Attachment A - Statement of Challenge (partial)

(Note to Bidders: A finalized Statement of Challenge, Attachments and Annexes will be set out in the Final Challenge-Based Solicitation.)

Background

As outlined in the *Government of Canada Digital Operations Strategic Plan*, the Government of Canada (GC) is working to provide reliable networks and infrastructure while increasing network security by transitioning to a single, modern, end-to-end enterprise class network that users can access anytime and anywhere. The integrity and security of the GC's data and information technology (IT) infrastructure is essential to the delivery of services to Canadians. With the increasing sophistication and frequency of cyberattacks, the GC must remain vigilant and continue to strengthen the GC's defences. The government has implemented world-class monitoring services and defensive measures at its network perimeter through SSC-managed gateways; however, not all GC organizations benefit from these services.

Problem Statement

Canada lacks an enterprise cloud-based security solution that provides the ability to deliver a consistent user experience from any device, any location, at any time.

In certain cases, Canada lacks cost-effective consistent security controls to protect GC data and assets in GC department remote sites and for GC and non-GC remote users, including SDAs (small departments and agencies), when accessing the Internet, cloud-based SaaS, IaaS, and PaaS, and GC on-premise services. This results in lost productivity, high cost, lower user satisfaction and morale, increased cybersecurity risks, and inconsistent user experience.

Canada wishes to improve and optimize the ability to securely consume and deliver cloud-based services effectively, efficiently, and quickly, using a SaaS-based cloud security solution. This will support Canada's journey to Zero Trust, which balances Canada's requirements to maintain visibility and security of Canada's access to the Internet and Cloud, while improving network performance and user experience.

Challenges Specific to the Solution

The problems to be solved by the Cloud-based Security Services (CSS) can be summarized as follows:

- Inconsistent performance and user experience when accessing public cloud-based IaaS, SaaS and PaaS services.
- The use of direct access to the Internet in order to access the public cloud or GC on-premise services exposes the GC and departments to threats. This includes users at remote sites and home offices, and mobile users. These "perimeters" must be protected appropriately.

- High costs associated with backhauling internet-bound traffic to regional GC hubs via Multiprotocol Label Switching (MPLS) circuits. Costs typically include the MPLS circuit, the cost of the internet circuits at the SSC Enterprise Internet Service (EIS) regional hub locations for that traffic, as well as the augmentation of the security stack at existing regional hubs. With respect to direct internet access, providing a GC-approved security stack at each remote location that has direct internet access is also costly.

- Inconsistent perimeter security services at remote locations, within some SSC partner departments, as well as within Small Departments and Agencies.

Definitions

- **Able to** – Expression that refers to a functionality or a component of the solution that must be actionable by users.

- **Mobile User** – A travelling GC user with a laptop computer, that can work from any location, including, but not limited to, home, hotel, café, etc.

- **GC Remote Site** – A GC building or office space that is occupied by GC employees, consultants, or contractors.

- **CSS End-User Software** – Includes any CSS-related software, such as a CSS agent/client, browser extensions, etc., that is installed on an end-user's laptop or desktop computer.

- **CSS Agent** – CSS endpoint software application (agent or client) that is installed on an end-user's device.

- **Managed Device** – A laptop or desktop computer that is owned and managed by the GC. CSS end-user software can be installed on these devices at the discretion of the GC or a GC department. Managed devices will generally have a GC device certificate installed.

- **Non-GC Managed Device** – An external organization's (non-GC) laptop or desktop computer that is not owned or managed by the GC. The installation of any CSS end-user software on non-GC Managed devices is at the discretion of the non-GC organization that owns or manages the laptop or desktop computer. The GC may have influence over the installation of CSS end-user software on these devices. An example of a non-GC Managed device is a laptop owned and managed by a university research department that conducts business with the GC.

- **Bring Your Own Device (BYOD)** – A personal laptop or desktop computer that is owned and managed by an end-user. CSS end-user software may be installed on these devices at the discretion of the end-user. The GC will likely have no influence over the installation of CSS software on these devices, which should be considered to be agentless or clientless.

- **Internet of Things (IoT) and Scientific Device** – A computing device that is embedded with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems. A scientific device is often controlled by a user, with a greater level of interaction with a user than an IoT device. IoT and scientific devices may have limited or no ability to have CSS end-user software installed on them.

- **External User** – A user that is not under the employ of the GC in any capacity, but requires access to GC applications, data, or services. An example of an External User is a university researcher, under the employ of the university, that collaborates with a GC research organization.

- **Multi-tenancy** – A single instance of the software and its supporting infrastructure may serve multiple customers. Each customer shares the software application and also shares a single database. Each tenant's data is isolated and remains invisible to other tenants.

