DRAFT FOR CONSULTATION

Cloud-based Security Services (CSS) Solution Pre-Screening Process

Purpose:

The purpose of the pre-screening process is to qualify and rank the CSS solutions against a set of mandatory and rated criteria that will allow Canada to rank the top scoring solutions, including a set aside of 1 solution who's OEM is a Small Medium Enterprise (SME). The provider of the top scoring solutions will be invited to sign a contract for the proof of concept so that Canada can work with the solution provider to ensure it meets the MVRs and to compare the solution against each other to select the best fit solutions. The result of this process is a set of qualified solutions.

Once the solutions are qualified, Canada will proceed with qualifying solution providers for each qualified solution and award a Standing Offer to those who qualify. Subsequently, Canada will select the solution provider for the SSC enterprise deployment.

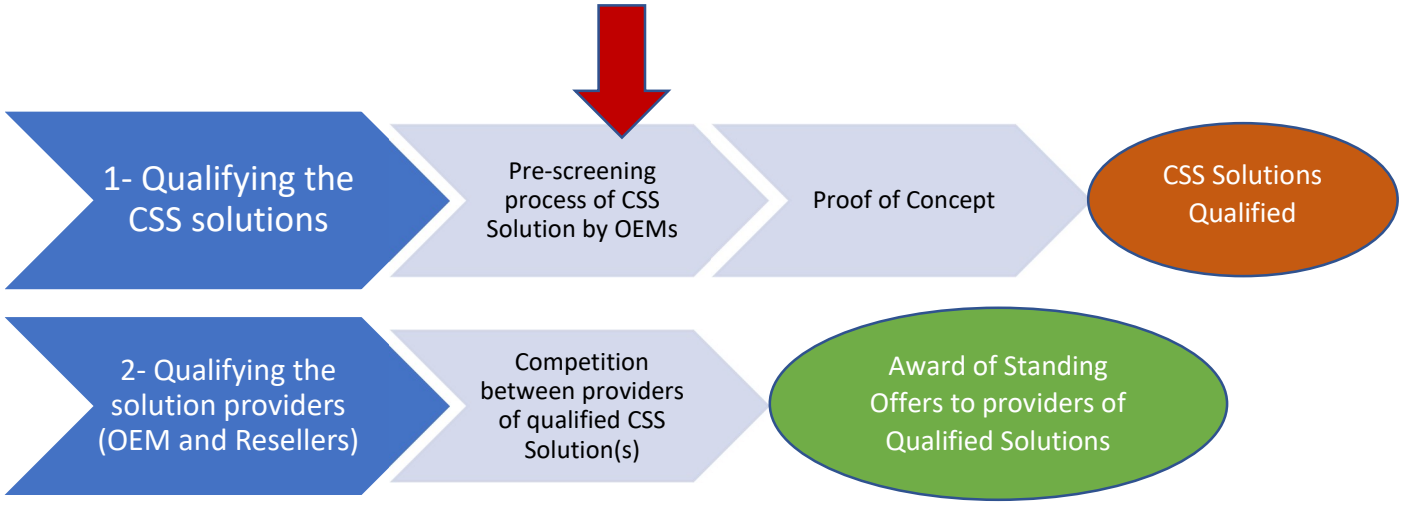

Figure 1: Proposed process diagram

Process:

The pre-screening applies evidence-based criteria that will be assessed and scored using a 3-part process as follows:

- Part A – Certification and Mandatory Requirements: The solution OEMs are requested to respond in writing to a set of required certifications and a first set of mandatory and rated criteria.
    - To be declared responsive, the solution OEM bid must comply with certifications and meet mandatory requirements.
    - Nonresponsive solution OEMs will be provided with feedback and one opportunity to remediate their response for any unmet certification or mandatory requirements .
    - Responsive solution OEMs will be invited to move on to Part B.

- Part B – Written Rated Response and Interactive Virtual Session: The written response to the rated criteria will be evaluated by the evaluation team and the solution OEMs will be invited to a 75-minute interactive virtual session to demonstrate their capacity to meet a second set of rated criteria.

Canada may decide to invite the top eight (8) ranking solution OEMs to a Demonstration stage.

Canada may decide to move directly to Proof of Concept under the following circumstances:

- if 6 or less solutions are responsive; or
- if 6 or less solutions have achieved a total rated score of 32 points or more in Part B Written Rated Response and Interactive Virtual Session. A total of 43 rated points are available.

The top four (4) ranking solution OEMs will be requested to submit a price proposal for the Proof of Concept as per the CBSOS and Statement of Work. The remaining responsive solution OEMs, if any, will remain in the queue.

If during the Proof of Concept, one or more of responsive solution OEMs do not satisfy the Minimum Viable Requirements, Canada may invite the next ranking responsive solution OEM in the queue to participate.

