Conferencing & Operator Assisted Services (COAS)

Industry Day

Prepared by: SSC Conferencing Services in conjunction with Enterprise IT Procurement

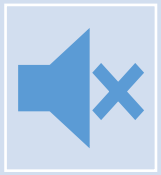
January 26, 2022

Shared Services Canada | Services partagés Canada

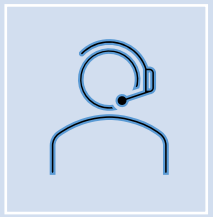
Canada

Instructions

This is a *Microsoft Teams* conference (Slido Instructions); the session will not be recorded



All lines will be muted until the Question and Answer (Q&A) period



We invite and will respond to your questions in both French and English however the presentation will be predominantly provided in English

The process for asking questions for the Q&A portion of the session will be explained further in this presentation

Industry Day Agenda

Welcome, Introductions & Background	Tim St-Jean, Director General, Conferencing Services
Context & Service Overview (portal, pricing etc.)	Charbel El-Helou, Director, Conferencing Services
Procurement Process	Daniel Clement, Manager, Enterprise IT Procurement
Supply Chain Integrity Overview	Sophia Cheaitani, A/Director, Security Architecture & Oversight
Recap, Q&A, Closing Remarks	Tim St-Jean, Director General, Conferencing Services

Welcome & Introductions

Presented by: Tim St-Jean

Shared Services Canada

- Conferencing Services Team
- Enterprise IT Procurement Team
- Supply Chain Integrity Team

Content and Service Overview

PRESENTED BY:

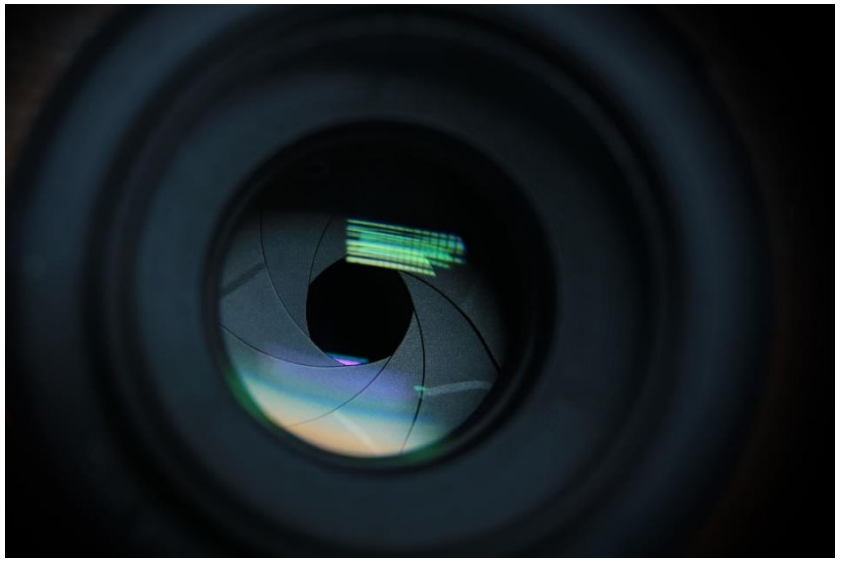
Charbel El-Helou
Director,
Conferencing Services

COAS VISION

"A fully outsourced cloud based service that will provide a modern, bilingual, accessible and reliable service to deliver audio conferencing, web conferencing and Operator Assisted Services to over 180 Government of Canada Departments, Agencies and Crown Corporations serving Canadians and Canadian interests both domestically and internationally."

COAS Objectives

- Service Deliverables
  - Customer experience
  - Modern, accessible and reliable
  - Standardized approach aligned with GC business culture
  - Scalable and flexible
- Service Benefits
  - Adapt to the GC's evolving conferencing needs
  - Agility in scheduling Operator Assisted Conferences
  - Improved financial stewardship



COAS: A suite of services…

1. Audio Conferencing

- Services are provided by the Vendor's own conferencing platform(s)

