RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
See Above

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Security and Information Operations Division/Division de la securite et des operations d'information
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Title - Sujet Defensive Cyber Operations	
Solicitation No. - N° de l'invitation W6369-17DE25/B	**Amendment No. - N° modif.** 003
Client Reference No. - N° de référence du client W6369-17DE25	**Date** 2018-02-28
GETS Reference No. - N° de référence de SEAG PW-$$QE-049-26594	
File No. - N° de dossier 049qe.W6369-17DE25	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-06-05**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Wight, Patti	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone (819) 420-1757 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** See Herein	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature**	**Date**

National Defence Défense nationale

Administrative Instructions

LCol Yves Turcotte, Senior Staff Officer Cyber Capability Requirement and Development

Canada

1. Building security reminder;
2. Restroom, Smoking and Break Areas; and
3. Questions.

Building Security

1. Visitors are restricted to the nom-members area of the Mess; and
2. Emergency exits are located at back, one on left, one on right, with Exit sign on the door.

Restroom

Men and women restrooms are located outside the main room on your right.

Smoking Area

Smoking Area is located outside the building.

Break Area

A break will be held at 10:00 at the entrance of this room.

Questions?

Defensive Cyber Operations – Decision Support (DCO-DS) and Cyber Security Awareness (CSA) and Projects

INDUSTRY ENGAGEMENT SESSION

Ottawa, Ontario

26 February 2018

INTRODUCTORY REMARKS

Cmdre R. Feltham

Director General Cyber

INTRODUCTORY REMARKS

Jeff Waring

Director General

Innovation, Science and Economic Development Canada (ISED)

OPENING REMARKS

Al Hamel
A/Director General
Land & Aerospace Equipment Procurement & Support Sector (LAEPSS)
Acquisitions Branch, PSPC

Al Hamel

A/Director General

- Biographical Sketch - Al Hamel, Col (Ret'd), CD, PEng

- A native of Coleville, Saskatchewan, Al Hamel started his academic and military career at Royal Roads Military College in Victoria, B.C. in 1970. Graduating from the Royal Military College of Canada in Kingston in 1974, and then trained as a military Communications and Electronics Engineering officer, Al set out on a 31-year adventure that included jobs such as Telecommunications Maintenance Officer at Canadian Forces Station Sioux Lookout in north-western Ontario, Regimental Signals Officer with the Royal Canadian Dragoons in Lahr, Germany, Commandant of the Canadian Forces School of Communications and Electronics in Kingston and Commander of the multinational, Signal Support Group at NATO's SFOR HQ in Sarajevo, not to mention a number of notable engineering and project management postings at Land Force Headquarters, St. Hubert and National Defence Headquarters in Ottawa. Al's last military appointment was as Director, Land Command Systems Program Management.

- Upon retiring from the Canadian Forces in April 2006, Al accepted a Public Service appointment with the Department of Public Works and Government Services Canada. After working for 4 ½ years in the IT Services Branch of PWGSC he joined Acquisitions Branch in October 2010, and he has been Senior Director, Electronics, Munitions and Tactical Systems Procurement since that time. He is also currently Acting Director-General, Land and Aerospace Equipment Procurement and Support Sector.

- Al holds a Bachelor's Degree in Electrical Engineering and a Master's Degree in Computer Engineering, both from the Royal Military College of Canada. He has been a Professional Engineer licensed to practice in the province of Ontario since 1976.

PSPC Mandate

- Public Services and Procurement Canada acts as a Common Service Agency for the Government of Canada
- Its activities are directed mainly toward providing other departments, boards and agencies with services in support of their programs
- Service Delivery includes:
  - Real Property
  - Accounting and Banking
  - Receiver General
  - Informatics and Telecommunications
  - Procurement and Contracting (focus of presentation)

Contracting Principles & Objectives

- Integrity
- Competition
- Openness and transparency
- Assist departments/agencies to meet their objectives
- Socio-economic objectives
- Legal and policy framework including Trade Agreements

Defence Procurement - What Do We Do?

- The Defence Production Act (1951) provides our Minister **exclusive authority** to acquire defence supplies/construction/projects
- Establish and manage contracts to acquire a wide range of technically complex systems for the Army, Navy and Air Force including the acquisition of:
  - Military and Civilian Aircraft & Systems
  - Ships & Marine Systems
  - Armament Systems & Munitions
  - Armoured Vehicles
  - Electronics & Communications Systems
  - Trainers & Simulators
  - Associated Repair & Overhaul Activities
  - Information Security and Electronic Warfare
- We manage procurements under the Munitions Supply Program to maintain a Canadian industrial capability for high volume ammunition and small arms. 13

Stakeholders in Canadian Defence Procurement

Finance

Treasury Board

Innovation Science and Economic Dev Canada

Regional Development Agencies

DND

Industry

PWGSC

Privy Council Office

Justice

Global Affairs Canada

Engagement Session Agenda

Opening Remarks - Director General Cyber	DND
Opening Remarks – Director General ITBB	ISED
Opening Remarks – Director General LAEPSS	PSPC
Industry Engagement Process	PSPC
Rules of Engagement	PSPC
Process for Facility Security Clearance Application / Controlled Goods Program Registration	PSPC
Industrial and Technological Benefits	ISED-C
Operational Requirements Overview	DND
Questions and Answers	All
Closing Remarks	PSPC

INDUSTRY ENGAGEMENT PROCESS

Patti Wight
Supply Specialist
Acquisitions Branch, PSPC

Industry Consultation

- It is Canada's intent to actively engage and consult Industry throughout the procurement process to ensure a successful project end-state.
- The Request for Information (RFI) and engagement process provides Industry with the opportunity to present their capabilities and considerations regarding Canada's requirements for the DCO-DS and CSA Projects.
- Canada may use the information gathered to assist in the development of a Request for Proposal (RFP).

Engagement Process Guiding Principles

Transparency: ensuring procurement integrity by sharing all procurement outcomes and activities with stakeholders;

Fairness: stakeholders will get an equal opportunity to access engagement activities;

Timeliness: Engagement activities will be planned and conducted early in the procurement process; and

Relevancy: to include tangible, useful and current outputs that are in alignment with Government of Canada priorities.

Proposed Engagement and Procurement Process

- **Phase 1: Winter 2016 to Autumn 2019**
  - **Letter of Interest:** A Letter of Interest (LOI) for both projects was issued in December of 2016 and closed January 2017.
  - **Request for Information:** A RFI to provide more detailed information to industry and will act as a continuous single point of official project(s) communication. Chiefly it will solicit detailed industry feedback on operational and technical requirements, cost and schedule.
  - **Unclassified Industry Day:** To present an overview of the requirements and engagement process.
  - **One-on-One Meetings:** Classified one-on-one meetings to distribute, present and discuss the classified Annex of the RFI.
  - **Group Follow-up Meeting:** Classified group follow-up meeting to distribute classified questions and answers.

Proposed Engagement and Procurement Process cont.

- **Phase 2: Autumn 2019**
  - **Request for Information:** The RFI issued in Phase 1 will remain open in order to provide direction and assistance to suppliers in obtaining security clearances.
  - **Draft Request for Proposal:** A draft RFP for each project or a single combined project may be released to suppliers meeting the security requirements for their review and input.
- **Phase 3: Summer/Autumn 2020**
  - **Request for Proposal:** The formal Request for Proposal for each project or a single combined project will be issued.
  - **Evaluation:** Bids will be evaluated in accordance with the terms of the RFP.
- **Phase 4: Summer 2021**
  - **Contract Award:** A contract(s) will be awarded to the winning bidder in accordance with the terms of the RFP.

Completed Industry Engagement

Letter of Interest (LOI)

A LOI for each project was released December 2016 and closed January 2017. The purpose of the LOIs was to inform industry at a high level of both projects, gain feedback and costing on potential solutions, and to advise industry that the ITB Policy may apply.

