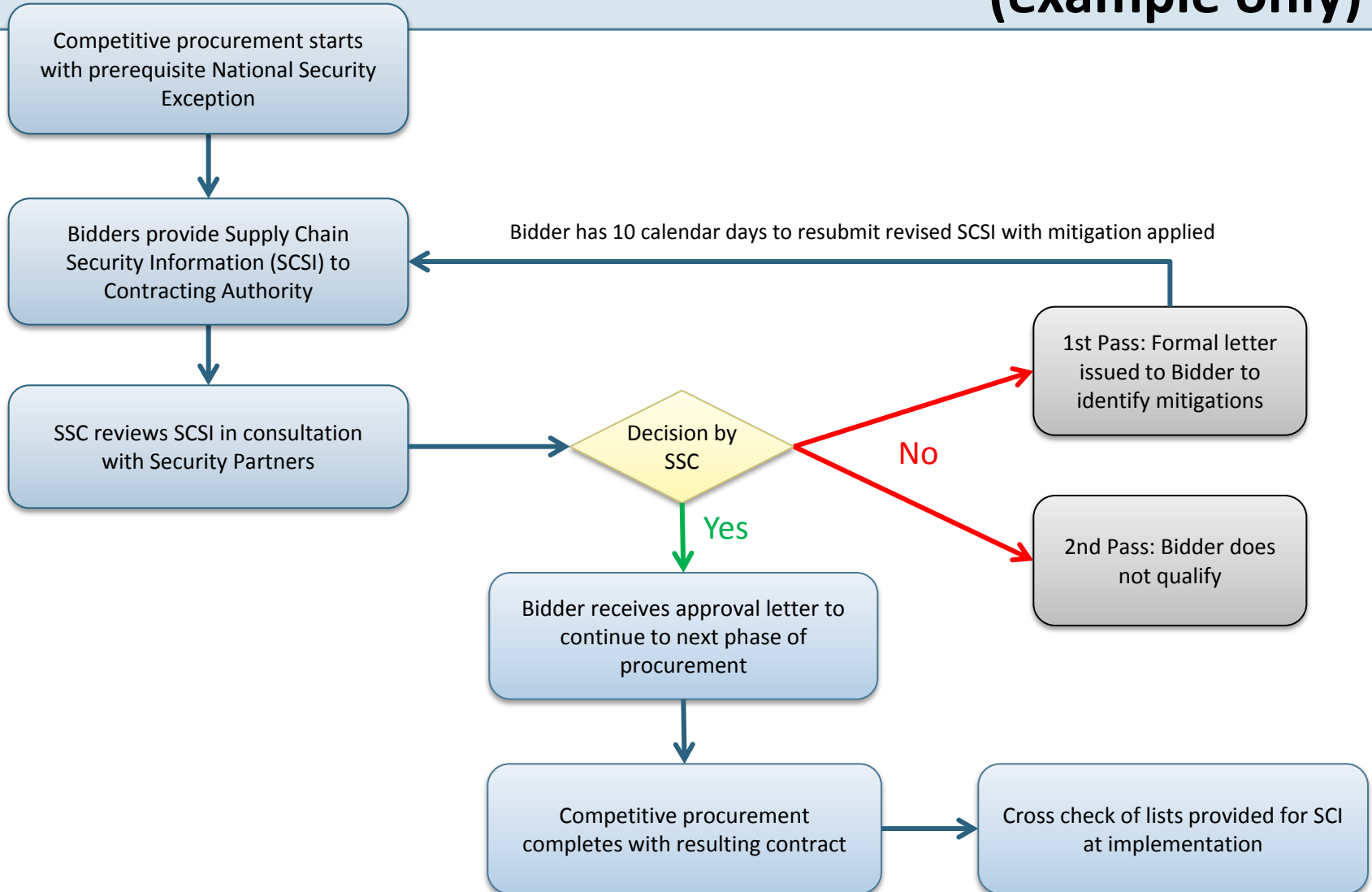


# Outcome of Assessment

- ✓ Bidders will only have two opportunities to submit SCSi packages.
- ✓ Bidders are required to propose a solution consistent with the version of the SCSi it submits as part of this SCI process.
- ✓ Once a Bidder's SCSi has been approved by Canada, no modifications are permitted except under exceptional circumstances, as determined by Canada.
- ✓ Resulting contracts will have SCI clauses included in the Terms & Conditions to:
  - facilitate Contractor or SSC initiated changes to SCSi
  - establish a regular audit cycle to keep SCSi up to date and assessed
  - address subcontractor "Change of Control"

