SHARED SERVICES CANADA

Challenge-Based Standing Offer Solicitation (CBSOS) - Initial

For

Cloud-based Security Services (CSS)

Solicitation No.	CSS092421B	Date	March 29, 2022

GCDocs File No.	101691102	Amendment No. 4

Issuing Office	Shared Services Canada 180 Kent Street, 13th Floor Ottawa, Ontario K1P 0B5	
Standing Offer Authority (The Standing Offer Authority is the person designated by that title in the Solicitation, or by notice to the Offeror, to act as Canada's "Point of Contact" for all aspects of the Solicitation process.)	Title	Christopher Bromfield
	Telephone No.	(343) 550-3959
	Email Address	christopher.bromfield@canada.ca
Closing Dates and Times 1. Invitation to Pre-screening Solutions (Closing 1) 2. Solicitation Closing - OEM (Closing 2) 3. Solicitation Closing - Resellers (Closing 3)	1. April 4, 2022 at 15:00 2. (To be Determined) at 15:00 3. June 30, 2022 at 15:00	
Email Address for Submitting Offers	christopher.bromfield@canada.ca	
Time Zone	EDT	
Destination of Goods/Services	See Herein	
Vendor/Firm Name and Address	Telephone No. :	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)	Name/Title Signature Date	

CBSOS - Initial for CSS: Invitation to Pre-screening Solutions

Purpose of Pre-screening Process

The purpose of the pre-screening process is to qualify and rank OEM Solutions against a set of mandatory and rated criteria that will allow Canada to rank the top scoring Solutions. The OEMs of the top scoring Pre-Qualified Solutions will be invited to sign a contract for the Proof of Concept so that Canada can work with the OEMs to ensure their Pre-Qualified Solution meets the Minimum Viable Requirements and to compare Pre-Qualified Solutions 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 Offerors (OEMs and Resellers) for each Qualified Solution and award Standing Offers to those who qualify. Subsequently, Canada will select the Qualified Solution Offerors for deployment.

Amendment No. 04

1. Amendment to SECTION 3 - OFFER PREPARATION INSTRUCTIONS

INSERT:

3.1 Submission of Written Documents by Offerors

Offerors are required to submit written documents at the following stage:

a) Stage 4B - Invitation to Pre-screening Solutions (Solicitation Closing 1) (See 3.1.1)

3.1.1 CBSOS Initial - Invitation to Pre-screening Solutions (Solicitation Closing 1)

The OEM Offerors must complete and submit the Table 1: Certifications, Table 2: Mandatory Requirements, and Table 3: Rated Criteria - Written Responses, by using the Pre-screening Solutions Tables (Annex A). The Tables must be received no later than the Offer Closing Date and Time of the CBSOS identified on the cover page of the Solicitation.

INSERT:

3.2 Electronic Submission of Offers Through Email

Electronic Submission of Offers Through Email

All Offerors must submit their Offers by email by the Offer Closing Date(s) to the email address identified on the cover page of the Solicitation as the "Email Address for Submitting Offers".

Electronic submission of Offers is mandatory.

a) Submission through Email: All Offerors must submit their Offers by email, as specified in this section.

b) Submissions not permitted after Offer Closing: Only emails that are received at the Email Address for Submitting Offers by Offer Closing will be considered part of the Offer.

c) Format of Offer Documents/Email Attachments: Offerors may submit Offers in any of the following approved formats:

i) PDF attachments; and

ii) documents that can be opened with either Microsoft Word or Microsoft Excel.

Offerors that submit Offers in other formats do so at their own risk, as Canada may be unable to read them.

d) Email Size: Offerors should ensure that they submit their Offer in multiple emails if any single email, including attachments, will exceed 10 MB.

e) Email Title: Offerors are requested to include the Solicitation number identified on the cover page of Solicitation in the "subject" line of each email forming part of their Offer.

f) Email Title Multiple Emails: Offerors that submit their Offer in multiple emails, are requested to indicate the number of the email and the total number of emails that encompass the Offerors entire Offer in the "subject" line of each email forming part of their submission (example "Email 1 of 5").

g) Time of Receipt: All emails received at the Email Address for Submitting Offers showing a "received" time before Offer Closing will be considered timely. In the case of a dispute regarding the time at which an email arrived at SSC, and the time at which the Offer is received by SSC will be determined:

i) by the delivery time stamp received by the Offer if the Offeror has turned on Delivery Status Notification for the sent email in accordance with RFC 1891 established by the Internet Engineering Steering Group (SMTP Service Extension for Delivery Status Notification); or

ii) if the Offeror has not turned on Delivery Status Notification for the sent email, in accordance with the date and time stamp on the SMTP headers showing the time of first arrival on a server used to provide the Government of Canada with email services.