Key Findings

- Technology exists to provide solutions in timely, cost-effective manner.
- Industry is prepared to fulfill Prime System Integrator, Sub-System Integrator or Product Supplier roles.
- Industry noted the close-coupling of the two projects and the need to consider them in a joint fashion as a single project.
- Industry advised more detail was required to support cost estimation exercise.
- One-on-one engagement sessions are required to provide SECRET cleared suppliers with Classified information to support a detailed analysis.

Purpose of Current Request for Information

This RFI is being issued with the key objectives of:

- Soliciting indicative pricing and scheduling information for the acquisition and in-service support for key requirements of the CSA and DCO-DS projects.
- Soliciting feedback on industry capabilities to assist in the development of the Industrial and Technological Benefits (ITB) Value Proposition.
- Collaborating with industry on the ITB and Value Proposition strategy.
- Serving as a continuous point of contact for Canada and Industry throughout the engagement and procurement process.
- Outlining the engagement approach and proposed procurement process.
- Providing schedule and procurement updates.
- Advising industry of key dates within the RFI process.
- Soliciting detailed industry feedback on the procurement process, operational and technical requirements, cost and schedule.
- Advising suppliers of the security requirements of the RFI, Draft RFP, RFP and resulting contract.
- Provide direction and assistance to non-cleared suppliers in obtaining security clearances.

Key Milestones of the Current RFI

- **Group Industry Engagement Session - 26 February 2018**
  - Unclassified Industry Day open to all interested industry respondents.
  - Present industry with an outline of the procurement process, the engagement approach, security requirements and an unclassified overview of the projects.
  - Present the Rules of Engagement for the procurement process - **Annex G of the RFI.**
  - Allow industry to ask questions and seek information in order to gain a sound understanding of the requirement.
- **Classified One-on-one Meetings – 26 February 2018 to 2 March 2018**
  - Present security cleared suppliers with an overview of the classified Annex C.
  - Provide security cleared suppliers with a hard copy of Annex C. Annex C will only be provided in person.
  - Invite suppliers to give feedback and discuss Annex C only.
  - If required a classified group follow-up meeting may be held to distribute classified questions and answers.
- **RFI Submissions – 23 March 2018**
  - Suppliers are requested to respond to the current RFI on or before 23 March 2018
  - All interested suppliers may submit formal responses to the questions posed in the RFI.

RULES OF ENGAGEMENT

Christine Picknell

Supply Specialist

Acquisitions Branch, PSPC

General Rules and Principles

These Rules of Engagement apply to the entire Engagement Process

- An overriding principle of the industry early engagement is that it be conducted with the utmost of fairness and equity between all parties. No one person or organization shall not receive nor be perceived to have received any unusual or unfair advantage over the others.
- These Rules of Early Engagement will apply beginning with the release of this RFI document and conclude with the release of the Request for Proposal.
- The Engagement Process will consist of the Request for Information, One-on-One Meetings, Group Follow-up Meeting and a possible draft RFP and any other processes deemed necessary by the Procurement Authority.
- In order to maximize the benefits of the Engagement Process, Canada may endeavor to solicit comments from participants on various issues raised.
- One-on-one sessions and the Group-follow-up meeting are only available to participants who meet the security requirements.
- Classified information may only be released to participants who meet the security requirements.

General Rules and Principles cont.

- Any solutions, ideas or issues raised during the One-on-One sessions will be analyzed for further consideration by Canada.
- A draft RFP for a final review before the official RFP is issued may be made available to participants meeting the security requirements.
- Canada will not disclose proprietary or commercially sensitive information concerning a participant to other participants or third parties except and only to the extent required by law.
- Potential respondents are advised that any information submitted to Canada in the engagement process may be used by Canada in the development of a competitive Request for Proposal.

Terms and Conditions

The following terms and conditions apply to the Engagement Process. In order to encourage open dialogue, participants agree to the following:

- Participants are expected to discuss their views concerning the procurement, and to provide positive resolutions to the issues in question. All interested participants meeting the security requirements shall have equal opportunity to share their ideas and suggestions.
- No electronic recordings, audio or visual, will be permitted during the one-on-one meetings.
- Participants must provide to Canada advance notification if they plan to have legal representation at the one-on-one meeting. Canada reserves the right to decline any meetings which include legal representation.
- Participants will NOT reveal or discuss any information to the MEDIA/NEWSPAPER regarding this requirement during this engagement process. If participants receive a question from the Media, participants are to direct the Media to contact the **PSPC Media Relations Office at 819-956-2313.**
- **Participants are to direct inquiries and comments ONLY to the PSPC Contracting Authority** or authorized representatives of Canada, as directed in notices given by the Contracting Authority. Any communication to unauthorized representatives of Canada may be subject to full disclosure by Canada on Buy and Sell.

Terms and Conditions

- Canada is not obligated to issue any RFP, or to negotiate any contract for the projects.
- If Canada does release a RFP, the terms and conditions of the RFP shall be subject to Canada's absolute discretion.
- Canada will not reimburse any person or entity for any cost incurred in participating in this industry engagement process.
- Participation is not a mandatory requirement. Not participating in this engagement process will not preclude a bidder from submitting a proposal when the final RFP is released.
- Draft documentation (RFP, Evaluation Plan, SOW) will be released to Participants who meet the security requirements for comments.
- Lobbyists will not be permitted to participate in the engagement process.
- By informal discussion and good faith negotiation, PSPC and the participant shall make all reasonable efforts to resolve any dispute, controversy or claim, arising out of or in any way connected with this Industry Engagement.

CYBER SECURITY PROJECT

SECURITY REQUIREMENTS THROUGH THE CONTRACT SECURITY PROGRAM



Policy, Planning and Security Branch , Industrial Security Sector
Outreach Division 2018

Overview

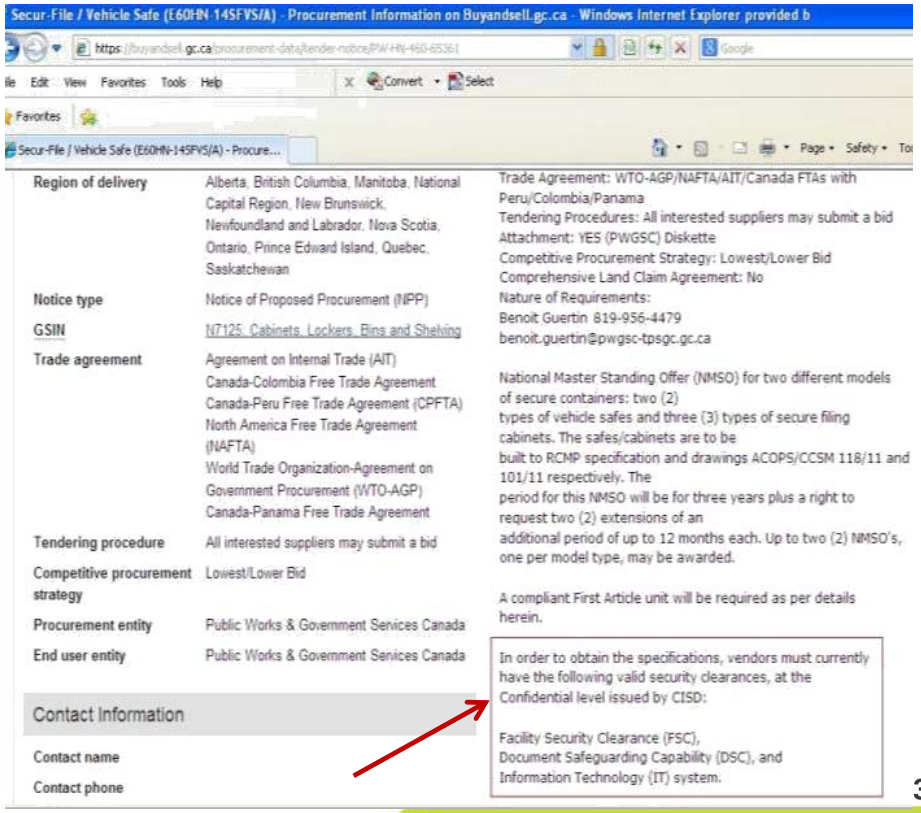
- Bid opportunities requirements
- Contract Security Program and registration
  - Organization security screening
  - Document Safeguarding Capability
  - Authority to Process Information Technology
  - Subcontracting
- Your role
- Webinars
- Contact us
- Useful links