# SCI Process Flowchart

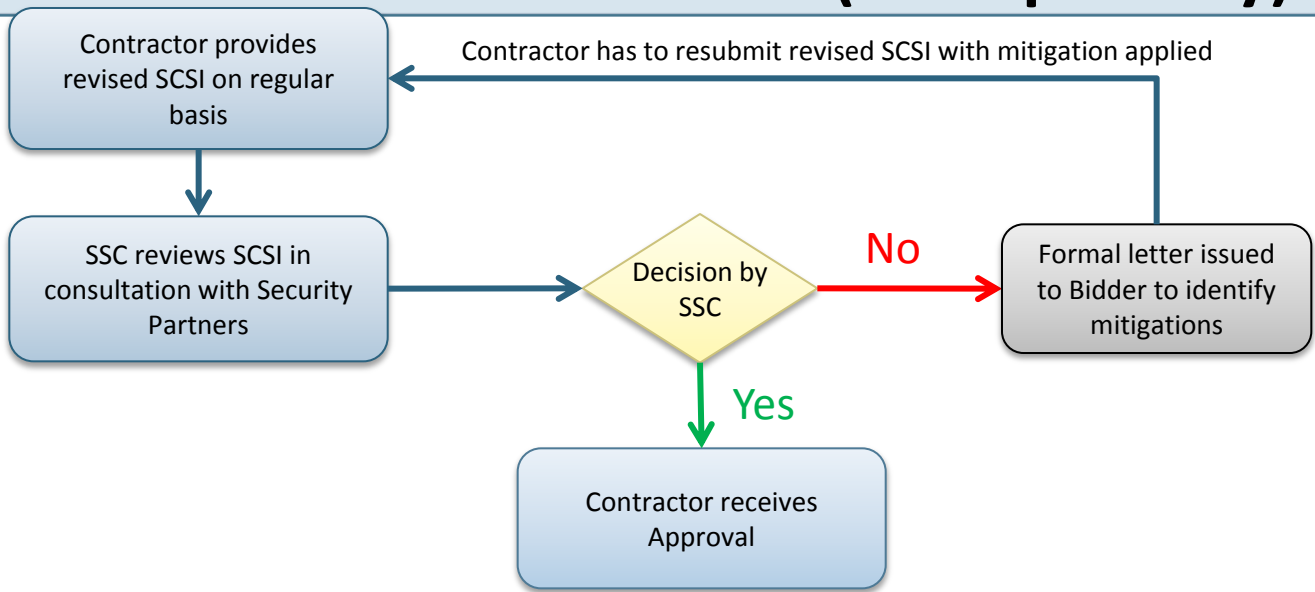
(example only)



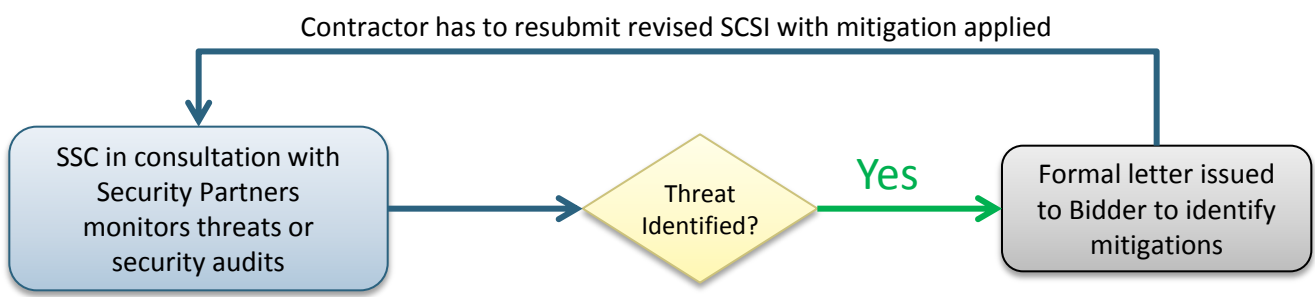
# Post-Contract SCI Auditing Flowchart

(example only)

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?

Please reserve questions  
for the end of all  
presentations.