h) Availability of PoC: During the 4 hours leading up to Offer Closing, an SSC representative will monitor the Email Address for Submitting Offers and will be available by telephone at the PoC's telephone number shown on the cover page of the Solicitation (although the SSC representative may not be the PoC). If the Offeror is experiencing difficulties transmitting the email to the Email Address for Submitting Offers, the Offeror should contact SSC immediately at the PoC's coordinates provided on the cover page of the Solicitation.

i) Email Acknowledgement of Receipt by SSC: On the day of Offer Closing, an SSC representative will send an email acknowledging receipt of each Offer (and each email forming part of that Offer, if multiple emails are received) that was received by Offer Closing at SSC's Email Address for Submitting Offers.

j) Delayed Email Offers: SSC will accept an email Offer received in the first 24 hours after Offer Closing only if the Offeror can demonstrate that any delay in delivering the email to the SSC Email Address for Submitting Offers is due to Canada's systems. Offers received

by email more than 24 hours after Offer Closing will not be accepted under any circumstances. As a result, Offerors who have tried to submit an Offer, but have not received an email acknowledging receipt from SSC should contact the PoC so that they can determine whether or not the Offer arrived at the SSC Email Address for Submitting Offers on time.

k) Responsibility for Technical Problems: By submitting an Offer, the Offeror is confirming it agrees that Canada is not responsible for:

i) any technical problems experienced by the Offeror in submitting its Offer, including emails that fail to arrive because they exceed the maximum email size of 10 MB or including email or attachments that are rejected or quarantined because they contain malware or other code that is screened out by SSC for security reasons; or

ii) any technical problems that prevent SSC from opening the email attachments. For example, if an attachment is corrupted or otherwise cannot be opened or cannot be read, it will be evaluated without that portion of the Offer. Offerors will not be permitted to submit substitute attachments to replace any that are corrupt or empty or submitted in an unapproved format.

2. Amendment to SECTION 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

INSERT:

SECTION 4 – EVALUATION PROCEDURES AND BASIS OF SELECTION

Offers will be assessed in accordance with the requirements of the Solicitation.

There are several steps in the evaluation process, which are described herein. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Offeror has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.

An evaluation team composed of representatives of Canada will evaluate the Offers. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

INSERT:

4.1 Evaluation Procedures – Pre-screening Process

The Pre-screening Process applies evidence-based criteria that will be assessed and scored using a 2-part process as follows.

Part A – Certification and Mandatory Requirements: OEMs are requested to respond in writing to a set of required certifications and mandatory requirements.

OEM responses must comply with the Certifications (Table 1) and meet the Mandatory Requirements (Table 2).

OEM responses that do not comply with the Certifications and meet the Mandatory Requirements will be provided with feedback and one opportunity to remediate their response for any unmet Certification or Mandatory Requirements.

Only OEM responses that comply with the Certifications and meet the Mandatory Requirements will be invited to move to Part B, where the Rated Criteria - Written Responses (Table 3) provided with their submitted written response will be assessed.

Part B – Written Rated Criteria and Interactive Virtual Session: OEMs are requested to respond in writing to Table 3: Written Rated Criteria with their response to Part A. OEM responses (Table 3) will be assessed, and OEMs will be invited to a 120-minute interactive virtual session to demonstrate their capacity to meet the rated criteria in the Attached Table 4: Rated Criteria - Interactive Virtual Sessions.

INSERT:

4.2 Basis of Selection – Pre-screening Process

To be declared responsive, an OEM Offeror's Solution must:

a) comply with all the requirements of the Solicitation;

b) comply with the certifications and meet all the mandatory technical evaluation criteria;

OEM Offeror's of Solutions not meeting a) and b) will be declared non-responsive and given no further consideration in the Solicitation process.

4.2.1 Ranking

Responsive OEM Solutions will be ranked in order of total score as determined by combining the scores from Part B - Written Rated Response (Table 3) and Interactive Virtual Session (Table 4).

INSERT:

4.3 Notification of Selection – Pre-Qualified Solutions

Canada will invite the eight (8) highest-ranking OEM Offerors of Pre-Qualified Solutions, that are compliant with the mandatory procedural requirements and the evaluation criteria described herein to make a demonstration, unless the following conditions are met:

- if 6 or less Pre-Qualified Solutions are responsive; or
- if 4 or more Pre-Qualified Solutions have achieved a total rated score of 44 points or more out of 63 available points.