Part A – Certifications and Mandatory Requirements

Certifications

The following certifications must be submitted as part of the pre-screening process Part A by completing the table below with the signature, name, title of a person authorized to sign on behalf of the solution OEM.

Table 1: Certifications

Certifications	**Self Assessment**		**Signature Name and Title of person authorised to sign on behalf of the solution OEM**
	Met	**Not Met**	
C1: Original Equipment Manufacturer (OEM) Certification **I certify that I am the OEM of the proposed CSS solution.** The definition of OEM is as follows: The company that makes the products (the "original" manufacturer).			
C2: SaaS Solution Certification **I certify that the proposed CSS solution is a Software as a Service (SaaS) solution.** The definition of SaaS is as follows: *Software that is owned, delivered and managed remotely by one or more providers. The provider delivers a software service based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at anytime on a pay-for-use basis or as a subscription based on use metrics.*			
C3: CSS Use Cases Compliance Certification			

Certifications	Self Assessment		Signature Name and Title of person authorised to sign on behalf of the solution OEM
	Met	Not Met	
I certify that the proposed CSS solution can meet the Use Cases defined within the CBSOS document, Attachment A – Statement of Challenge. Titles of each Use Case are provided below for ease of reference: • Use Case 1a: Mobile User (managed device) accessing Cloud-Based Services • Use Case 1b: Mobile User (managed device) accessing GC On-Premise (EDC) Services • Use Case 2a: Mobile User (non-GC managed device) accessing Cloud-Based Services • Use Case 2b: Mobile User (non-GC managed device) accessing GC On-Premise (EDC) Services • Use Case 3a: BYOD User accessing Cloud-Based Services • Use Case 3b: BYOD User accessing GC on-premise (EDC) Services • Use Case 4a: User Access to Internet of Things (IoT)/Scientific Devices via the Internet • Use Case 4b: IoT/Scientific Devices access other IoT/Scientific Devices or systems via the Internet • Use Case 5a: External User using a Non-GC Managed or BYOD Device accessing GC Cloud Services • Use Case 5b: External User using a Non-GC Managed or BYOD Device accessing GC On-Premise (EDC) Services • Use Case 6a: User (Managed Device) at a remote GC site accessing Cloud-Based Services • Use Case 6b: User (Managed Device) at a remote GC site accessing GC On-Premise (EDC) Services • Use Case 7: User with a Managed Device at a remote GC site accessing cloud-based services via the Internet, and GC On-Premise (EDC) Services via a Regional Hub			
C4: Multi-Tenant Management Certification I certify that the proposed CSS solution provides multi-tenant management to allow GC administrators from different organizations to manage, generate customized reports and administer specific portions of the solution within their authorized domain, as follows: • Administrator 1 can manage, administer, and generate templated and customized reports for Tenant 1. • Administrator 1 cannot manage, administer, or generate templated and customized reports for Tenant 2. • Administrator 2 can manage, administer, and generate templated and customized reports for Tenant 2. • Administrator 2 cannot manage, administer, or generate templated and customized reports for Tenant 1. • Administrator 3 can manage, administer, and generate templated and customized reports for Tenants 1, 2 and the service as a whole.			

Certifications	Self Assessment		Signature Name and Title of person authorised to sign on behalf of the solution OEM
	Met	Not Met	
Definitions related to Multi-Tenant Management: In the context of the CSS Pre-Screening, multiple domains, multi-tenant or multi-tenancy means a mode of operation of software where multiple independent instances of one or multiple functions, features, applications and/or network communications and network transactions that operate in a shared server or appliance. The instances (tenants) are logically isolated, but physically integrated. The degree of logical isolation must be complete, but the degree of physical integration will vary.			

Mandatory Requirements

The following mandatory requirements must be met.

The solution OEM must submit the table below, completed with a self-assessment and a refence to where the substantiating evidence is located in the written response. Evidence may include:

- Screenshots of the solution in use
- Extracts from product technical specifications or documentation
- Product manuals
- System architecture and design diagrams

Table 2: Mandatory Requirements

Mandatory Requirements	Self Assessment		Reference to Evidence Provided
	Met	Not Met	
M1 – Cloud-based perimeter security services The solution must provide cloud-based perimeter security services. The solution OEM must demonstrate that the CSS solutions provides the following list of perimeter security services: a) A Layer 4-7 firewall that permits and denies access based on IP addresses, ports, protocols, application, identity, groups, and locations, such as a Next Generation Firewall (NGFW); b) Filtering of malicious software and malware from user-initiated internet traffic and enforces policy compliance for web traffic, and prevents access to unacceptable and illegal web sites and web sites known to contain malicious threats and viruses, such as a Secure Web Gateway (SWG); c) Analyze the decrypted traffic for intrusion attempts and block intrusions, such as an Intrusion Detection and Prevention System (IDPS);			