# Cyber & Supply Chain Threats to the Government of Canada (GC)

## Network Solutions Supply Chain (NSSC)

July 14th, 2015

Jérôme Tremblay – Advisor, Cyber Security  
Communications Security Establishment (CSE)



# 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

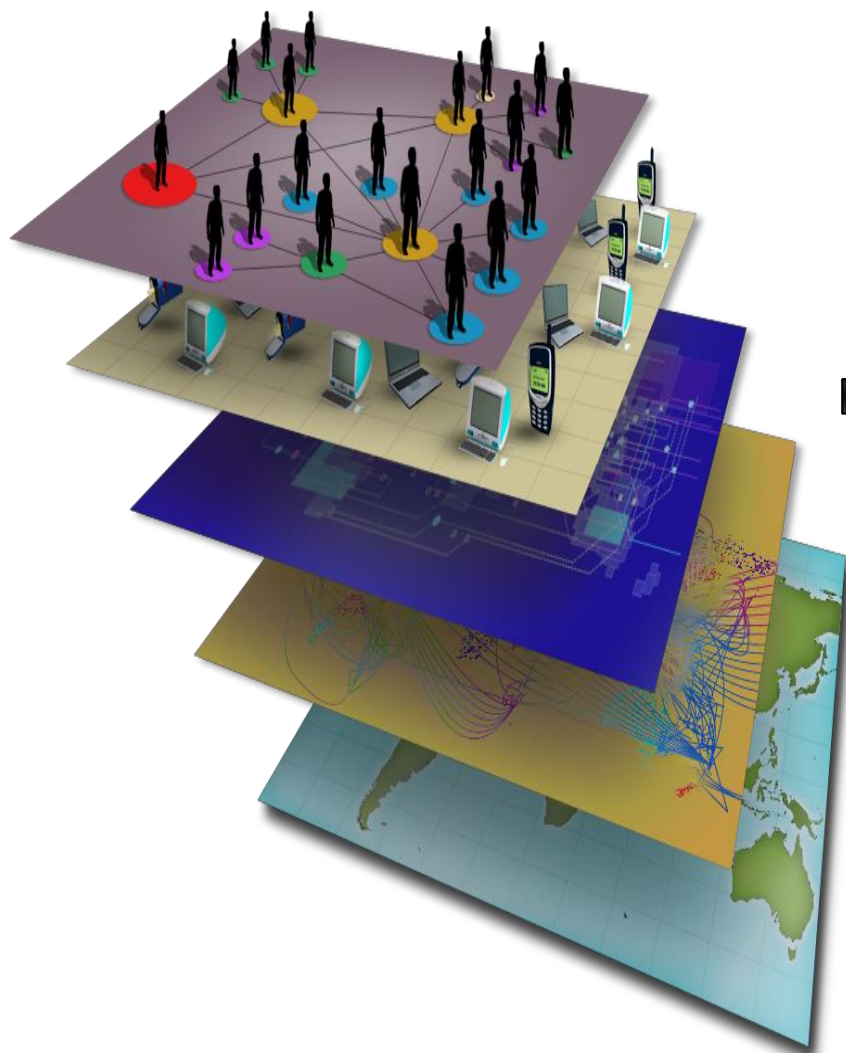
- Today, malicious cyber activities are directed against Canada and our closest allies on a daily basis.
- Threat actors range in sophistication from malfeasant hackers to organized crime groups, to terrorists to nation states.
- Canadians trust the GC to defend Canada's cyber sovereignty and protect 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

# Worst Case Scenario

- Complete and persistent network access by the adversary.
- While it is unlikely a foreign state would carry out attacks aimed at disrupting or denying communications in times of peace, the risk of such attacks would be high in a time of any given conflict.
- In a conflict scenario, it would be too late to implement a robust defence against a compromised communications backbone.

# 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.

# Cyber Supply Chain Issues

---

## **Cyber Supply Chain Issues**

Technology is *evolving too quickly* for legislation.

---

No *international framework or standard guidance* for cyber supply chain guidance.

---

*Reliance on globally sourced IT equipment* exposes system/networks to a larger risk of untrusted vendors.

---

Organizations are being driven into *'The Cloud'*.  
*Interconnections between complex computer networks and software* are ubiquitous.

---

Organizations are increasingly *procuring COTS software or outsourcing development*, but procurement processes do not account for the issues of a complex supply chain.