- **Software as a Service (SaaS)** – A SaaS solution is defined as 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.

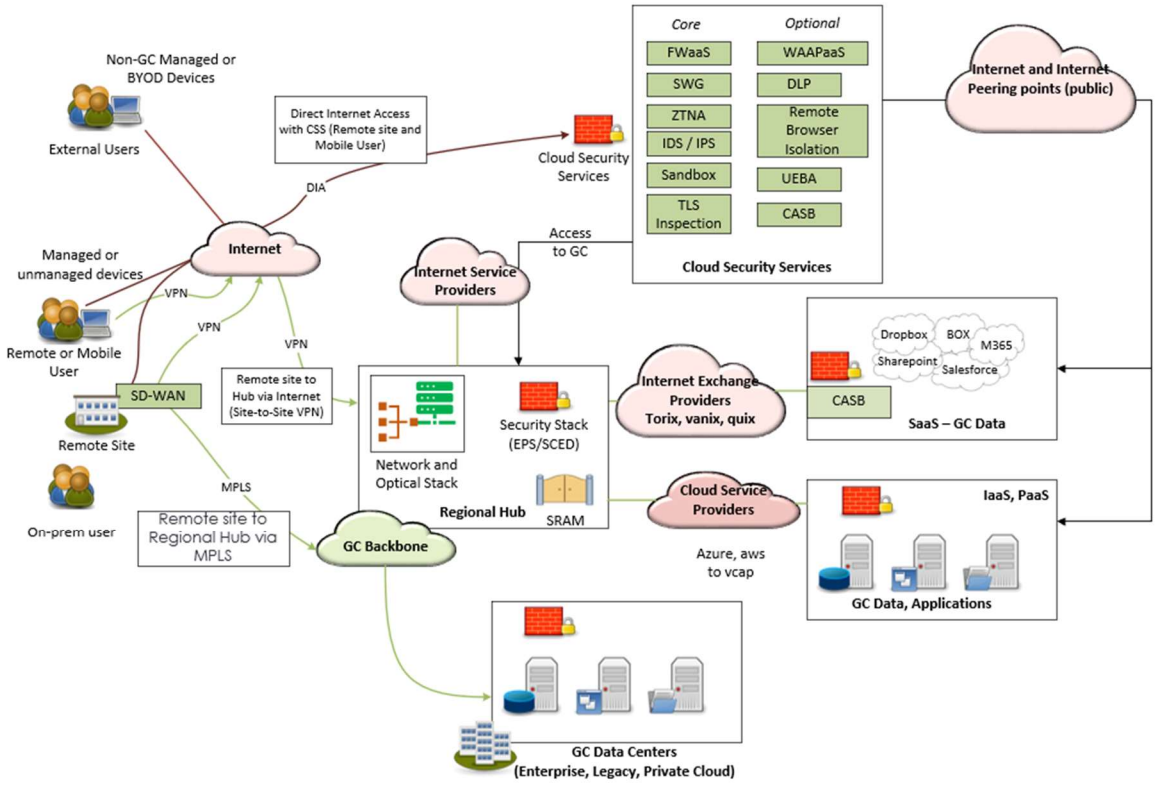
- **Vendor** – The Contractor that provides the solution under this contract.

- **Parent Organization** – A top-level organization that has control, visibility and access levels to all information throughout the subordinate organization and subordinate business units as well as its own.

- **Child Organization** – A subordinate organization that has control, visibility and access levels to only information throughout its own organizational business unit and subordinate business units and not to others.

Proposed High-Level Architecture

The following diagram illustrates the proposed high-level CSS architecture:



Uses Cases Based on Proposed High-Level Architecture

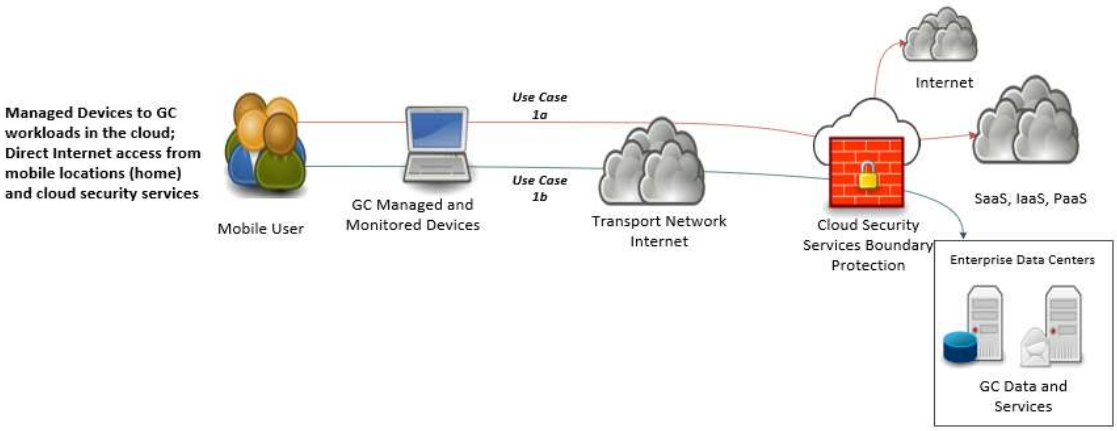
The following use cases constitute the operational environment in which SSC intends to take advantage of CSS.