Bid opportunities requirements

Security requirements can be found in:

- The tender notice's description
- The solicitation documents
  - E.g. Check the table of contents for security requirements (these are typically found in "Part 7 – Resulting Contract Clauses" and the SRCL is typically attached as an annex)

Buyandsell.gc.ca



Contract Security Program

- Enables industry to participate in sensitive government contracts in Canada and abroad;
- Provides security screening services for organizations and their employees;
- Ensures the necessary contract security clauses are included as part of contracting vehicles;
- Ensures industry complies with contracting security requirements.

How can I register in the CSP?

A Government of Canada **approved source** must sponsor your organization.

- The approved source must submit a Request for Private Sector Organization Screening (**PSOS**) and when applicable a Security Requirement Check List (**SRCL**) for your organization.

- The PSOS will identify the type of security screening required.

Who is an approved source recognized by the CSP?

- A government procurement officer – an officer who carries out specialized advanced purchase of goods and services;
- A Government of Canada security officer or project manager leading a project you have bid on or intend to bid on;
- A prime contractor registered in the CSP for whom you are subcontracting (for approved subcontracts only); or
- National and Designated Security Authorities on behalf of a foreign company or government that is contracting to your organization.

Types of security screenings

	Information and Assets	Organization Screening	Personnel Security Screening
CLASSIFIED National Interest	Top Secret	Facility Security Clearance (FSC)	Top Secret
	Secret		Secret
	Confidential		
PROTECTED Non-national Interest	Protected C	Designated Organization Screening (DOS)	Enhanced Reliability Status
	Protected B		Reliability Status
	Protected A		

Organization screening

Upon receipt of a valid request for PSOS from an approved source, the CSP will contact your organization to request information to begin the registration process **by email or by mail**.

The CSP will request the following information:

- Your organization's structure, ownership and legal status;
- The appointment of a Company Security Officer (CSO) and/or Alternate Company Security Officer (ACSO);
- Identification of Key Senior Officials (KSOs) (when accessing Confidential, Secret or Top Secret info/assets);
- Personnel security screening forms and documents for CSO, ACSO and/ or KSOs.

Document Safeguarding Capability

- If the RFI/RFP/contract requires the **safeguarding of sensitive information and/or assets at your site(s)**, your organization will also need to obtain a Document Safeguarding Capability (DSC) at the level specified in the tender notice/contract.

- The CSP will conduct physical security inspections **before contract award** for the following contract security requirements:

    - Document Safeguarding Capability
    - Authority to Process Information Technology

Authority to Process Information Technology

- If you are required to **use your IT systems to access, produce, process and store protected or classified information electronically for a government contract**, your organization will also need to obtain the Authority to Process IT at the level specified in tender notice/contract.

- IT requirements are defined in the technical document attached to the contract.

- An IT security inspections for IT contract security requirements must be conducted, typically **after contract award**

- The IT inspection looks at all IT assets utilized to create the contract deliverable.

Processing timelines

Company security clearances	Estimated processing timelines
Designated Organizational Screening	Three months or more
Facility Security Clearance (Secret)	Six months or more
Facility Security Clearance (Top Secret)	Twelve months or more
Document Safeguarding Capability	Varies
Authority to Process IT	Varies

Service standards

Personnel Security Screening	CSP Service Standards
Reliability Status (simple)	7 business days
Reliability Status (complex*)	Up to 120 business days
Secret (simple)	Up to 4 months
Secret (complex*)	Up to 12 months
Top Secret	12 months +

* Additional information and/or verifications required.

Subcontracting

Subcontracts are used when a prime contractor wishes to subcontract **a portion** of the prime contract to another organization or self-employed individual.

The organization who intends to subcontract is responsible for:

1. Completing an SRCL identifying the security requirements of the subcontract;
2. Requesting a PSOS on behalf of the subcontractor;
3. Submitting the SRCL and PSOS form to the CSP for approval;
4. Obtaining and inserting the security clauses and SRCL into the subcontract;
5. Validating the subcontractor's organization and personnel are cleared; and
6. Submitting a copy of the awarded subcontract containing the SRCL to the CSP.

Work cannot start until the subcontractor obtains the appropriate security screening

Phase 1

Procurement / Engagement Activity	Security Clearance Required
Phase 1	
Request for Information (RFI):	
Unclassified Industry Day	None
View Annex C	Facility Security Clearance: SECRET, CAN, US, Personnel Viewing: SECRET CAN, US,
Obtain a hard copy of Annex C Obtain a hard copy of any Classified Questions and Answers	Facility Security Clearance: SECRET, CAN, US, Personnel Transporting Document: SECRET, CAN, US Document Safeguarding: SECRET
Attend Classified One-on-one Meetings Attend Classified Group Follow-up Session	Facility Security Clearance: SECRET, CAN, US, Personnel Attending: SECRET, CAN, US,
Unclassified Questions and Answers	None – will be publically posted

Phase 2

Phase 2	
Draft Request for Proposal*	Document Safeguarding: SECRET
View Classified Information	Personnel: SECRET, Canadian Eyes Only
Obtain a hard copy of Classified Information	Facility Security Clearance: SECRET, Canadian Eyes Only Personnel Transporting Document: SECRET, Canadian Eyes Only Document Safeguarding: SECRET
Attend Classified Meetings	Personnel: SECRET, Canadian Eyes Only

Phase 3

Phase 3	
Request for Proposal*	Facility Security Clearance: SECRET, Canadian Eyes Only Personnel: SECRET, Canadian Eyes Only Document Safeguarding: SECRET
View Classified Information	Personnel: SECRET, Canadian Eyes Only
Obtain a hard copy of Classified Information	Facility Security Clearance: SECRET, Canadian Eyes Only Personnel Transporting Document: SECRET, Canadian Eyes Only Document Safeguarding: SECRET
Attend Classified Meetings	Personnel: SECRET, Canadian Eyes Only

Phase 4

Phase 4	
Contract*	Facility Security Clearance: TOP SECRET, Canadian Eyes Only Personnel: TOP SECRET SIGINT, Canadian Eyes Only* Document Safeguarding: SECRET, NATO SECRET

Your role

- Find an approved source.
- Comply with the CSP registration process.
- Obtain and maintain organization security clearance.
- Screen personnel involved in government sensitive contract.
- Meet physical and IT security requirements if necessary.
- Identify subcontractors and ensure security of subcontracts if necessary.

Webinars

- How to obtain a clearance with the Contract Security Program
- Document safeguarding capability
- Contracting outside of Canada
- Handling and safeguarding
- Subcontracting
- Completing a designated organization screening application
- Completing a facility security clearance application

Request a copy of the recording:
SSIDSICSensibilisation.ISSCISDOutreach@tpsgc-pwgsc.gc.ca

Contact us

General Inquiries

Phone
Toll-Free: 1-866-368-4646
National Capital Region: 613-948-4176

Email
ssi-iss@tpsgc-pwgsc.gc.ca

Website
http://www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html

Useful links

Contacts for Goods and Services Identification Number (GSIN) codes
https://buyandsell.gc.ca/procurement-data/goods-and-services-identification-number/contacts-for-gsin-codes

Contract Security Resources (NEW)
http://www.tpsgc-pwgsc.gc.ca/esc-src/ressources-resources-eng.html

Contract Security Program Forms
http://ssi-iss.tpsgc-pwgsc.gc.ca/formulaires-forms/index-eng.html

Video – E-fingerprinting
http://www.tpsgc-pwgsc.gc.ca/esc-src/formation-training-eng.html#s3

Thank you!