If either of the conditions are met, Canada will proceed directly to the Proof of Concept. Before finalising the CBSOS Final - Pre-Qualified Solutions, Canada will remove the Demonstration Stage from the evaluation process found in CBSOS - Initial No.: CSS0924221B, Stage 6B: Demonstration - OEM. The four (4) highest-ranking Solution OEM responses will be notified (Notification of Selection) of Canada's intent to award Standing Offers for the Pre-Qualified Solutions - Proof of Concept.

For example:

- Scenario 1: If Canada only receives 3 responsive submissions, Canada will proceed directly to the Proof of Concept.

- Scenario 2: If Canada receives 7 responsive submissions, and 5 have a score above 44 points, Canada will proceed directly to Proof of Concept.
- Scenario 3: If Canada receives 10 responsive submissions, and only 3 have a score of 44 or more, then Canada will rank the Pre-Qualified Solutions based on their scores and the top eight ranking Pre-Qualified Solution OEMs will be invited to the Demonstration stage.

4.3.1 Tie Breaker

In the vent that Canada proceed directly to Proof of Concept, the four (4) highest-ranking responsive Pre-Qualified Solution will be recommended for Standing Offer award for the Proof of Concept, on the condition that, the second highest-ranking responsive Offer is not within (+/- 1%) of the highest-ranking responsive Offer. In the event that the second highest-ranking responsive Offer is within (+/- 1%) of the highest-ranking responsive Offer, these Offers will be ranked in descending order using the following steps.

- Step 1: The points obtained for Written Rated Criteria (Table 3) WR1: *On-Premise and Cloud-based CSS Deployment* will be used to rank the subsequent tied solution OEMs from the highest score to the lowest score.
- Step 2: The points obtained for the Written Rated Criteria (Table 3) *WR2: Deployment Readiness: CCCS Assessment Process* will be used to rank the subsequent tied Offers from the highest score to the lowest score.
- Step 3: The points obtained for the Written Rated Criteria (Table 3) *WR3: Security Readiness* will be used to rank the subsequent tied Offers from the highest score to the lowest score.
- Step 4: The points obtained for the Written Rated Criteria (Table 3) WR5: *Data Residency* will be used to rank the subsequent tied Offers from the highest score to the lowest score.

3. Amendment to add Annex A - Invitation to Pre-screening Solutions – Tables

Annex A - Invitation to Pre-screening Solutions – Tables

The OEMs must provide their written responses using Tables 1, 2 and 3 below with reference to the substantiating evidence as attachments, where applicable.

The written response must include the following:

- Response to Part A - Certifications and Mandatory Requirements: Tables 1, 2 and attachments (1 electronic copy in PDF format)
- Response to Part B - Written Rated Response and Interactive Virtual Session: Table 3 only and attachments (1 electronic copy in PDF format)

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, and 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: *SaaS is a software distribution model where the software is owned, hosted and managed remotely by a single provider. The provider delivers a software service based on one set of common code and data definitions that is consumed over the internet 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 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.			

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** (Appendix, Page and Paragraph references)
	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); 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);			

Mandatory Requirements	Self Assessment		Reference to Evidence Provided (Appendix, Page and Paragraph references)
	Met	Not Met	
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 OEM 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 (Appendix, Page and Paragraph references)
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	Points will be allocated as follows: The evidence of this capability is demonstrated = 3 points	

Rated Criteria	Point Allocation Max Score = 43 points Self-Score	Reference to Evidence Provided (Appendix, Page and Paragraph references)
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.	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 (Appendix, Page and Paragraph references)

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 any three of the following endpoint security products: a) McAfee b) Windows Defender c) Cisco AMP for Endpoints d) CrowdStrike Falcon e) Trend Micro f) SentinelOne g) Sophos	OEM to select and provide evidence for up to three of the seven products listed. For each of the three, 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 (Appendix, Page and Paragraph references)
The term “automate”, “automatically”, 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.		
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:**	

Rated Criteria	Point Allocation Max Score = 43 points Self-Score	Reference to Evidence Provided (Appendix, Page and Paragraph references)
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 120-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 4: Rated Criteria – Interactive Virtual Session

	Rated Criteria for the Interactive Virtual Session Points	Max Score = 20
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, including all hops through the internet from the user's endpoint to the destination. Points will be allocated as follows: • The evidence is demonstrated = 6 points • The evidence is partly demonstrated (not showing all hops and latency) = 3 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:	

	Rated Criteria for the Interactive Virtual Session Points	Max Score = 20
	• 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)** 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.	

	Rated Criteria for the Interactive Virtual Session Points	Max Score = 20
	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	

4. All Other Terms Remain Unchanged

All other terms set forth in the CBSOS shall remain unchanged and this Amendment No. 4 and the CBSOS shall be deemed a single integrated document for all purposes.