1. **Use Case 1a: Mobile User (Managed Device) accessing Cloud-Based Services**

A GC mobile user with a Managed Device accesses cloud services outside of a GC office (e.g. at home, hotel, public internet connection). All user traffic flows through a secure encrypted tunnel from the user's endpoint to the CSS solution, then to the destination in the public cloud (e.g. general internet access, SaaS, IaaS, or PaaS).

Use Case 1b: Mobile User (Managed Device) accessing GC On-Premise (EDC) Services

A GC mobile user with a Managed Device accesses GC on-premise services outside of a GC office (e.g. home, hotel, public internet connection), protected by security services within the CSS solution. All user traffic flows through a secure encrypted tunnel from the user's endpoint to the CSS solution, then to the destination in a GC Enterprise Data Centre (EDC).

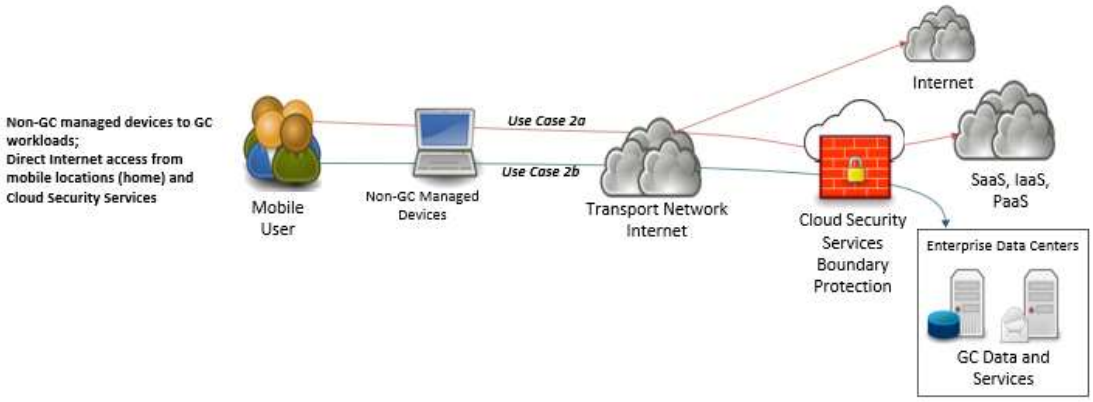


2. Use Case 2a: Mobile User (Non-GC Managed Device) accessing Cloud-Based Services

A GC mobile user with a non-GC Managed device accesses cloud services outside of a GC office (e.g. at home, hotel, using a public internet connection). Traffic to specific GC applications and services flows through a secure encrypted tunnel from the user's endpoint to the CSS solution, then to the destination in the public cloud (e.g. SaaS, IaaS, or PaaS). Access to applications or services that are not specifically identified (e.g. general internet browsing) will go directly to the Internet, bypassing the CSS.

Use Case 2b: Mobile User (Non-GC Managed Device) accessing GC On-Premise (EDC) Services

A GC mobile user with a non-GC Managed device accesses GC on-premise applications and services outside of a GC office (e.g. at home, hotel, using a public internet connection). Traffic to specific GC applications and services flows through a secure encrypted tunnel from the user's endpoint to the CSS solution, then to the destination within a GC EDC.



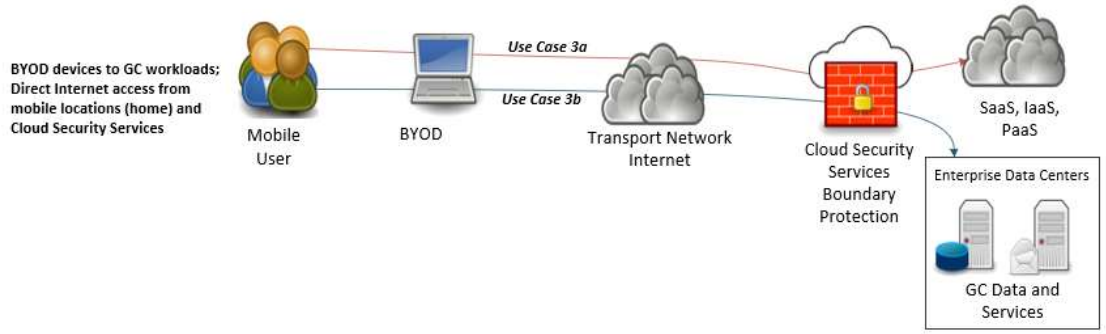
3. Use Case 3a: BYOD User accessing Cloud-Based Services