Annex

Project Screening Requirements

Project Stage	Description of Project Stage	Level of Personnel Clearance and Document Safeguarding (e.g. Reliability, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
1	Industry Engagement Stage supporting Options Analysis Phase	• SECRET for Personnel Assigned, and • SECRET for Document Safeguarding	• Reviewers of Annex C of RFI during Options Analysis Phase	Classified Meeting Room for One-on-One Industry Engagement Meeting / SECRET	Canadian, UK, USA, Australia
2	Industry Engagement Stage supporting Definition Phase	• SECRET for Personnel Assigned, and • SECRET for Document Safeguarding	• Reviewers of Classified Annexes of RFI	Classified Meeting Room for One-on-One Industry Engagement Meeting / SECRET	Canadian
3	Solicitation Stage supporting Definition and/or Implementation Phase	• SECRET for Personnel Assigned, and • SECRET for Document Safeguarding	• Reviewers of Classified Annexes of RFP	Classified Meeting Room for One-on-One Industry Engagement Meeting / SECRET	Canadian

Project Screening Requirements

Project Stage	Description of Project Stage	Level of Personnel Clearance and Document Safeguarding (e.g. Reliability, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
4	Contract Award Stage during Implementation Phase	• TOP SECRET (SIGINT) for Personnel Assigned, and • SECRET and NATO SECRET for Document Safeguarding	• Project Manager, • Senior Business Systems Analyst, • Senior Systems Engineer/Developer, • Field Service Representatives, and • Equivalent tasked Subcontractors	High Security Zones within DND / TOP SECRET (SIGINT)	Canadian
		• NATO SECRET and SECRET for Personnel Assigned, and • NATO SECRET and SECRET for Document Safeguarding	• Intermediate Engineer/Developer, • Junior Engineer/Developer, and • Equivalent tasked Subcontractors	Security Zones within DND / NATO SECRET and SECRET	Canadian
		• Enhanced Reliability for Personnel Assigned, and • No Requirement for Document Safeguarding	• Administrative Staff	No Site Access / UNCLASSIFIED	Nil

©Copyright

Controlled Goods Program

Defensive Cyber Operations - Decision Support Project
Industry Day
February 26, 2018

Dominic Dubé
Chief, Program Management and Learning
Controlled Goods Program
Public Services and Procurement Canada (PSPC)

The Controlled Goods Program

- Established in 2001 to support the provision of the Canadian exemption under the U.S. International Traffic in Arms Regulations (ITAR)

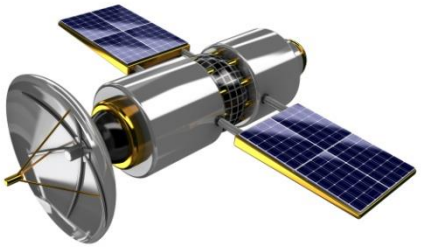
- Legislated by the Defence Production Act (DPA) and Controlled Goods Regulations (CGR)

The Controlled Goods Program's Raison d'être

"To ensure that controlled goods are safeguarded while in the custody of private sector companies and protected against unauthorized access."

Definition of controlled goods

- Controlled goods are primarily goods, including components and technical data that have military or national security significance, which are controlled domestically by the Government of Canada and defined in the *Defence Production Act*.



Summary, controlled goods are

- goods, including components and technology (for example, blueprints and technical specifications in paper or electronic format), with strategic significance or national security implications, regardless of where they are manufactured

- defense articles originating from the United States that are controlled by the United States Munitions List—part 121 of the United States *International Traffic in Arms Regulations*, as amended from time to time

- goods, regardless of where they are manufactured, that are manufactured from technical data originating from the United States and are controlled by the *International Traffic in Arms Regulations*

Controlled Goods List

- Controlled Goods List contained in the schedule (section 35) of the *Defence Production Act*

- Guide to the schedule to the *Defence Production Act*
  - provides a simplified listing of the items that are identified as controlled goods in the *Defence Production Act*.
  - helps identify whether or not an item is included on the Controlled Goods List
  - schedule takes precedence over the guide

Why individuals and organizations must register

- It is the law. Individuals and organizations must register in the Controlled Goods Program if they need to **examine**, **possess** or **transfer** controlled goods. During registration, applicants must demonstrate this need.

- Failure to register may be considered an offence under federal laws, and could lead to prosecution and sanctions.

Any person who fails to comply with the *Defence Production Act* may:

- have their registration with the Controlled Goods Program suspended or revoked
- face prosecution for failing to comply and be subject to a fine not exceeding $2,000,000, and/or imprisonment not exceeding 10 years

As an individual or an organization, you must register before you:

- examine, possess or transfer controlled goods in Canada
- transfer controlled goods outside of Canada
  - registration is required before getting an export permit from Global Affairs Canada
- receive bid solicitation documents containing controlled goods or controlled technology

Understand if you are examining, possessing or transferring controlled goods

- **Examine** means to consider in detail or subject to analysis in order to discover essential features or meaning
- **Possess** means either actual possession, where the person has direct physical control over a controlled good at a given time, or constructive possession, where the person has the power and the intention at a given time to exercise control over a controlled good either directly or through another person or persons
- **Transfer** means, with respect to a controlled good, to dispose of it or disclose its content in any manner

Roles in the Controlled Goods Program

Owner

- any owner of 20% or more of the outstanding voting shares or interests of the business

Authorized Individual

- usually the owner or another senior official of the organization with signing authority

Designated Official

- completes mandatory training for designated officials
- conducts security assessments of employees, officers and directors
- determines the risk of transferring controlled goods to anyone who is not registered or is not exempt from registration and authorizing the extent to which they may examine, possess or transfer controlled goods
- verifies the information provided to them by temporary workers, international students and visitors for the purpose of applications for exemption and submit the exemption requests to the CGP

How to register

To register in the Controlled Goods Program, you must complete the following steps:

1. Appoint an authorized individual
2. Appoint a designated official
3. Complete the application for registration form
4. Complete a security assessment application form for each required individual
5. Review your applications and supplementary documentation
6. Submit your application

Application for Registration

- submit a completed & signed Application for Registration
  - Section H (Certification and consent), is signed by the Authorized Individual
- provide evidence of the legal status of the company (e.g. copy of Certificate of Incorporation, Master Business Licence, etc.)
- clearly provide a description of your business activities in relation to controlled goods on the application form as well as any companies with whom you have / will have a business relationship involving controlled goods. If you have supporting documentation regarding justification for registration, such as a contract, an RFP, a Third Party E-mail / Letter, please submit those as well
- controlled goods to be listed in section D.10
  - when bidding on contracts with a controlled goods, check with bid authority to obtain CGL item numbers and descriptions

Authorized Individual and all Owners of 20% or more

- submit a completed & signed Security assessment application
- two pieces of government-issued identification (at minimum one must be photo identification)
  - proof of citizenship (for example, birth certificate, passport, permanent resident card)
  - proof of residence (for example, driver's license, government-issued document with address)
- fingerprint criminal record check report or criminal record name check report. When completing the form, please use "**private sector**" for employment and ensure the results are sent to the applicant's home address, so they can then be submitted with the application and other documentation
  - for foreign individuals or those who have lived outside of Canada for 6 consecutive months or more within the last five years, we require a Criminal History check from a recognized police agency – Example: Certificate of Good Conduct; FBI Check, Police certificate