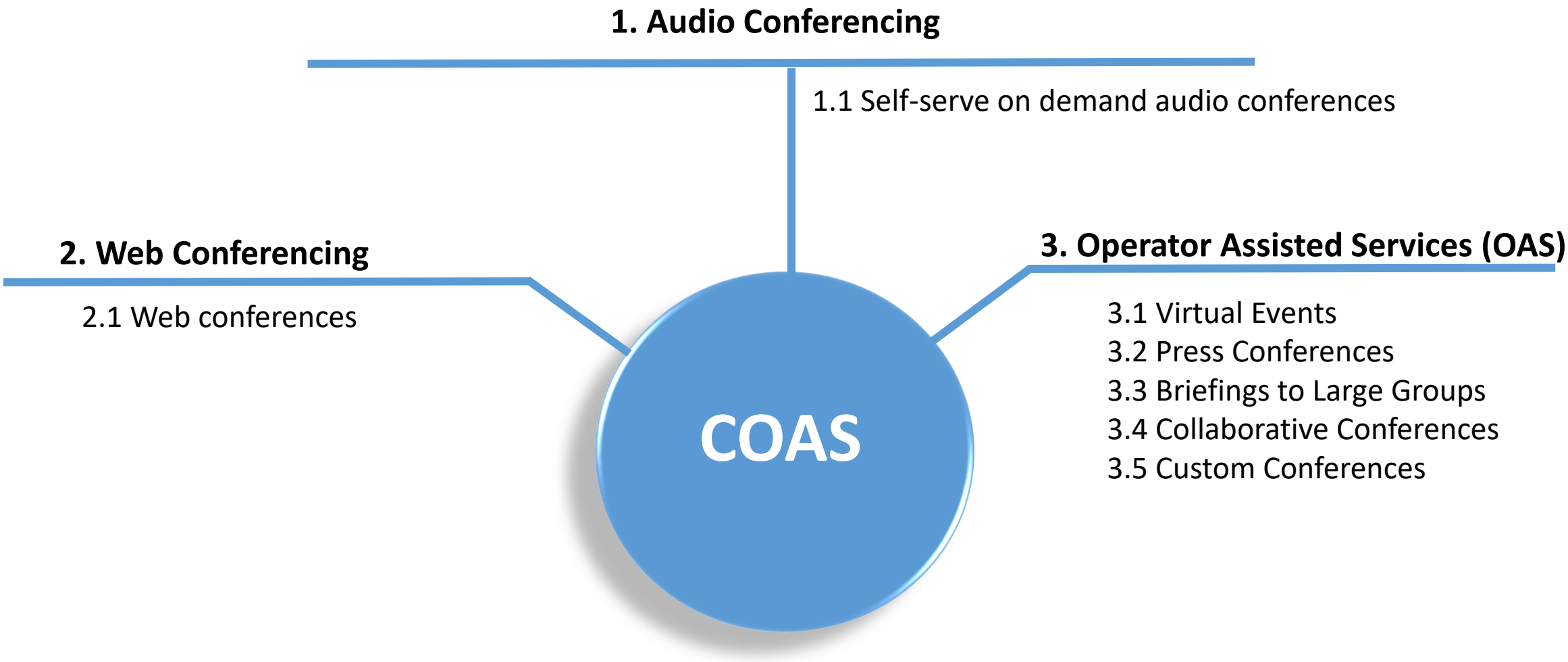
2. Web Conferencing

- Services are provided by the Vendor's own conferencing platform(s)

3. Operator Assisted Services (OAS)

- **Stream 1:** Services are provided by the Vendor's own conferencing platform(s)
- **Stream 2: Optional Future Solution** Services **to be** provided by the Vendor's resources leveraging the Government of Canada's conferencing platforms

COAS: Service Product Breakdown



COAS: High Level Requirements

- **Cloud based:** Underlying conferencing platform; aligned with SSC 3.0 Departmental Strategy
- **Compliant:** in accordance to Official Languages Act, Accessibility Act and Privacy Act
- **Secure:** Currently projected to be Protected A
- **Supported:** Help Desk support for all users
- **Provisioned**: Capacity from a service delivery and resourcing standpoint
- **Self-serve portal:** service management and client use

Industry Feedback

SSC has conducted a thorough review of lessons learned and feedback received from Industry from past procurement initiatives similar to this one.