---

# 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 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.
- If required, CSE will provide follow-up briefings on supply chain risk mitigation to interested suppliers for GC shared services.
- 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?

Please reserve questions for the end of all presentations.





Service | Innovation | Value

# Shared Services Canada

## Procurement and Vendor Relationships Network & End User Branch

# Network Solutions Supply Chain (NSSC) Vendor Engagement Webinar

## SSC Way Forward and NSSC Presentation

Tom Brandt  
Senior Director  
Intra-Building Networks Sector

Jason Weatherbie  
Director  
Transformation Initiatives Procurement

July 14, 2015



Shared Services  
Canada

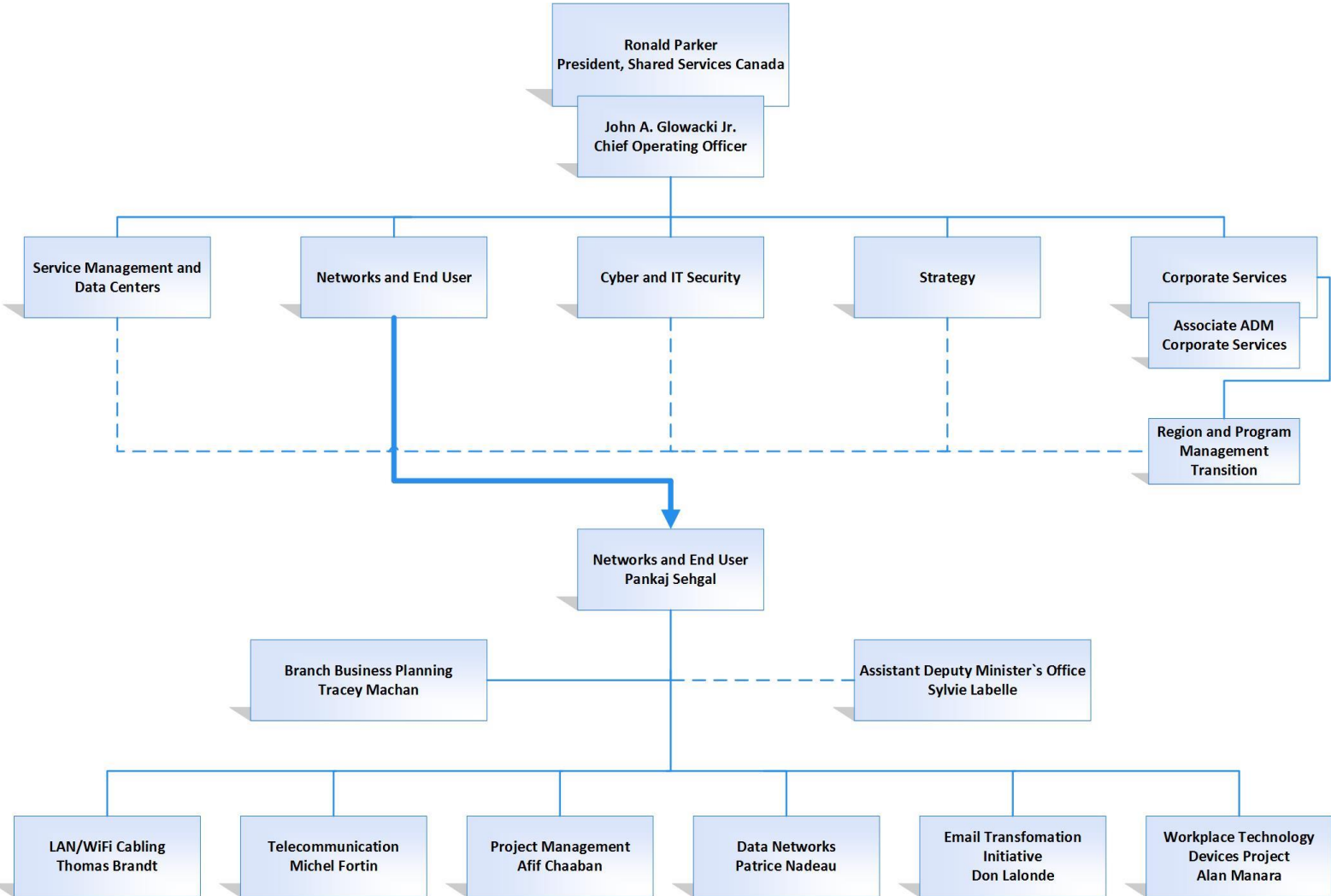
Services partagés  
Canada

Canada 

# SSC Way Forward – Moving from Planning to Implementation

- As SSC enters its third year of operation, the Department is increasingly focused on transformation and the shift from planning to implementation.
