Rethinking Security Requirements in the Federal Procurement Process

Public Services and Procurement Canada
Services publics et Approvisionnement Canada

Canada

CIPMM 2023
Toronto Workshop

November 1, 2023

John Von Zuben
Assets and Facilities Management: Centre of Expertise – Security
Public Services and Procurement Canada
Ontario Region

Presentation Overview

- Contract Security Program (CSP)
- Security requirements and screenings
- Screening timelines and validity periods
- Special considerations for IT and cloud
- CSP Application for Registration form
- Screening process for foreign suppliers
- Contract security best practices
- Tools for suppliers
- Contact us

Contract Security Program (CSP)

- Supports federal government departments in the delivery of services and activities through the security screening of private sector organizations and personnel requiring access to protected/classified information and assets, or to secure sites
- Operates in a rapidly evolving industrial security landscape – supporting Government of Canada priorities by seeking to balance national security interests with economic prosperity for Canadian industry
- Is triggered based on contract security requirements identified by federal government departments and agencies, when
  - PSPC is the contracting authority or upon request by the contracting department
  - domestic contracts with security requirements are awarded to foreign suppliers or involve access to foreign or NATO classified information
  - when foreign contracts with security requirements are awarded to Canadian industry

Security Requirements and Screenings

Provisional security clearance

- required for organizations that need to access protected or classified information and assets at the pre-solicitation or bid preparation stage of a procurement process

Designated organization screening

- required for organizations that need to access protected information and assets, and/or operations zones to execute a contract or subcontract

Facility security clearance

- required for organizations that need to access classified information and assets (confidential, secret, top secret) and/or restricted security zones to execute a contract or subcontract

Foreign ownership, control or influence (FOCI) evaluation

- required for organizations that need to access COMSEC, NATO classified and foreign classified information or assets to execute a contract or subcontract

Security Requirements and Screenings (cont'd)

Document safeguarding capability

- required for organizations that need to safeguard protected or classified information and/or assets at their business location(s) to execute a contract or subcontract

Authority to process information technology (IT)

- required for organizations that need to use their own IT system(s) to produce, process or store sensitive information electronically to execute a contract or subcontract

Personnel screening: Reliability status

- required for employees of an organization who need to access protected information or assets and/or to operations zones to perform work on a contract or subcontract

Personnel screening: Security clearance (secret or top secret)

- required for employees of an organization who need to access classified information or assets and/or restricted security zones to perform work on a contract or subcontract

Security Requirements and Screenings (cont'd)

Type of screening	Initiation	Completion
Provisional security clearance	Pre-solicitation stage (for all potential bidders)	Before access is granted
Designated organization screening	Bid evaluation stage (for all confirmed bidders)	At contract award
Facility security clearance	Bid evaluation stage (for all confirmed bidders)	At contract award
FOCI evaluation	Once the successful bidder has been selected	At contract award
Document safeguarding capability (DSC)	Bid evaluation stage (for all confirmed bidders)	After contract award, before access is granted
Authority to process IT	After contract award, once DSC is granted	Before access is granted
Personnel security screening	At or after contract award	Before access is granted

Screening Timelines and Validity Periods

Type of screening	Timelines	Validity period
Provisional security clearance	Varies based on level	Duration of solicitation process
Designated organization screening	2 months or more	Minimum 2 year
Facility security clearance (conf/secret)	6 months or more	Minimum 1 year
Facility security clearance (top secret)	12 months or more	Minimum 1 year
FOCI evaluation	6 months or more	Duration of contract
Document safeguarding capability	45-90 business days	Duration of contract
Authority to process IT	45-90 business days	Duration of contract
Reliability status (simple vs complex)	7 vs 120 business days	Up to 10 years
Secret clearance (simple vs complex)	75 vs 120 business days	Up to 10 years
Top secret clearance	12 months or more	Up to 5 years

Special Considerations for IT and Cloud

- Cloud service providers must first be assessed by the Canadian Centre for Cyber Security (CCCS) – consult the **CCCS website** for a list of assessed cloud service providers
- Cloud solutions can be utilized to house data up to protected B within data centres located within Canada
- Suppliers that need to access protected A and B information via a cloud solution require a designated organization screening and a document safeguarding capability
- These suppliers also require an authority to process IT if they will be using their own IT systems to access the cloud solution and GC IT infrastructure
- The supplier's company security officer and personnel identified as *privileged users* require secret level clearance
- The client department must identify how the supplier will be accessing the secured environment and conduct a local IT assessment of the cloud solution utilized for the contract