Designated Official(s)

- submit a completed & signed Security assessment application
- two pieces of government-issued identification (at minimum one must be photo identification)
  - proof of citizenship (for example, birth certificate, passport, permanent resident card)
  - proof of residence (for example, driver's license, government-issued document with address)
- fingerprint criminal record check report - Please have electronic fingerprints taken. When completing the form, please use "**private sector**" for employment and ensure the fingerprint results are sent to the applicant's home address, so they can then be submitted with the application and other documentation

Processing times

- An application for registration, along with all supporting documentation, can take 32 business days to process.
- You may inquire about the status of your registration after a four week waiting period.
- we accept only complete applications
- if incomplete (missing signatures, missing supporting documents, missing fingerprint results, etc.), the application will be returned

Submitting applications

Mail / Courier:
Controlled Goods Program
Public Services and Procurement Canada (PSPC)
3rd floor
2745 Iris St
c/o PSPC Central Mail Room
Portage III, 0B3
11 Laurier St
Gatineau QC K1A 0S5

E-mail: dmc-cgd@tpsgc-pwgsc.gc.ca

Facsimile: (613) 948-1722

Registration checklist

- ❑ Company
  - ❑ Application for Registration
  - ❑ Evidence of the legal status of the company
- ❑ Authorized Individual
  - ❑ Security assessment application
  - ❑ two pieces of government-issued identification
  - ❑ fingerprint criminal record check report **or** criminal record name check report
- ❑ all Owners of 20% or more
  - ❑ Security assessment application
  - ❑ two pieces of government-issued identification
  - ❑ fingerprint criminal record check report **or** criminal record name check report
- ❑ Designated Official(s)
  - ❑ Security assessment application
  - ❑ two pieces of government-issued identification
  - ❑ fingerprint criminal record check report

Questions?

Website: http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-eng.html

Email: DMC-CGD@tpsgc-pwgsc.gc.ca

Toll-free number: 1-866-368-4646

National Capital Region: 613-948-4176

Call us Monday to Friday, 8:00 am to 5:00 pm Eastern time. Services are available in English and French.

Cyber Security Awareness (CSA), and Defensive Cyber Operations–Decision Support (DCO-DS)

Industrial and Technological Benefits Policy

Leveraging Economic Benefits

Economic Benefits to Canada

- The Government of Canada is **consulting with industry** to understand how best to leverage these cyber procurements for the economic benefit of Canada.

- The **Industrial and Technological Benefits** (**ITB**) Policy may be applied on the Defensive Cyber Operations-Decision Support (DCO-DS) and Cyber Security Awareness (CSA) projects.

Objective of Engagement

- To present highlights of the market analysis that informs our economic leveraging approach

- To highlight questions provided to industry in the Request for Information
  - Industry feedback will also be used to inform the Government of Canada on how best to leverage this procurement to support industrial growth and innovation in Canada

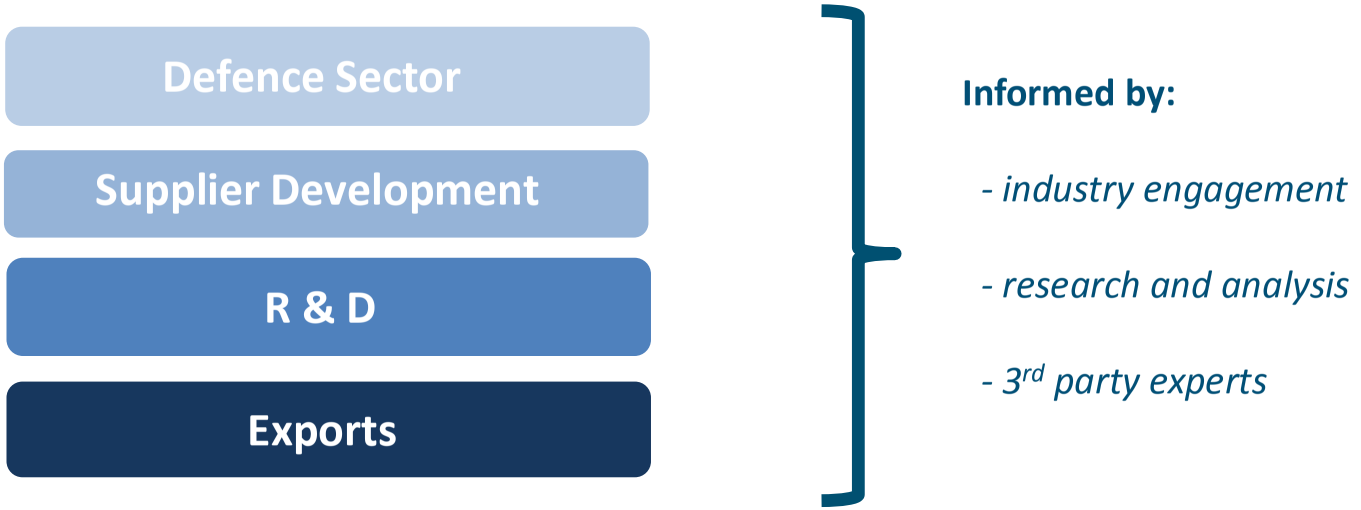
Industrial and Technological Benefits (ITB) Policy

- **Companies awarded defence procurement contracts are required to undertake business activity in Canada equal to the value of the contract**
- Four objectives:
  - Support the long-term sustainability and growth of Canada's defence sector
  - Support the growth of prime contractors and suppliers in Canada, including small and medium-sized enterprises in all regions of the country
  - Enhance innovation through R&D in Canada
  - Increase the export potential of Canadian-based firms

The Value Proposition (VP)

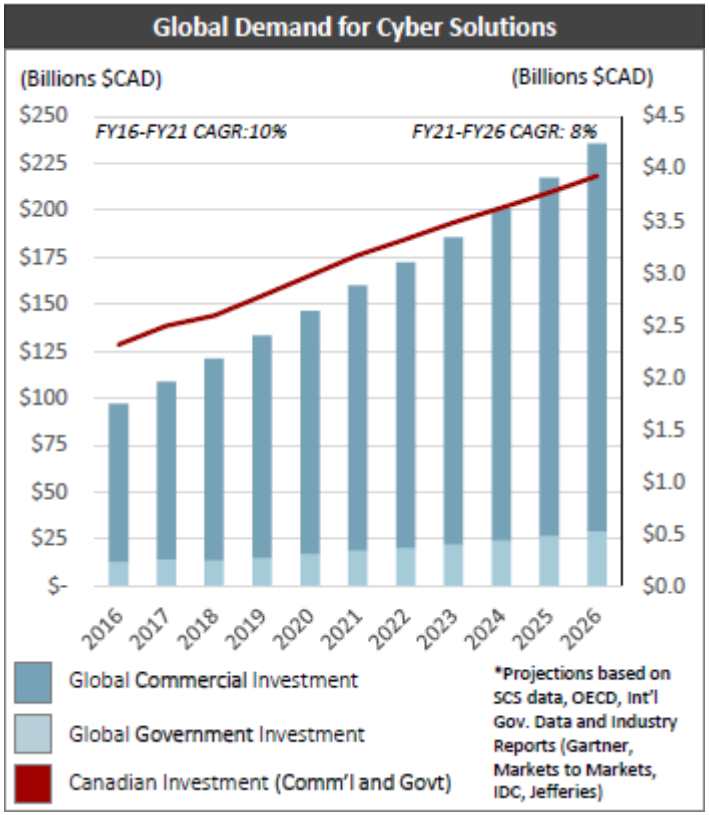
- **The VP is the economic benefits package that a bidder proposes in its bid submission**
- Canada will develop evaluation criteria that will be used to measure a bidder's level of commitment to undertake work and invest in the Canadian economy
- The VP evaluation criteria:
  - will be informed in part through industry consultation
  - is a weighted factor in winner selection
  - Will be tailored to each project