- SSC will need to balance competing demands of managing two IT infrastructure contexts: (i) the legacy environment and (ii) the transformed end state.
- Savings, security and service are the measures by which SSC will gauge success.
- SSC will continue to engage Partner Departments to confirm business requirements and align the Partner Department's schedules with SSC departmental priorities.
- Consultations with industry will continue to play a part as SSC refines its approach with respect to building and managing the IT infrastructure.
- Internally, SSC will reinforce the importance of managing and leading change and adopting a 'One SSC' approach to both.
- SSC is transforming internally in lockstep with the execution of its transformation plan.

# New Departmental Structure



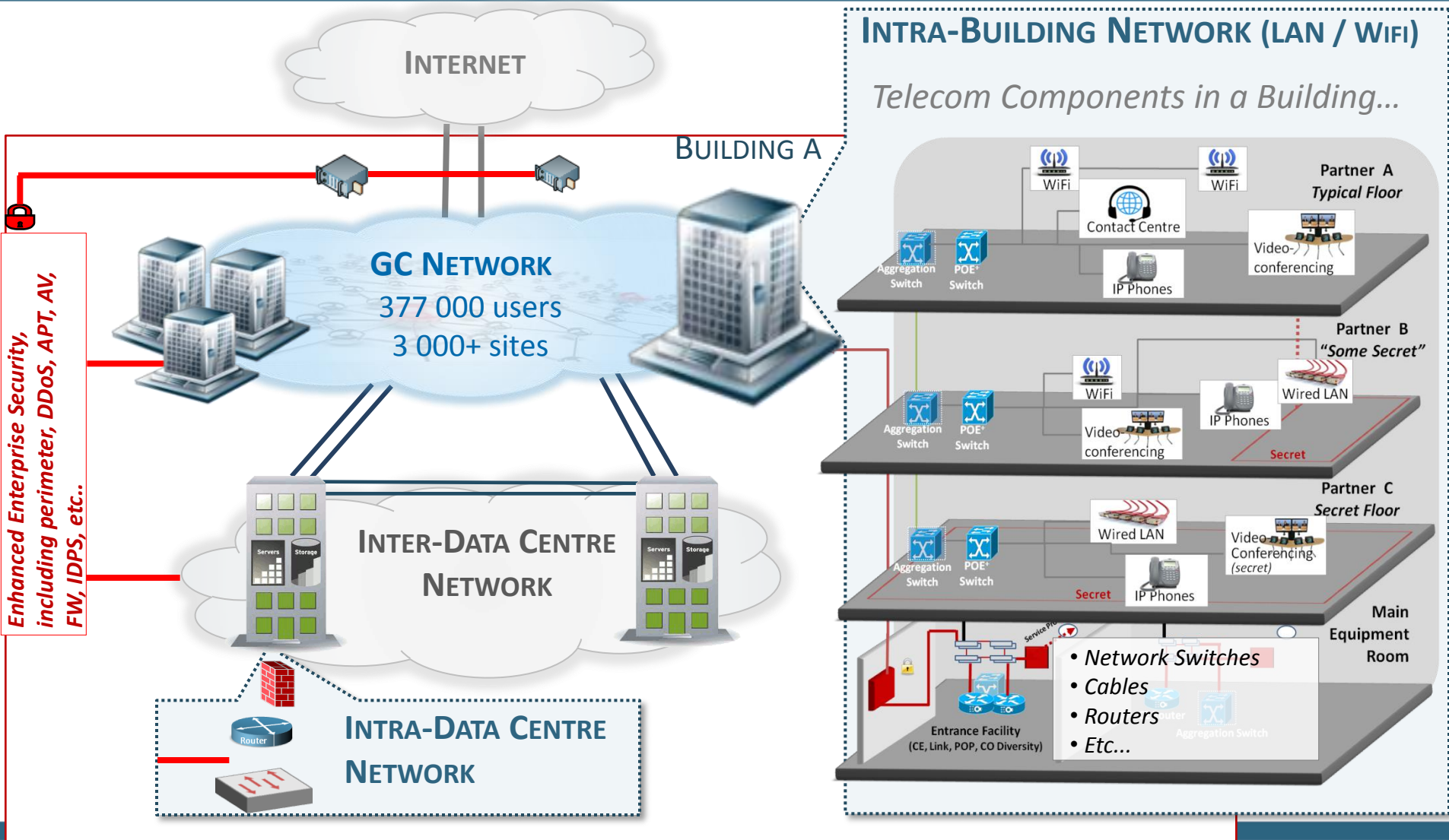
# SSC Transformation Plan – *Business Requirements*