In order to ensure success, SSC is looking for feedback on the following topics:

1. Conferencing industry standards (what has evolved?)
2. OEM capabilities and any limitations
3. Bilingualism
4. Accessibility
5. Security & privacy
6. Operator capabilities
7. Cost model for pricing and billing

Following the Industry Day, SSC will provide Questions asking for responses from the Industry, and welcomes additional questions and feedback to SSC.

Break – 5 Minutes

Procurement Process

PRESENTED BY:

Daniel Clement
Manager,
Enterprise IT Procurement

COAS Procurement – Industry Day

Purpose: Canada is engaging the Industry to communicate SSC's Conferencing and Operator Assisted Services requirements and to collaborate with the conferencing community through feedback, questions and answers.

1. Feedback and questions can be posed to Canada **during** this session in an open, transparent and anonymous forum via Slido; all questions and answers captured during today's session will be **posted on Buy and Sell**.
2. Vendors will have a **second opportunity** to submit additional questions and feedback **within 5 days following Industry Day**. Follow-up questions and responses will also be posted on Buy and Sell.
3. Vendors may also **request a 1-on-1 virtual session** with Canada in writing **up to three (3) days after the Industry Day**.

1-on-1 Virtual Sessions (post Industry Day)

- Canada recognizes and extends the offer to interested vendors to collaborate with SSC in follow-up 1-on-1 session(s).
- Vendors are invited to request a two (2) hour session by sending an email to the Contracting Authority **up to 3 days after Industry Day.**
- All questions and answers other than those deemed proprietary by Canada will be posted to Buy and Sell.
- Vendors are encouraged to ask their questions in the language of their choice.

COAS Industry Day

	COAS Industry Day and 1-on-1 Meeting					
	Topic	**Frequency**	**Attendees**	**Date/ Time**	**Location**	**Areas of Discussion**
	Industry Day Meeting – January 26, 2022					
1	**General Overview**	1			Virtual via MS Teams	• Business Requirements • Procurement Process • SCI • Next Steps
	1-on-1 Meetings (2 hours each - either 09:00 to 11:00 *OR* 13:00 to 15:00) available from February 7 -18, 2022					
2	**Vendor Meeting 1**	1 per Vendor			Virtual via MS Teams	Vendor's Choice

COAS Procurement – RFP Phase

- Canada values Industry feedback which will support SSC's requirements
- The procurement will consist of audio conferencing and web conferencing and two streams - Stream 1 (and Stream 2 as an optional future solution) for the Operator Assisted Services portion
- Vendors will be required to supply all services including the two streams for the Operator Assisted Services portion as the future optional Stream 2 is onboarded; therefore, vendors must respond and ultimately, upon contract award, deliver Stream 1, and Stream 2 (as an optional future solution).
- Vendors must clearly and effectively specify how they meet the mandatory experience as required in the solicitation; and may be required to articulate how they will meet the mandatory service requirements.
- Prior to contract award, the successful bidder must demonstrate how their solution meets all of the mandatory service requirements in addition to meeting security clearance requirements in support of Contract Award. Vendors who are new to government procurement and may not yet have a government security clearance, we ask that you please contact the Contracting Authority following this industry day to arrange for sponsorship in order to begin the security clearance process.

Break – 5 Minutes

Supply Chain Integrity Overview

PRESENTED BY:

Sophia Cheaitani
Acting Director,
Security Architecture and Oversight

Agenda

1. Context
2. Supply Chain Integrity Process
3. IT Product List Template
4. SCI Process Flowchart
5. On-going SCI Auditing Flowchart

Nature of the SCI Process

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

SCSI Submission Requirements

Respondents must submit the required information to the Contracting Authority before the imposed deadline. The mandatory elements will be clearly identified in the RFP document:

IT Product List:

- Information regarding all Products over which Canada's Data would be transmitted and/or stored that will be used and/or installed to perform any part of the Work described in the resulting contract
- Products include any hardware that operates at the data link layer of the OSI Model (i.e. Layer-2) and above, any software and Workplace Technology Devices.
- Include Products used by both the Respondent and by each of their proposed subcontractors in any context (installation, testing, production, delivery, support, maintenance, etc.)

Ownership Information: Manufacturers and suppliers, including subcontractors, ownership information, DUNS Numbers.

SCSI Assessment Process

- Canada will assess whether, in its opinion, the SCSI creates the possibility that the proposed solution (including the subcontractors used to implement that solution) could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information.