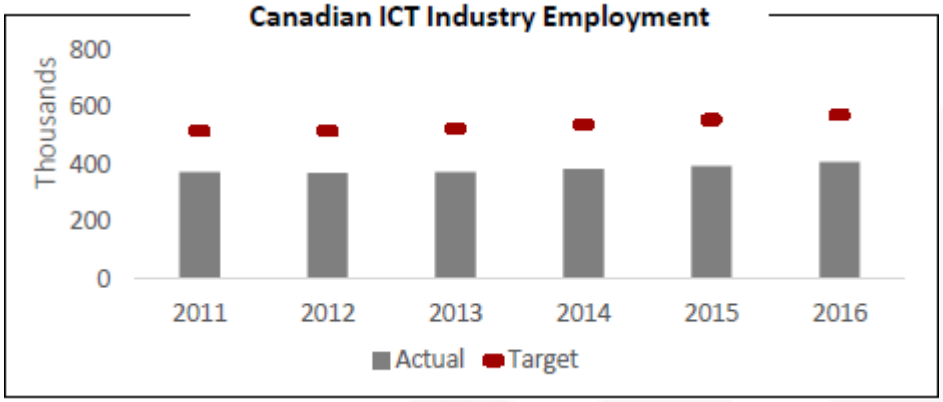
After a contract is awarded, the contractor is required to begin fulfilling its ITB obligation and the commitments made through the Value Proposition.



Market Research and Analysis

- Due to the fast evolving nature of information technology and related threats, the global cyber market will grow from roughly $110 billion in 2017 to more than $163 billion in 2021.
- Canada has an estimated 1000 firms within the broad ICT industry, with more than 200 firms specific to the cybersecurity market.





Market Research and Analysis

- Large competitive space with hundreds of firms, majority of which are small and medium businesses
- 98% of Canadian cyber firms are not defence sector focused, instead targeting customers in the growing commercial market
- Existing cyber infrastructure concentrated around geographical clusters, including a world-class academic sector, that can support cyber innovation and serve as engines of growth
- Areas of technical strength in Canada include:
  - Artificial Intelligence
  - Quantum Computing
  - Identity and Access Management
  - Data Loss Prevention

Key Observations for Leveraging Economic Benefits

- The high number of **small and medium businesses** (SMB) highlights opportunities for technology transfer, supply chain integration and partnerships with large firms to advance SMB growth and scale up innovative technologies

- Higher demand and long-term profitability in the commercial sector indicate a propensity for investment focused on **commercial applications** of cyber technology

- A shortage in the cyber talent pool indicates the importance of investment in **skills development and training** within industry and academia to build domestic capacity and address current and future workforce needs

- There is a strong base in Canada for conducting advanced R&D activities, as well as opportunities for collaboration with Canadian academic institutions for **research and commercialization** of cyber technologies

- Mixed potential for **export** of cyber technologies and services, with greater opportunities focused on traditional markets such as Five Eyes and NATO allies

Questions for Industry

Please see RFI document – Annex F – Industrial and Technological Benefits Policy

Defence Sector

Objective: To promote economic development and long-term sustainment of Canadian businesses engaged in the manufacturing and delivery of products and services for use in government defence and security applications.

1. What Canadian capabilities could be used to directly support the production and delivery of the Cyber Security Awareness (CSA) and Defensive Cyber Operations-Decision Support (DCO-DS) solutions?

2. What percentage of direct work on the CSA and DCO-DS projects can be achieved in Canada?

Supplier Development, incl. SMB

Objective: To improve the competitiveness of Canadian companies, independent of the Contractor or Eligible Donors, by strengthening productivity, skills development, and the ability to overcome market challenges.

1. The Canadian cybersecurity industry comprises close to 1000 companies, most of which are small and medium-sized businesses (SMB). What opportunities are there to partner with Canadian SMB with less than 250 employees to perform direct work on the CSA and DCO-DS projects?

2. What types of investments should Canada incentivize that would produce maximum benefit to Canadian companies in the cybersecurity market (defence or commercial sector)?
   a. Examples:
      i. Creation of skills and training initiatives to attract and retain skilled workers (e.g.: coding and programming, network engineering, and software development and integration);
      ii. Investments in new capital equipment and resources;
      iii. Support for security certifications (e.g.: Top Secret, ITAR) for Canadian companies, especially small and medium-sized businesses;

3. The ITB Policy requires that at least 15 percent of the contractor's ITB obligation (equal to the value of the contract) be represented by work with Canadian SMB with less than 250 employees. To what extent can you commit to a SMB requirement of over 15 percent in order to nurture the development of Canadian SMB within the cybersecurity sector (includes both direct work on these procurements and work in other business areas)?

4. Apart from these procurements, in what other areas of production and service-provision do you see opportunities to assist cybersecurity SMBs to scale up, in order to respond to domestic and global demand?

Research and Development

Objective: To promote scientific investigation that explores the development of new goods and services, new inputs into production, new methods of producing goods and services, or new ways of operating and managing organizations.

1. Are there opportunities to partner with Canadian post-secondary or publicly-funded research institutions to perform direct work on the CSA and DCO-DS projects?

2. What high-value R&D investments in Canada, either in the defence or commercial sectors, could Canada motivate bidders to make as a result of these procurements (e.g. cloud security, mobile security, security analytics)?
   a. What opportunities exist to incentivize investment in emerging cross-sectoral technologies where Canadian capabilities exist (e.g. quantum computing, augmented/virtual reality, artificial intelligence/machine learning)?

3. Is there potential to develop research consortia or centres of excellence in partnership with Canadian post-secondary or publicly-funded research institutions, and if so, what research areas might your company pursue?
   a. If not, what other research or development partnerships could be formed to support technology development in areas related to the CSA and DCO-DS projects?

4. Is there potential to invest in research and development partnerships with Canadian cyber sector SMBs and start-up companies, including funding for late-stage R&D and commercialization of innovative products or services?

5. What should the minimum R&D requirement be (as a percentage of anticipated bid price) in order to motivate bidders to invest in high-value, innovation within Canada's cyber sector?

Export

Objective: To promote the ability of Canadian companies, including SMBs, to successfully tap into export markets, thereby increasing their productivity, and competitiveness in the global market.

1. Please describe any export opportunities from Canada directly related to these procurements.

2. Is it feasible to secure sufficient intellectual property rights and an exclusive global product mandate to export from your Canadian-based operations, including subsidiaries and supply chain partners?

3. Please describe any high value export opportunities from Canada related to broader cybersecurity applications, whether commercial or defence, that can be leveraged as a result of these procurements.

Other

1. Given the significance of cyber resilience as an emerging technology area, would it be desirable for Canada to have a Value Proposition weighting, for the CSA and DCO-DS projects, of higher than 10% of the overall bid evaluation, in comparison to price and technical merit?

2. Within the Value Proposition, what are your recommended minimum percentages of weighting for each of the Value Proposition pillars (defence, supplier development, R&D, export, and other—if applicable)?

3. Should the CSA and DCO-DS projects include a Value Proposition pillar related to skills development?
   a. If yes, what types of investments and partnerships in skills development would be of highest value to the Canadian cyber sector?

4. In what business areas, whether in the defence or commercial sectors, do you see opportunities to assist aboriginal entrepreneurs and businesses, and women entrepreneurs or women-owned businesses in Canada?

Next Steps

- Your feedback will be used to develop a strategy for leveraging economic benefits from the CSA and DCO-DS procurements, to foster innovation in the Canadian cyber sector, including the growth of Canadian companies and creation of jobs across the country.

- For more information on Industrial and Technological Benefits as well as the Value Proposition Guide, please visit:

  http://www.canada.ca/itb

- Please provide your written responses to the questions in Annex F of the RFI to the PSPC Contracting Authority.