A GC mobile user with a BYOD device, with no ability to install any CSS software, accesses cloud-based services outside of a GC office (e.g. at home, hotel, using a public internet connection) protected by security services within the CSS solution. Traffic to specific GC applications and services flows through a secure encrypted tunnel from the user's endpoint to the CSS solution, then to the destination in the public cloud (e.g. SaaS, IaaS, or PaaS). Access to

applications or services that are not specifically identified (e.g. general internet browsing) will go directly to the Internet, bypassing the CSS.

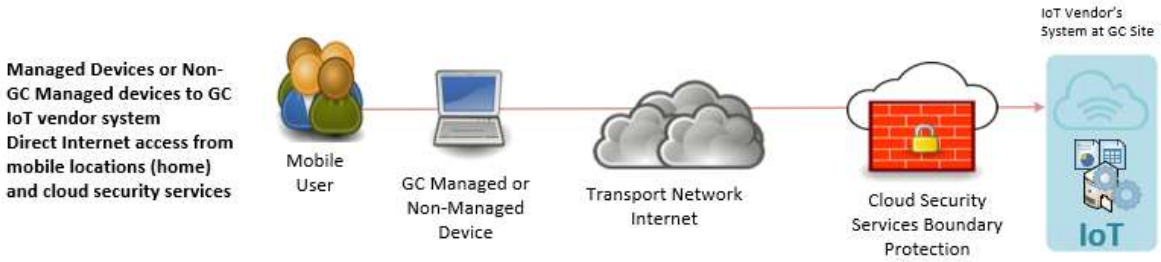
Use Case 3b: BYOD User accessing GC On-Premise (EDC) Services

A GC mobile user with a BYOD device, with no ability to install any CSS software, accesses GC on-premise services outside of a GC office (e.g. at home, hotel, using a public internet connection) protected by security services within the CSS solution. All user traffic flows through a secure encrypted tunnel from the user's endpoint to the CSS solution, then to the destination in a GC EDC.



4. Use Case 4a: User Access to IoT/Scientific Devices via the Internet

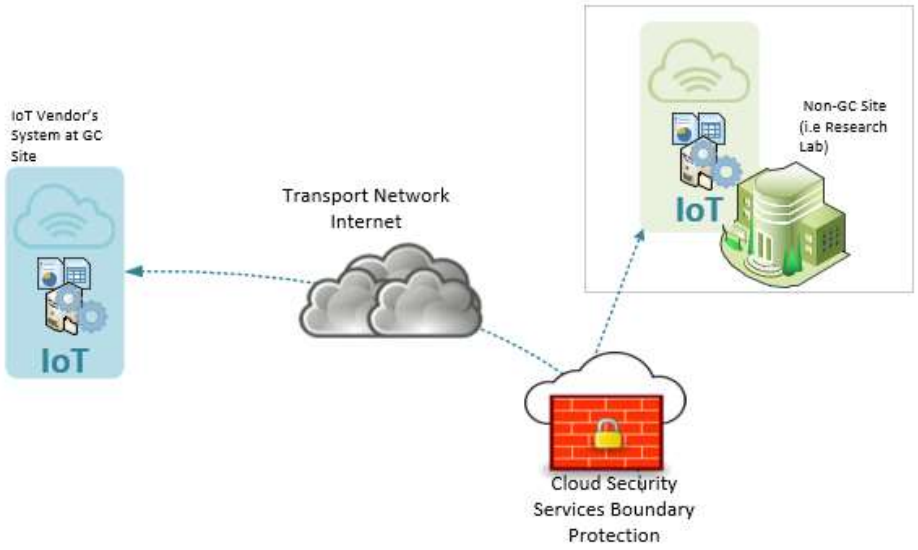
An IoT device, such as a sensor, robot, or other scientific device that resides within the GC, may need to be accessed or controlled by a GC user or External User via the Internet. Traffic would flow between the users' devices and the IoT or scientific device via the CSS.



Use Case 4b: IoT/Scientific Devices access other IoT/Scientific Devices or systems via the Internet

An IoT device, such as a sensor, robot, or other scientific device that resides within the GC, may need to communicate with other IoT devices or systems that reside outside of the GC (such as to a non-GC research lab, or to an IoT vendor's system) via the Internet. Traffic would flow between the IoT or scientific devices and systems via the CSS.