Mandatory Requirements	Self Assessment		Reference to Evidence Provided
	Met	Not Met	
d) Identify and block malware embedded in files in transit and files containing malware, protecting against current and new threats. The solution evaluates and determines progressive and highly sophisticated advanced threats by inspecting applicable file contents, such as an Advanced Threat Detection (ATD); e) Decrypt and inspect SSL and TLS traffic for threats, protecting SSC against efforts to use malicious code hidden in encrypted traffic flows, such as a Secure Sockets Layer, Transport Layer Security (SSL/TLS) Inspection); and f) Recognize file transfers via SCP and SFTP, to be inspected by other security services, such as an SSH Inspection.			
M2 - User Experience Measurement Capability The solution must provide a historical user experience measurement capability that reports on user experience and trends using a rating scale. A rating scale is defined as a qualitative scale that measures the users experience from poor to high user experience. The solution OEM must demonstrate the user experience measurement capability in the form of screenshots of a dashboard or a report that includes historical user experience and trends.			

Part B – Written Rated Response and Interactive Virtual Session

Written Rated Criteria

The following rated criteria will be rated as per the point allocation described in the table.

The solution OEMs must submit the table below, completed with a self-score and a refence to where the substantiating evidence is located in the written response. Evidence may include:

- Screenshots of the solution in use
- Extracts from product technical specifications or documentation
- Product manual
- System architecture and design diagrams
- Copies of certifications

Table 3: Rated Criteria – Written Response

Rated Criteria	Point Allocation Max Score = 43 points Self-Score	Reference to Evidence Provided
WR1: On-Premise and Cloud-based CSS Deployment (3 Points) The solution OEM should provide evidence that the proposed CSS solution is capable of deploying an instance of the CSS solution in a physical location as determined by the GC, such as a GC Enterprise Data Centre (EDC), that is fully managed by a centralized CSS management platform that manages both on-premise CSS deployments and a cloud-based CSS environment. The solution OEM should provide extracts from product technical specifications to confirm that the proposed solution can be fully implemented in a data center.	Points will be allocated as follows: The evidence of this capability is demonstrated = 3 points The evidence of the capability is not adequately demonstrated = 0 points **Self-Score:**	
WR2: Deployment Readiness: CCCS Assessment Process (10 Points) The solution OEM should provide evidence that the proposed CSS solution has completed or is in the process of completing the Canadian Centre for Cyber Security (CCCS) Cloud Service Provider (CSP) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100). The solution OEM should provide documentation from CCCS in the form of a letter, an email or a report that confirms that the process is complete or is in progress.	Points will be allocated as follows: • The evidence is demonstrated = 10 points • The evidence is not demonstrated = 0 points **Self-Score:**	

Rated Criteria	Point Allocation Max Score = 43 points Self-Score	Reference to Evidence Provided

WR3: Security Readiness (Up to 10 Points)
The solution OEM should provide evidence that the proposed CSS solution is in the process of or has completed the independent third-party certifications listed below.
 	
The solution OEM should provide the certification documentation or confirmation from the third-party that the certification is in progress for each of the following.
 	
(a) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Certification achieved by an accredited certification body.
 	
(b) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services achieved by an accredited certification body.
 	
(c) ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors – Certification achieved by an accredited certification body
 	
(d) AICPA Service Organization Control (SOC) 2 Type II Audit Report 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality - issued by an independent Certified Public Accountant.
	For (a), (b) and (c), points will be allocated as follows for each certification:
	• Currently have the certification = 2 points
	• Currently in the certification process, but not completed = 1 points
	• Not certified, and not currently in the certification process = 0 points
	
	Self-Score:
	
	For (d), points will be allocated as follows:
	• Currently have the certification = 4 points
	• Currently in the certification process, but not completed = 2 points
	• Not certified, and not currently in the certification process = 0 points
	
	Self-Score:	

WR4: Endpoint Security Integration (Up to 3 Points) The solution OEM should provide evidence that the solution can automate the responses to threats that have been identified by the following endpoint security products: a) McAfee ePO b) Windows Defender c) Cisco AMP for Endpoints The term “automate”, “atomically”, and “automatic” refer to a process or event that takes place without any human intervention. The solution OEM must provide documentation (references to product manuals and screen shots from solution configuration screens) to confirm that the proposed solution meets this requirement.	For each security product listed above, points will be allocated as follows: • The capability is demonstrated = 1 point • The capability is not demonstrated = 0 points **Self-Score:**	