- **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 earlier) and IT Security controls for all components and services.

# SSC Transformation Plan – *Functional Requirements*

- **Integration** across technology types.
- **Adoption of Industry 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 review of Total Cost of Ownership** to ensure best value to Canada.
- Must support a **secure, multi-tenant environment** (GC Domains and Zones).
- Must support the **changing IT Security landscape** and threat environment through technology and services.

# SSC Transformation Overview – Service Components



# Strategic Context

- SSC operates network infrastructure services across the GC, which currently comprises over 70,000 network devices, including more than 40,000 LAN switches and routers and over 550 firewalls.
- Current service delivery model is GC-owned and operated for LAN, Data Centre Network (DCN), and IT Security services, supported by 2 primary procurement vehicles:
  1. **Network Equipment Support Services (NESS)** standing offer - used to obtain networking and network security equipment and related services (installation and configuration).
  2. **Network Infrastructure Management Services (NIMS)** - used for maintenance services.
- Two key challenges with current procurement vehicles include:
  - NESS does not support the procurement of **Solutions** (only components).
  - Existing procurement vehicles have been extended several times.
- Numerous other procurements take place outside of these vehicles to meet SSC requirements in order to achieve “solutions” outcomes for SSC clients.

# Quick History on NSSC and Next Steps

1. The NSSC initiative started with the Data Centre Networks (DCN) Industry Day\* back in February 27, 2014.
2. Once Industry feedback and one-on-ones were completed, SSC incorporated DCN into the NSSC initiative.
3. The NSSC initial Industry Day\*\* took place May 28, 2014 and SSC requested feedback and received responses from Industry.
4. Since that time, SSC has considered a couple of different options.
5. Given the size, complexity, scope and scale of this procurement, SSC wants to ensure that we create effective procurement vehicles that meet the needs of our Way Forward business models.
6. SSC will present two options during this session and pose questions for Industry to review and provide feedback.

\* Please see DCN Industry Day materials here: <https://buyandsell.gc.ca/procurement-data/tender-notice/PW-14-00618340>

\*\*Please see NSSC Industry Day materials here: <https://buyandsell.gc.ca/procurement-data/tender-notice/PW-14-00635469>



# NSSC Guiding Principles

- Adoption of technology industry standards to ensure flexibility, compatibility (eg. QoS) 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.
- Must balance competition with minimizing the number of procurement vehicles.
- Must provide best value and reduce total cost of ownership (TCO) for the operations and management of services over entire contracting period.
- Solutions should be acquired to ensure interoperability and compatibility between procured and existing solutions/services.

# NSSC Scope

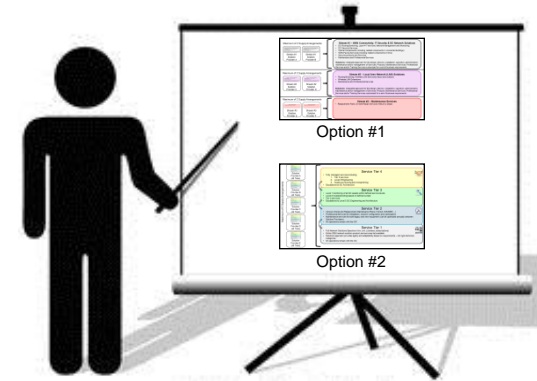
- Establish a new procurement vehicle for network and security products and solutions that are flexible enough to support: national locations for SSC and SSC clients for:
  - Local Area Network;
  - DC network;
  - WAN Connectivity;
  - IT Security Services; and
  - maintenance of existing (legacy) network products and security products and services.
- Details to follow on the overview of options slides.

# Solution Definition

Integrated approach for the design, delivery, installation, operation, administration, maintenance and/or management of Services, Products, Maintenance Services, Professional Services and/or Training Services customized for a set of business requirements.