Access to and between the devices would be permitted or denied by the CSS.

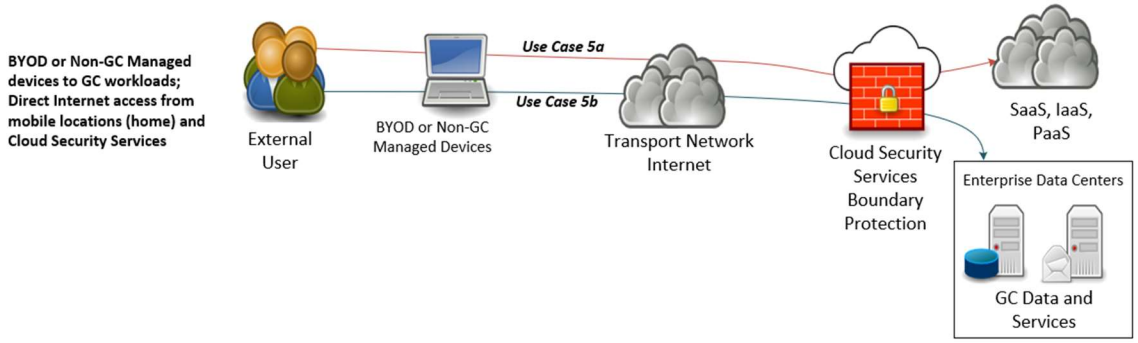


5. Use Case 5a: External User using a Non-GC Managed or BYOD Device accessing GC Cloud Services

External User using a non-GC Managed or BYOD device accesses GC cloud-based (e.g. SaaS, IaaS, PaaS) applications, data or services from outside of the GC. Access would be permitted or denied by the CSS.

Use Case 5b: External User using a Non-GC Managed or BYOD Device accessing GC On-Premise (EDC) Services

External User using a non-GC Managed or BYOD device accesses GC on-premise applications, data or services in a GC EDC from outside of the GC. Access would be permitted or denied by the CSS.

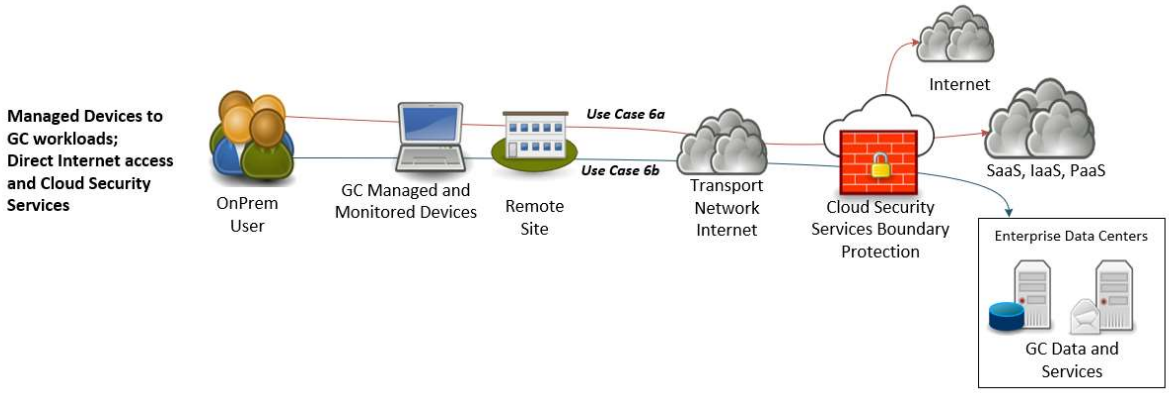


6. Use Case 6a: User (Managed Device) at a remote GC site accessing Cloud-Based Services

GC user with a Managed device accesses cloud services via a GC remote site's direct internet breakout, protected by security services within the CSS solution. All user traffic flows through a secure encrypted tunnel to the CSS solution.