National Defence Défense nationale

Operational Requirements Overview

- Maj Martin Rivard, Project Director, CSA/DCO-DS
- Mr Raghu Balakrishnan, Project Manager, CSA/DCO-DS

Canada

Outline

- Background
- Vision
- Operational View
- Operational Mentor and Capability Development Team
- Cyber Entities
- Cyber Defence Functions and Tasks
- Performance Objectives
- Data Quality and Confidence
- Notional Component Architecture View
- Information Requested

Policy Coverage

- Strong Secure Engaged: Canada's Defence Policy (June 2017) (SSE #65 and SSE #87)
- Canada's Industrial and Technological Benefit (ITB) Policy

Introduction: A New Canadian Defence Policy

CANADIAN INTERESTS

Protection of Canada and Canadians □ Leadership in the World □ Global Stability and Conflict Prevention, Peace, Prosperity, and Trade □ Human Rights, Inclusion, and Gender Equality

WHY CHANGE IS NEEDED

New sources of threat

Rising instability and unpredictability, erosion of the global order

Years of underinvestment and short-term management of people and capital within Defence

New opportunities

KEY AREAS FOR CHANGE

New policy and new investments

Structural change

STRONG. SECURE. ENGAGED.
AT A GLANCE

STRONG AT HOME

- Enhanced air and maritime surveillance and control, including Arctic
- Concurrent response to multiple domestic emergencies
- Support to counter-terrorism
- Search and rescue support
- Looking after our people

SECURE IN NORTH AMERICA

- Modernize NORAD
- Expanded aerospace and maritime domain awareness and control
- Cutting edge defence innovation

ENGAGED IN THE WORLD

CAF prepared to concurrently deploy:

- 2 major sustained deployments
- 1 major time-limited deployment (6-9 months)
- 2 minor sustained & 2 minor time-limited deployments
- 1 Disaster Assistance Response Team (DART) mission
- 1 Non-combatant Evacuation Operation

NEW INITIATIVES

Putting our People First

- New **Total Health and Wellness Strategy**
- Reinvented **transition of ill and injured** to service/civilian life
- **Tax relief** for deployed operations
- Taking care of **Families**
- **Integrate GBA+** and meet **gender** & **diversity** targets
- **Increase of 3,500 Regular Force** for key priorities
- **Increase of 1,500 Reserve Force** – full-time capability, part-time force
- **Increase of 1,150 civilians** to support operations

Investing in the Future Force

- **Invest** additional $62B for capital expenses to $104B
- Rebuild **core capabilities**: **88** fighter aircraft, **15** surface combatants, [illegible] joint support ships, **6** Arctic offshore patrol ships
- Increase emerging capabilities in **cyber**, **space**, and **remotely piloted vehicles** to maintain effectiveness and interoperability with allies
- Capability enhancements, including **intelligence**, **satellite communications**, **surveillance** and **logistics vehicles**

Modernizing the Business of Defence

- A **transformative innovation agenda** with defence research clusters linked to procurement
- More accountable, transparent, and streamlined **defence procurement** process
- **Reduced carbon footprint** through green infrastructure and focus on energy efficiency
- Modernized **infrastructure management** through expanded partnership with the private sector

Background

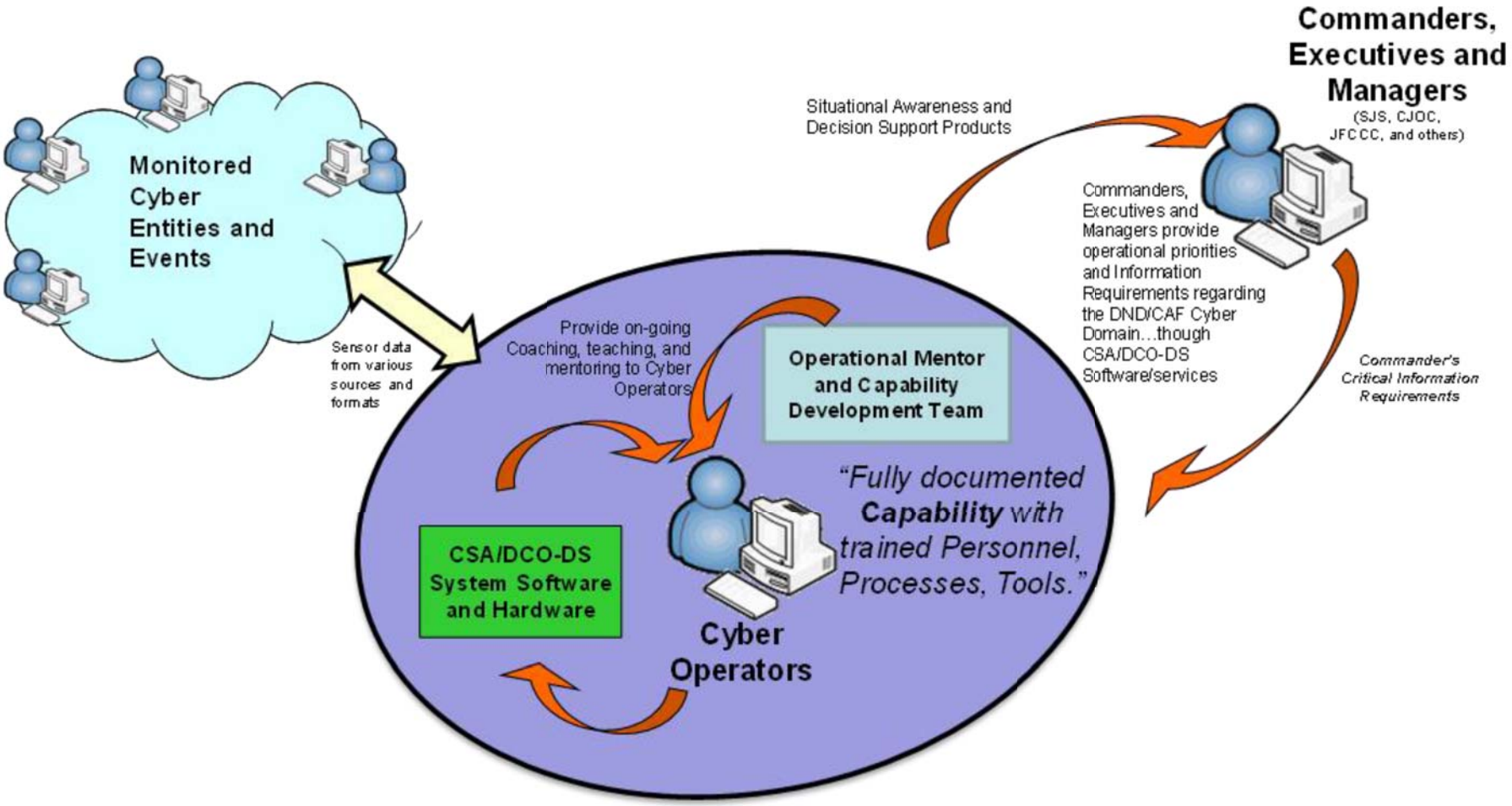
- The **CSA project** will transform how DND/CAF manages the confidentiality, integrity and availability of the increasingly complex DND/CAF cyberspace. This will be accomplished by focusing on identifying and securing its cyberspace, providing an end-to-end situational awareness that enables commanders to make informed decisions concerning the security posture of their cyberspace.

- The **DCO-DS project** will improve DND/CAF's ability to conduct Defensive Cyber Operations (DCO). This will be accomplished by providing a response capability against advanced threats, and enhancing DCO decision making, making the process more agile, responsive and effective in order to maintain Commanders' freedom of manoeuvre in cyberspace.