# Overview of Options

1. SSC will present the following two options and pose questions for Industry to review and provide feedback.
2. SSC is also open to other viable strategies if they ensure best value and service to the Crown.



# Option #1 – Technology and Solutions Streams

## 2 Supply Arrangements

Stream #1 – WAN Connectivity, IT Security & DC Network Solutions

- DC Routing/Switching, Layer 4-7 services, Network Management and Monitoring
- DC Security Services
- Optical Components (including related components in connected buildings)
- WAN-Facing Services (including related components in DCs)
- Network Operations and Services
- Maintenance and Professional Services

Business: Integrated approach for the design, delivery, installation, operation, administration, maintenance and/or management of Services, Products, Maintenance Services, Professional Services and/or Training Services (submitted for a set of business requirements).

**Stream #1  
Solution  
Provider A**

Stream #1 – WAN Connectivity, IT Security & DC Network Solutions

- DC Routing/Switching, Layer 4-7 services, Network Management and Monitoring
- DC Security Services
- Optical Components (including related components in connected buildings)
- WAN-Facing Services (including related components in DCs)
- Network Operations and Services
- Maintenance and Professional Services

Business: Integrated approach for the design, delivery, installation, operation, administration, maintenance and/or management of Services, Products, Maintenance Services, Professional Services and/or Training Services (submitted for a set of business requirements).

**Stream #1  
Solution  
Provider B**

### Stream #1 – WAN Connectivity, IT Security & DC Network Solutions

- DC Routing/Switching, Layer 4-7 services, Network Management and Monitoring
- DC Security Services
- Optical Components (including related components in connected buildings)
- WAN-Facing Services (including related components in DCs)
- Security products and Services
- Maintenance and Professional Services

## 2 Supply Arrangements

Stream #2 – Local Area Network (LAN) Solutions

- Routing/Switching, Wireless LAN Services (indoor and outdoor)
- Network Operations and Services
- Maintenance and Professional Services

Business: Integrated approach for the design, delivery, installation, operation, administration, maintenance and/or management of Services, Products, Maintenance Services, Professional Services and/or Training Services (submitted for a set of business requirements).

**Stream #2  
Solution  
Provider C**

Stream #2 – Local Area Network (LAN) Solutions

- Routing/Switching, Wireless LAN Services (indoor and outdoor)
- Network Operations and Services
- Maintenance and Professional Services

Business: Integrated approach for the design, delivery, installation, operation, administration, maintenance and/or management of Services, Products, Maintenance Services, Professional Services and/or Training Services (submitted for a set of business requirements).

**Stream #2  
Solution  
Provider D**

### Stream #2 – Local Area Network (LAN) Solutions

- Routing/Switching, Wireless LAN Services (indoor and outdoor)
- Wireless LAN Extensions
- Maintenance and Professional Services

## 2 Supply Arrangements

Stream #3 – Maintenance Services

- Replacement Parts, On-Site Repair Services, Return to Depot

**Stream #3  
Solution  
Provider E**

Stream #3 – Maintenance Services

- Replacement Parts, On-Site Repair Services, Return to Depot


**Stream #3  
Solution  
Provider F**

### Stream #3 – Legacy & Maintenance Services

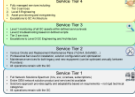
- Replacement Parts, On-Site Repair Services, Return to Depot
- Maintenance Services for products procured in Streams 1 and/or 2

# Option #2 – Integrated Solutions Tiers


Maximum of 5 Supply Arrangements



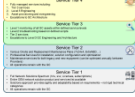
Solution Provider A  
(All Tiers)




Solution Provider B  
(All Tiers)



Solution Provider C  
(All Tiers)




Solution Provider D  
(All Tiers)




Solution Provider E  
(All Tiers)

### Service Tier 4




- Fully managed services including:
  - Tier 3 services
  - Level 3 Engineering
  - Asset provisioning and evergreening
- Escalations to GC Architecture

### Service Tier 3




- Level 1 monitoring of all GC assets within defined service levels
- Level 2 troubleshooting based on GC-defined scripts
- Tier 2 services
- Escalations to Level 3 GC Engineering and Architecture