Use Case 6b: User (Managed Device) at a remote GC site accessing GC On-Premise (EDC) Services

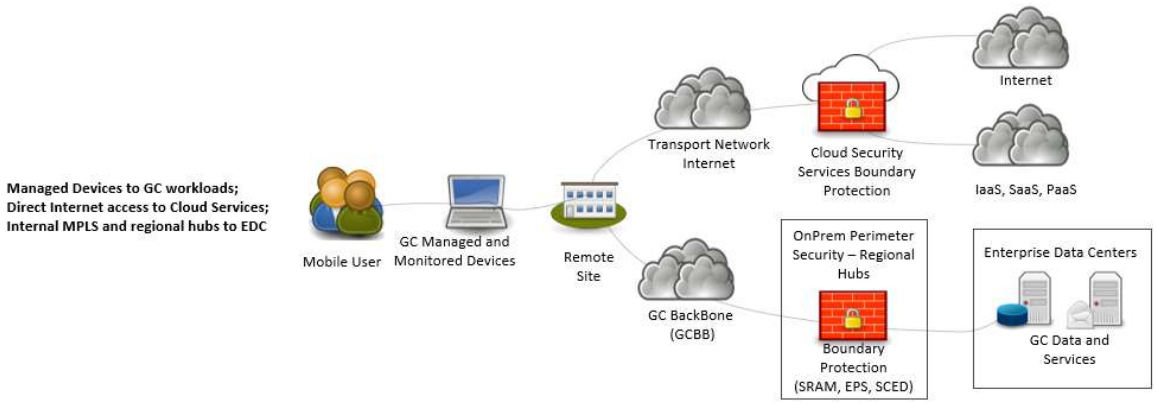
GC user with a Managed device accesses on-premise GC services located in a GC EDC via a GC remote site's direct internet breakout, protected by security services within the CSS solution. All user traffic flows through a secure encrypted tunnel to the CSS solution.



7. **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**

A user with a Managed device at a remote GC site accesses cloud-based services via the site's direct Internet connection. Select user traffic flows through a secure encrypted tunnel from the user to the CSS solution, then to the destination in the public cloud (e.g. general internet access, SaaS, IaaS, PaaS).

The user also accesses GC On-Premise (EDC) services via a GC Backbone (GCBB) MPLS circuit between the remote GC building and a regional hub. All traffic between the GC On-Premise (EDC) services and the user flows through the regional hub.



Mandatory Minimum Viable Requirements

The sections below describe the expected minimum capabilities of the Solution. It describes:

- the functional requirements: what the solution must do (all the time) and must be able to do when prompted; and
- the non-functional requirements: how the solution must interact with the environment and other devices.

1. Capabilities (CAP):

CAP1: The solution must provide access to the general internet, IaaS, PaaS, and SaaS cloud-based services to approved mobile users who are connecting via a direct internet connection using:

a) a GC Managed device;
b) a non-GC Managed device.

CAP2: The solution must provide access to IaaS, PaaS, and SaaS cloud-based services to approved mobile users who are connecting via a direct internet connection using a BYOD device.

CAP3: The solution must provide access to web-based, on-premise GC applications, data and services to users who are connecting via a direct internet connection using a BYOD device.

CAP4: The solution must provide access to the general internet, IaaS, PaaS, and SaaS cloud-based services to authorized users located at GC remote sites who use a direct public internet connection from a GC Managed device.

CAP5: The solution must provide access to on-premise GC applications, data, and services to authorized users located at GC remote sites who use a direct public internet connection from a GC Managed device.

CAP6: The solution must allow authorized administrators to be able to configure user, group, and device access policies used to:

a) permit or deny user, group, and device access to services, regardless of where the service resides, based on access policies configured by the GC, and individual GC departments and agencies;
b) limit access to services, regardless of where the services reside, to those services that have been explicitly permitted, as defined within access policies created by the GC and individual GC departments and agencies; and
c) deny any access and visibility to all services that a user, group, or device is not explicitly permitted to access.

CAP7: The solution must provide the following User Experience capabilities for GC Managed and Non-GC Managed devices:

a) continuous performance monitoring of a user's experience;
b) provide a user experience score over time, where the score is used to identify the level of the user experience (e.g. poor, acceptable, high user experience), and user experience trends;
c) provide user experience reports;
d) alert administrators when a user's experience score drops below a predefined threshold; and
e) allow administrators to determine where and why a user is experiencing poor performance.

CAP8: The solution must be able to automatically disable the CSS agent when a user is at a GC physical office.

CAP9: The solution must be able to prevent end users from logging out or disabling the CSS agent, to prevent bypassing the solution.

CAP10: The solution must allow authorized administrators to select which CSS regional data centre location user traffic is forwarded to.

CAP11: The solution must provide access to on-premise GC applications, data, and services, where overlapping or duplicate IP addresses exist.

CAP12: The solution must allow access to trusted applications directly, as identified by Canada, bypassing the CSS.

CAP13: The CSS solution must not require the use of more than one CSS agent on any end-user device.

CAP14: The solution must provide access to GC on-premise IoT and scientific devices to External Users.

CAP15: The solution must provide access for GC on-premise IoT and scientific devices to communicate and transmit data to other non-GC IoT and scientific devices and systems, located outside of the GC (e.g. OEM IoT systems, external research labs).