Vision

The CSA and DCO-DS Projects' Vision is to provide the CAF with a sustainable, state-of-the-art cross domain defensive cyber security operations capability.

Operational View



The Task of the Cyber Operators

- In the context of the CSA & DCO-DS projects, the task of the Cyber Operators is to:
  - "secure DND/CAF Cyber Domain to support the defence of Canada"
- For this task to be successful, the Cyber Operators require tools and procedures to:
  - detect, recognize and identify hostile or otherwise unauthorized **cyber entities** within the DND/CAF Cyber Domain, and
  - provide Commanders, Executive and Managers with the timely information to make informed decisions.

Cyber Entities

- “any distinct thing or actor that exists within the cyber infrastructure [cyberspace].”

  - **Non-human Cyber Entities**. These are participant system elements (physical or virtual) such as workstations, routers, switches, processes, files, servers and memory. The table at Appendix 2 to Annex B lists the key attributes that must (where applicable) be collected for each non-human cyber entity.

  - **Human Cyber Entities**. These are actual people and their personas operating within cyberspace. The table at Appendix 3 to Annex B lists the key attributes that must (where applicable) be collected for each human cyber entity.

Operational Mentor and Capability Development (OMCD)

- Professional services, in the form of OMCD team, will be co-located with the delivered capability during implementation and throughout its life-cycle.

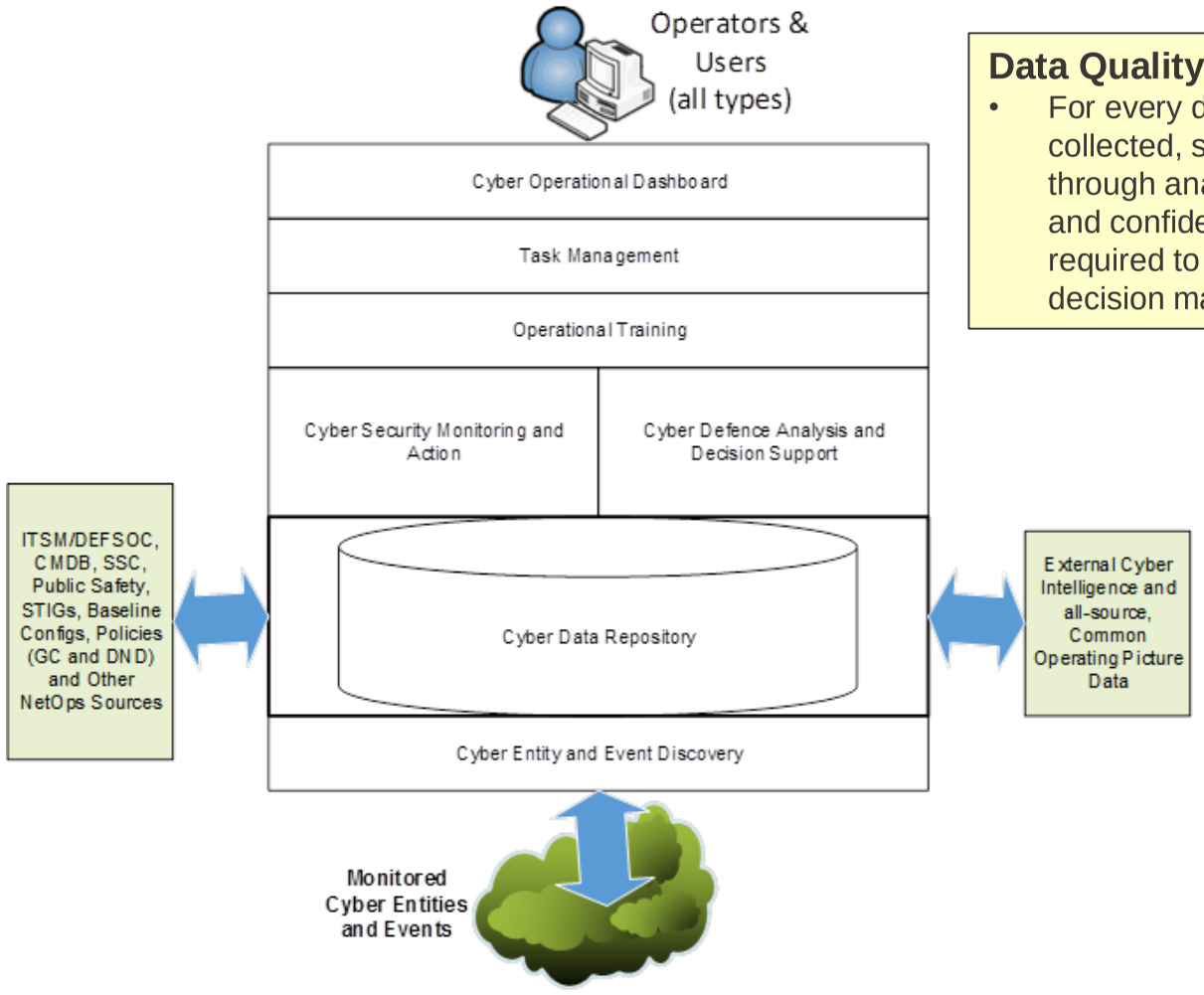
- The role of OMCD is to coach, teach and mentor the cyber operators (at all applied rank levels) to achieve their mission through continuous:
  - business transformation,
  - skills development,
  - collective training development and coordination, and
  - cyber tool development and sustainment.

Capability Performance Objectives

… detect, recognize and identify hostile or otherwise unauthorized cyber entities within the DND/CAF Cyber Domain, and provide Commanders, Executive and Managers with the timely information to make informed decisions.

Response Time	Activity
Within Seconds	**Aim: DETECTION.** Detect that a Cyber Entity has become active (connected) and initiate automated responses appropriate for the situation. Initiate Data Collection and Control.
Within Minutes	**Aim: RECOGNITION and IDENTIFY.** Determine nature of a Cyber Entity (Friend or Foe), its key attributes and initiate automated responses appropriate for the situation. Continue Data Collection and Control.
Within an Hour	**Aim**: Complete **IDENTIFICATION** with full classification and attribution to initiate more comprehensive actions.
Within a Day	**Aim**: **Updated Threat/Risk Analysis and Defensive Planning,** supported by on-going Forensic and Intelligence gathering.
Within a Week	**Aim**: Implement new defense techniques operational with new tactics, techniques and procedures based on lessons learned.
Within a Month	**Aim**: Evolve the overall security posture of DND/CAF Cyber Domain to an improved defensive capability.

Notional Component Architecture View



Data Quality and Confidence:

- For every data field or attribute collected, stored or deduced through analysis, a data quality and confidence figure of merit is required to enable sound decision making.

Information Requested

- Section 1: Executive Summary
- Section 2: Corporate Profile:
- Section 3: Proposed Concept of Solution. Respondents are asked to provide:
  - Outline Plan of Solution
  - High Level Outline Plan and Sequence of Events
  - Estimated Costs for Each Deliverable (using the Notional Component Architecture View approach if possible)
    - an indicative cost estimate, with a per-unit description, for any or all deliverables defined in Annex B that the respondent intends to provide.
    - Cost = Price/Unit x Quantity of Units
- Section 4: General Comments and Advice.

This is critical to help the project develop a project budget for the approval process.

Key Pricing Information Required

- Project Management, Integration Engineering and System Design and supporting Documentation
- All hardware, software, installation, system configuration, and acceptance testing
- Business Transformation Services
- In-Service Support System and Professional Engineering Services
- Initial-cadre training
- Essential that pricing models are scalable based on:
  - Number of users on network?
  - Number of Points of Presence or Sites?
  - Number of key nodes or servers?
  - Number of events per second per device, IT asset, Cyber entity, etc.
  - Or some combination of above

QUESTIONS

CLOSING REMARKS

THANK YOU!