Rated Criteria	Point Allocation Max Score = 43 points Self-Score	Reference to Evidence Provided
WR5: Data Residency (Up to 10 Points) The solution OEM should provide evidence that the CSS solution is currently deployed in an environment where the data and control planes of the solution reside within Canada. The solution OEM must provide documentation that confirms the solution satisfies this requirement.	Points will be allocated as follows: • The criteria is demonstrated = 10 points • The criteria is not demonstrated = 0 points **Self-Score:**	
WR6: Remote Browser Isolation (RBI) Capability (Up to 4 Points) The solution OEM should demonstrate that the solution's RBI capability can permit and deny: a) file uploads b) file downloads c) screen captures d) copy and pasting of any information being displayed **RBI is defined as a** native RBI capability that allows for a user's web browsing activity to be executed on a remote server in an isolated environment, instead of on the user's computer. RBI is hosted in the CSS OEMs cloud environment, protecting user computers from web-based threats, containing the threats to the isolated environment. The solution OEM must provide extracts from product technical specifications, product manuals or screenshots to confirm that the proposed solution meets the RBI capability.	For each capability listed, points will be allocated as follows: • The capability is demonstrated = 1 point • The capability is not demonstrated = 0 points **Self-Score:**	
WR7: Non-Web-based App access (Up to 3 points) The solution OEM should demonstrate the solution's capability to provide secure access to non-Web-based applications for mobile users who are using a BYOD device with no CSS client software installed, via the following features: a) Remote Desktop Protocol (RDP); b) Secure Shell (SSH); and c) remote file system mounting like Server Message Block (SMB). A non-web-based application is an application that is accessed without the use of a web-browser, and is typically executed on a users computer.	Points will be allocated as follows: • The feature is demonstrated = 1 point • The feature is not demonstrated = 0 points **Self-Score:**	

Rated Criteria for the Interactive Virtual Session

The solution OEMs who have met the certifications and the mandatory requirements will be invited to a 75-minute Interactive Virtual Session. The rated criteria must be demonstrated using the actual solution, either in a production or demonstration environment, using the same software versions as the production solution.

Table 3: Rated Criteria – Interactive Virtual Session

	Rated Criteria for the Interactive Virtual Session **Max Score = 20 Points**
IR1	**User Experience – Latency Measurements (Up to 6 Points)** The solution OEM should provide evidence that the solution is capable of providing latency measurements on a hop-by-hop basis. The following evidence should be demonstrated: • the latency of all hops; and • hops through the internet from the user's endpoint to the destination. Points will be allocated as follows for each evidence: • The evidence is demonstrated = 3 points • The evidence is partly demonstrated (not showing all hops) = 2 points • The evidence is not demonstrated = 0 points
IR2	**User Experience – Application Response Time (2 Points)** The solution OEM should provide evidence that the solution can determine destination public and private application availability and response time to determine if the application is responsible for poor user experience. Points will be allocated as follows: • The capability is demonstrated = 2 points • The capability is not demonstrated = 0 points
IR3	**Cloud Access Security Broker (CASB) (3 Points)** The solution OEM should provide evidence that the solution has a native CASB capability that includes: a) Data Loss Prevention (DLP); b) User and Entity Behaviour Analytics (UEBA); c) Government Regulatory and policy compliance; and d) Threat detection. Points will be allocated as follows: • The four listed capabilities are demonstrated = 3 point • Three or less of the listed capabilities are not demonstrated = 0 points
IR4	**Cloud Security Posture Management (CSPM)(Up to 3 points)** The solution OEM should provide evidence that the solution has a native CSPM capability that: a) monitors, assesses and evaluates security compliance and regulatory violations in IaaS and PaaS environments; and b) notifies administrators and provides reporting of security policy non-compliance, misconfigurations, and regulatory violations and automates their remediation. Points will be allocated as follows: • The two listed capabilities are demonstrated = 3 points • One or less of the capabilities are demonstrated = 0 points
IR5	**SaaS Security Posture Management (SSPM)(Up to 3 points)**

	Rated Criteria for the Interactive Virtual Session **Max Score = 20 Points**
	The solution should provide evidence that the solution has a native SSPM capability that: a) monitors and detects settings that introduce security risks in SaaS environments; b) provide alerts for misconfigurations; and c) either automates **or** provides guided remediation to resolve the risks. Points will be allocated as follows: • The three listed capabilities are demonstrated = 3 points • Two or less of the listed capabilities are not demonstrated = 0 points
IR6	**Auto Application Discovery (3 points)** The solution OEM should demonstrate the solution's capability to: a) automatically discover, identify, and display applications within the CSS management interface, that are being requested and accessed by CSS users or devices, without having to import logs; and b) allow CSS administrators to directly apply access policies to these applications via the CSS management interface, after the application has been automatically discovered and identified. Points will be allocated as follows: • The two listed capabilities are demonstrated= 3 points • One or less of the listed capabilities are not demonstrated = 0 points