CAP16: The solution must support Network Address Translation (NAT).

2. Security (SEC):

SEC1: The solution must encrypt all data in transit while:

a) enforcing secure connections to the Cloud Services, by providing data-in-transit protection between Canada and the Cloud Service using TLS 1.2, or subsequent versions;
b) using up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in CSE's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securelyconfiguring-network-protocols-itsp40062) and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-andprotected-b-information-itsp40111);
c) using a minimum of 256-bit ECDSA key length; and
d) using a minimum of 2048-bit RSA key length.

SEC2: The solution must be able to use GC PKI keys issued by a GC Certificate Authority to protect access to GC hosted applications, data and services.

SEC3: The solution must authenticate users using the following web authentication methods:

a) federation using Security Assertion Markup Language (SAML) 2.0, where the End User credentials and authentication to cloud services are in an Identity Provider (IdP) that is under the sole control of Canada; and
b) the GC's implementation of ADFS using the SAML 2.0 protocol.

3. Security Capabilities (SCAP):

SCAP1: The solution must provide the following cloud-based perimeter security services:

a) a Layer 4-7 firewall that permits or denies access based on IP addresses, ports, protocols, application, identity, groups, and locations (i.e. Next Generation Firewall (NGFW));
b) filter unwanted software/malware from user-initiated internet traffic, enforce policy compliance for web traffic, and prevent access to unacceptable/illegal web sites and web sites known to contain malicious threats or viruses (i.e. Secure Web Gateway (SWG));

c) analyze the decrypted and normal traffic for intrusion attempts, and block intrusions (i.e. 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 (i.e. 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 (i.e. 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 ATD (i.e. SSH Inspection)

SCAP2: The solution must be able to automatically block all files that have been identified as malicious across all tenants.

SCA3: The solution must allow files that have been identified as malicious to be quarantined and made available to the GC for further investigation.

SCAP4: The solution must recognize and be able to control web applications regardless of port and protocol.

SCAP5: The solution must be able to identify the operating system and browser agent of the user, and trace activities back to individual users.

SCAP6: The solution must track and log administrative changes. The change logs must:

a) include the time, date, administrator username and change details;
b) be stored securely; and
c) be protected to ensure, and prove, that they have not been altered or tampered with (i.e. non-repudiation).

SCAP7: The solution must transmit logs to multiple GC SIEM systems.

SCAP8: The solution must provide security device posture assessments for GC Managed and Non-GC Managed devices as a means to permit or deny access privileges to applications, data and services.

4. <u>Authentication (AUTH):</u>

AUTH1: The solution must be able to authenticate using the following GC authentication methods:

a) authenticate devices using GC issued device certificates;
b) perform authentication and authorization for users stored in GC directories accessible over LDAPS;
c) authorize users via a combination of user groups and user attributes; and
d) authenticate devices and users supporting SSO.

AUTH2: The solution must be able to apply the following Multi-Factor Authentication (MFA) methods:

a) multi-factor OTP device;
b) soft token on portable device;
c) multi-factor push notification to mobile device;
d) GC PKI user certificate; and
e) smart cards.

AUTH3: The solution must be able to force CSS administrators to use a GC-provided two-factor authentication (2FA) solution.

6. Connectivity (CON):

CON1: The solution must ensure a high-quality user experience to cloud services by:

a) peering directly with cloud service providers and internet exchange providers; or
b) leveraging the networking of the underlying cloud service providers that host the CSS solution.

7. Interoperability (IOP):

IOP1: The solution must function on the following operating systems:

a) Microsoft supported Windows OS family;
b) Apple supported macOS and iOS family;
c) Google supported Android OS; and
d) Commercially and community supported Linux OS.

IOP2: The solution must support web-based access from the following web browsers: Apple Safari, Microsoft Edge, Google Chrome, and Mozilla Firefox.

8. Integration (INT):

INT1: The solution must integrate with GC SOAR solutions, using Representational State Transfer (REST).

INT2a: The solution must function with a another vendor's CASB agent installed on an end-user's device.

INT 2b: The solution's CASB agent and the other vendor CASB agent must function together and direct traffic as defined by Canada.

INT3a: The solution must function with a different vendor's VPN agent installed on an end-user's device.

INT3b: The solution's agent and the other vendor VPN agent must function together and direct traffic as defined by Canada.

INT4: The solution must apply the following Zero Trust approaches:

a) continuous evaluation and authorization of user identity and access requests;
b) enforcement of policy based on user profiles retrieved from one or more GC identity repositories; and
c) users are granted access to apps, data and services based on identity, geolocation, device authentication and posture assessment, and other user and device contextual inputs.