### Service Tier 2



- Various Onsite and Replacement Maintenance Plans for proposed OEM product list in Tier 1
- Maintenance services for legacy equipment (can be optimized annually between Solution Providers)
- Professional Services for installation, solution configuration and optimization
- All operations remain with the GC

### Service Tier 1



- Full Network Solutions Spectrum LAN, WAN, DC, Security (H/W, S/W, Licenses, subscriptions)
- Entire OEM network and security products list available
- Accountable for full integration of proposed OEM products (Routers; LAN Switches; Wireless; Layer 4-7 Switches; Optical components; WAN Optimizers; Security Devices; (Firewall, IPS, VPN); etc...)
- All operations remain with the GC

# Proposed Procurement Model for both Options #1 and #2

1. All requirements are expected to be competed (RFP or RFQ) regardless of dollar value.
  - For specific exceptions, requirements up to **\$1M** will be ordered through a Call-up process for emergency or other situations.
2. The NSSC would be a Supply Arrangement with up to a maximum of six (6) Solution Providers capable of supporting all services identified.
3. A Call-up could be for a capital purchase or a multi-year service order or combination thereof.
4. RFx pricing will update the Supply Arrangement pricing tables (any price from an RFQ will now be the new price for that product/service).

# Next Steps

- SSC is asking questions on the next few slides (and also included in a question package to be posted on Buy and Sell).
- Industry feedback on presentations to be received by July 17, 2015, 4:00 PM.
- There may be follow-up questions/clarifications with vendors that provide written feedback.
- Evaluate input/feedback received to refine procurement and sourcing strategy.
- Incorporate feedback into the development of the ITQ.





# Shared Services Canada

## Procurement and Vendor Relationships Network & End User Branch

# Network Solutions Supply Chain (NSSC) Vendor Engagement Webinar

Overview of Questions to Vendors

Jason Weatherbie  
Director  
Transformation Initiatives Procurement

July 14, 2015



# Key discussion topics and questions for Industry feedback

## Question 1

- Scope
  - a. Is the scope of the NSSC procurement vehicle clear to you?
  - b. Is the intent of both procurement options clear to you? If not, please clarify.
  - c. Of the two options presented, which do you prefer? And why?
  - d. Please outline the Pros and Cons of each Option.

# Key discussion topics and questions for Industry feedback

## Question 2

- Option #1 - Technology and Solutions Streams
  - a. Is delivering any of these 3 streams obtainable for you?
  - b. If you believe that the above is not achievable, what business model would you propose that ensures SSC is provided the best value and service?

# Key discussion topics and questions for Industry feedback

## Question 3

- Option #2 - Integrated Solutions Tiers
  - a. Is delivering on all 4 integrated service tiers obtainable for you?
  - b. Could you partner with other suppliers to deliver all 4 tiers?
  - c. If you believe that the above is not achievable, what business model would you propose that ensures SSC is provided the best value and service?

# Key discussion topics and questions for Industry feedback

## Question 4

- Maintenance pricing

Today, using existing vehicles, SSC procures individual annual maintenance requirements that can be over \$1M dollars each.

- a. How would you propose SSC manage requirements of \$1M (and above) that impact large volume maintenance requirements?

# Key discussion topics and questions for Industry feedback

## Question 5

- RFQ/Call-up pricing

Once a Solution Provider bids during an RFQ (win or lose) the price quoted will be the Solution Provider's new revised price for that product or service.

- a. Please provide feedback.
- b. If the above is not effective, what do you propose to ensure best pricing for SSC?

# Key discussion topics and questions for Industry feedback

## Question 6

- Savings
  - a. Which of the two options (Streams or Tiers) do you anticipate the Crown achieving the best savings possible and why?
  - b. If these two options are not viable, what alternative option(s) do you recommend for the Crown to obtain Best Value?

# Key discussion topics and questions for Industry feedback

## Question 7

- Other considerations/factors:
  - a. What are the other considerations/factors that the Crown needs to take under advisement?



## Closing Remarks

- Thank you for participating in our engagement session.
- The Question Package will be on the Buy and Sell website.
- The intention is to solicit vendor feedback on the options presented as well as any other suggestions vendors may have.
- At SSC's discretion, we may initiate one-on-one sessions with those vendors that responded to the questions and that require additional clarification.
- Once vendor feedback is received and one-on-ones are completed, SSC will incorporate it into the NSSC strategy.
- Industry feedback on presentations to be received by Friday July 17, 2015, 4:00 PM.