Special Considerations for IT and Cloud (cont'd)

When a procurement requires the use of cloud solutions, departments must:

- complete a security classification guide to identify the various levels of screening required for each position/task
- include both the security classification guide and the statement of work with the security requirements check list (SRCL) submission package to the CSP
- obtain cloud-specific contract security clauses from the CSP and insert them in the contractual documentation
- upon contract award, **provide the awarded contract**, the IT technical document and approved SRCL to the CSP

In addition, departments should:

- clearly identify in block 4 of the SRCL that there are cloud security elements
- ensure to include ″cloud″ in the email subject line when summiting the SRCL package to the CSP

Special Considerations for IT and Cloud (cont'd)

Example of a Security Classification Guide To be completed in addition to question 10.a) of the SRCL when multiple levels of personnel screening are therein identified. Indicate which personnel screening levels are required for which portions of the work / access involved in the contract.			
level of personnel clearance (e.g. reliability, secret)	position / description / task	access to sites and/or information + levels of information to be accessed	citizenship restriction (if any)
Reliability status	IT infrastructure contractor working on data migration	Access to operational zones Access to server data library	
Secret clearance	Privilege user, configuring the cloud security controls, access rights and system architecture	Access to the cloud system infrastructure	

CSP Application for Registration Form

To sponsor Canadian suppliers for security screening when security requirements have been identified, procurement officers are required to collect the CSP Application for Registration form (AFR) from the suppliers for:

- ✓ pre-solicitations
- ✓ competitive solicitations
- ✓ requests for standing offer (SO) and requests for supply arrangement (SA)
- ✓ sole source and directed contracts

Instances where collecting the AFR is not mandatory:

- × To sponsor an underrepresented supplier, as part of social procurement
- × To sponsor an organization for an upgrade to their existing security clearance, as part of a solicitation process conducted under a PSPC-issued method of supply (i.e., an established SO or SA)

Screening Process for Foreign Bidders

- If foreign suppliers are bidding on a contract with security requirements, the procurement officer must
  - collect the Initial International Security Screening form from the foreign supplier as part of their bid response
  - sponsor the foreign supplier for security screening during the bid evaluation stage
- Upon receipt of the sponsorship request:
  - Classified level: Canada's designated security authority (DSA) will contact the national security authority (NSA) or DSA of the foreign supplier's country to request a facility security clearance per the bilateral security instrument in place with the foreign NSA/DSA
  - Protected level: The CSP will determine if an alternative solution can be put in place based on the foreign supplier's country of origin (foreign supplier will be required to provide proof of how they will meet the security requirements, with the concurrence of equivalencies accepted by Canada's DSA)

Contract Security Best Practices

Early engagement

- Remove the guesswork by engaging with the CSP for advice and guidance on complex procurements before releasing the RFP/RFI/ITQ, particularly when foreign bidders are involved

Foreplaning

- Reduce delays by planning ahead and working with clients to integrate CSP processing times in project and procurement timelines, particularly for classified and NATO classified contracts

Project phasing

- Award contracts faster by phasing-in security requirements when access to sensitive information/assets/sites is only required for later phases of the project or contract

Risk mitigation

- Reduce red tape by challenging overinflated security requirements and risk-mitigating access
- Consult the CSP for advice and guidance on risk acceptance and mitigation strategies

Tools for Suppliers

The CSP offers tools to help diverse suppliers navigate the security screening process and complete the necessary forms, including :

- An **information toolkit** for suppliers
- **Guidance** on completing the CSP Application for Registration form
- **Pre-recorded webinars** on obtaining a designated organization screening, facility security clearance and document safeguarding capability
- **Instructional videos** on completing personnel security screening forms
- A **guide** to completing and submitting personnel security screening forms

Contacting the CSP

General inquiries

Phone

Toll-free: 1-866-368-4646
National capital region: 613-948-4176
Monday to Friday, 9 am to 12 pm and 1 pm to 5 pm (Eastern time)

Email

ssi-iss@tpsgc-pwgsc.gc.ca

Website

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




©Copyright