- In conducting its assessment, Canada may request from the Respondent any additional information that they require to conduct a complete security assessment of the SCSI.

- Assessment of the SCSI requires that a complete package be submitted before the established deadline.

CSE Cloud Assessment

This assessment assumes that the SaaS provider has:

- A valid ISO 27001 certificate or a valid SOC 2 Type II report if procuring an Unclassified or Protected A SaaS solution.
- Valid ISO 27001, ISO 27017, ISO 27018, ISO 27036 Certificates and a valid SOC2 Type II report if procuring a Protected B SaaS solution.

- Departments Must consider this supply chain security risk evaluation of the Software as a Service (SaaS) as one of the security assessments that feed into their risk management decision-making.

- In accordance with Treasury Board Secretariat (TBS) Direction on the Secure Use of Commercial Cloud Services, departments have the responsibility to ensure that the third party assurance and security assessment are conducted using the GC-approved methodology prior to authorization for operation. This supply chain integrity risk assessment alone is not enough for compliance with the TBS directives.

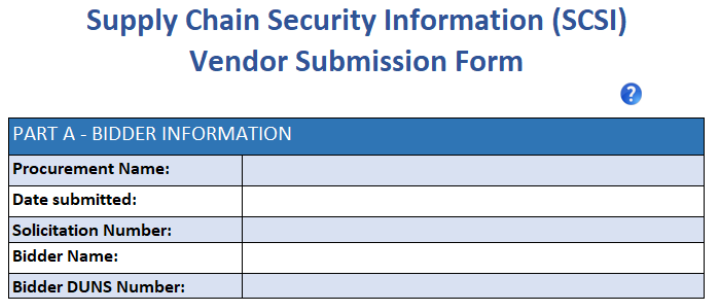
Outcome of Assessment

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

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

IT Product List Template

- Respondents are requested not to repeat multiple iterations of the same Product (e.g. if the serial number, location and/or color is the only difference between two products, they are considered the same Product with regards to Supply Chain Integrity).
- Products include any hardware that operates at the data link layer of the OSI Model (i.e. Layer-2) and above, any software and Workplace Technology Devices.
- There are also help and example sheets on the form.



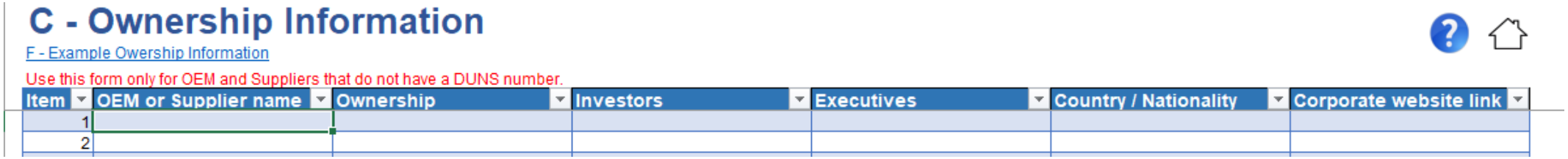
Supply Chain Security Information (SCSI)
Vendor Submission Form

PART A - BIDDER INFORMATION	
Procurement Name:	
Date submitted:	
Solicitation Number:	
Bidder Name:	
Bidder DUNS Number:	

B - Product List

Example IT Product List

Item	OEM Name	OEM DUNS Number	Product Name	Model / Version	Product URL	Vulnerability Information	Supplier Name	Supplier DUNS Numb	Supplier URL	Additional Information
1										
2										



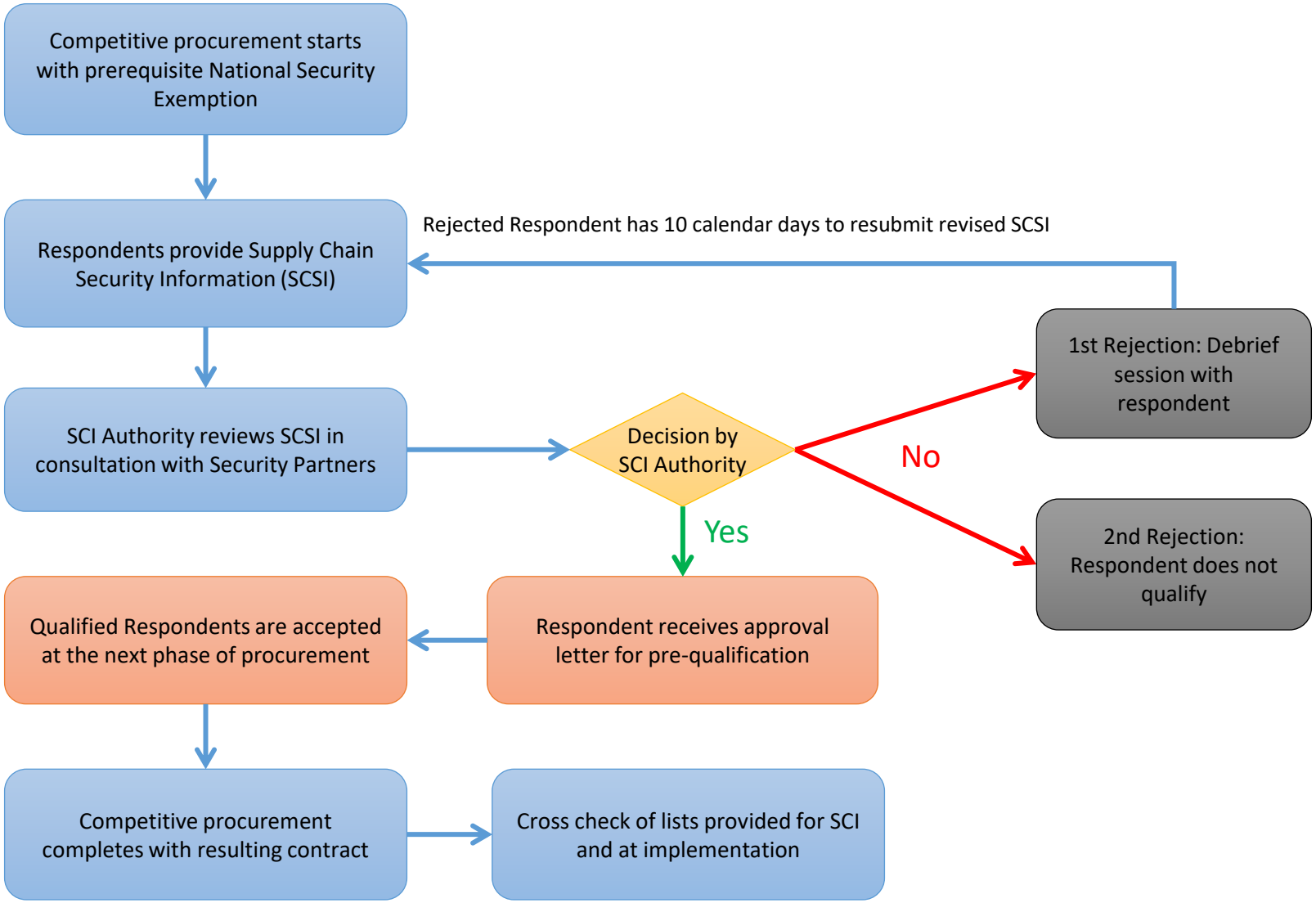
C - Ownership Information

F - Example Owership Information

Use this form only for OEM and Suppliers that do not have a DUNS number.

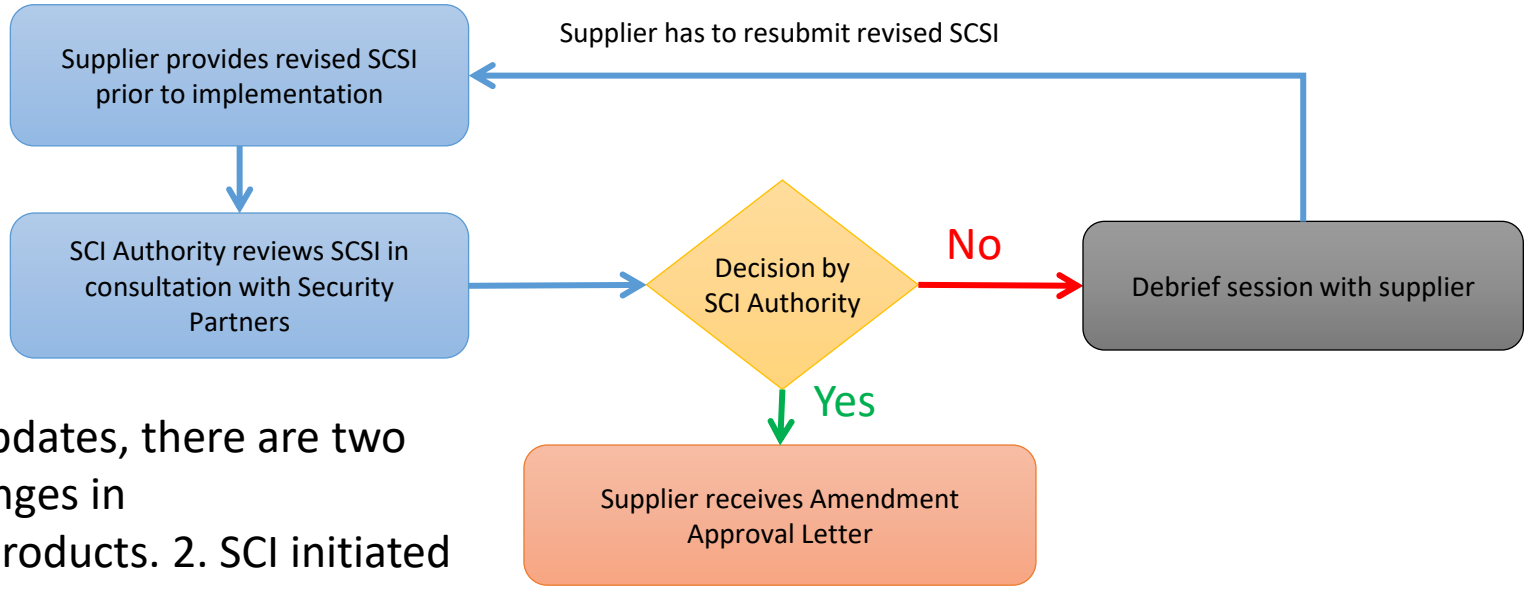
Item	OEM or Supplier name	Ownership	Investors	Executives	Country / Nationality	Corporate website link
1						
2						

Supply Chain Integrity (SCI) Process



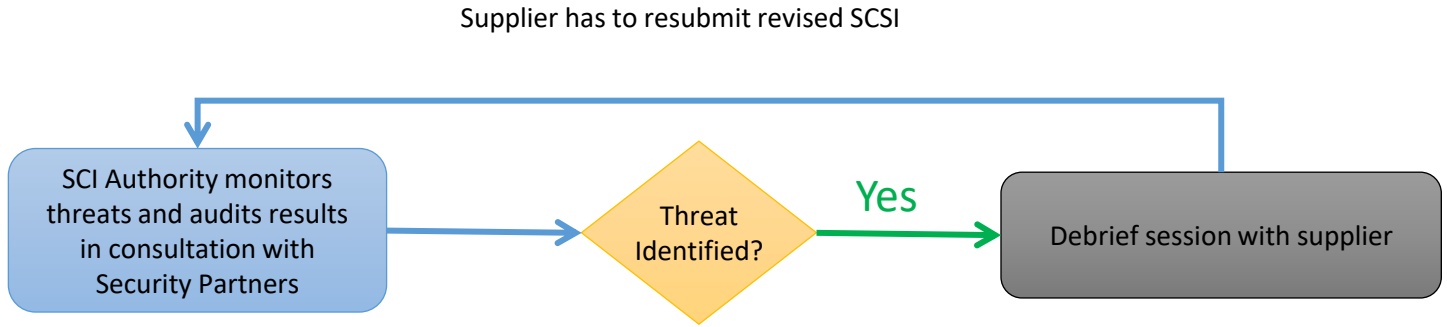
Ongoing SCI Auditing

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



In addition to regular SCSI updates, there are two triggers for an audit - 1. Changes in ownership/subcontractors/products. 2. SCI initiated audit, which can be triggered by a security incident or at random

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



Re-cap, Q&A, Closing Remarks

PRESENTED BY:
Tim St-Jean
Director General, Contact Centre &
Conferencing Services

Questions and Answers