9. Management (MGMT):

MGMT1: The solution must be able to provide multi-tenancy, allowing GC administrators from different organizations to manage, generate customized reports and administer specific portions of the solution within their authorized domain.

MGMT2: The solution must be able to apply granular Role-Based Access Control (RBAC) to administrative users.

MGMT3: The solution must provide multi-tenant operator organizations through hierarchical RBAC in which the top-level organizations (Parent) have full visibility and control over all subordinate (Child) organizations and policies.

MGMT4: The solution must allow the GC to implement global policies that apply to tenants that cannot be changed or deleted by Child organization administrators.

MGMT5: The solution must restrict the ability of Child organizations to affect the policy or behaviour of the solution for any other organization, including the Parent Organization.

MGMT6: The solution must be able to:

a) generate customized role-based ad hoc reports; and
b) send tenant-specific logs to the tenant department.

10. Deployment and Operating Environment (ENV):

ENV1: The solution must be able to be deployable in a configuration that ensures that device endpoints are able to connect to the solution during an equipment or site failure.

ENV2: The solution must scale to a minimum of 100,000 concurrent users.

Non-Compulsory Requirements

Non-Compulsory Use Case: Server-to-Server connections in a Cloud IaaS environment

A GC workload on a server in one IaaS environment (i.e. AWS, Azure, GCP) connects to another GC workload/server in a different IaaS environment, protected by security services within the CSS solution. Access to these services is based on policies.

NCR1: The solution must provide the following type of secure access between servers in a cloud IaaS environment:

a) server-to-server communications between cloud IaaS providers, such as between AWS and Azure; and
b) inter-region server-to-server communications within a single cloud service provider, for example, between a server in Region 1, and a server in Region 2.

NCR2: Support for International Users – The solution must connect GC users and External Users physically located outside of Canada directly to CSS data centres located within Canada and to GC-approved CSS data centres located outside of Canada.

NCR3: Cloud Security Posture Management (CSPM) – The solution must have a native CSPM capability that:

a) monitors, assesses, and evaluates security compliance and regulatory violations in IaaS and PaaS environments;
b) notifies administrators and provides reporting of security policy non-compliance, misconfigurations, and regulatory violation; and
c) automates the remediation of identified security policy non-compliance, misconfigurations, and regulatory violations.

NCR4: SaaS Security Posture Management (SSPM) – The solution must have a native SSPM capability that monitors and detects settings that introduce security risks in the SaaS environment, provides alerts for misconfigurations, and either automates or provides guided remediation to resolve the risks.

NCR5a: Remote Browser Isolation (RBI) – The solution must have 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.

NCR5b: The solution's native RBI capability must be hosted in the CSS OEM's cloud environment.

NCR5c: The solution's native RBI capability must protect user computers from web-based threats by containing the threats to the isolated environment.

NCR5d: The solution's native RBI capability must permit and deny:

a) file uploads;
b) file downloads;

c) screen captures; and
d) copy and pasting of any information being displayed.

NCR6: Native Cloud Access Security Broker (CASB) – The solution must have a native, integrated CASB capability that includes, at minimum: Data Loss Prevention (DLP), User and Entity Behaviour Analytics (UEBA), regulatory and policy compliance, and threat detection.

NCR7: SD-WAN – The solution must have a native, integrated SD-WAN capability.

NCR8: Auto-Application Discovery – The solution must automatically discover and identify applications that are being accessed by CSS users or devices, allowing CSS administrators to easily apply user access policies to these applications.

NCR9: User and Entity Behaviour Analytics (UEBA) – The solution must detect and provide alerts on suspicious user and device behaviour.

NCR10: The solution must provide automated actions to block potential threats based on behaviour that has been identified as a potential risk or threat. For example, if suspicious user behaviour is detected, the solution automatically denies access, quarantines the user or device, and reports the suspicious behaviour to an administrator.

NCR11: Endpoint Security Integration – The solution must be able to integrate with GC-supported endpoint security software such as McAfee, Windows Defender, and Cisco AMP for Endpoints to:

a) automate the responses to threats that have been identified by the Endpoint Security solution; and
b) provide threat information that has been identified by the CSS solution to the endpoint security solution, such that the endpoint security solution can automate a response to the identified threat.

NCR12: GC On-premise CSS Deployment – The solution must provide the option of deploying an instance of the CSS solution in a GC data centre. A single instance of the centralized cloud CSS management platform must manage both the on-premise CSS deployment and the cloud-based CSS environment.

NCR13: The solution must have direct peering with internet exchange providers at a minimum of 100Gbps.

NCR14: The solution must be able to authenticate and authorize with Open Authorization version 2 with OpenID (OAuth 2.0).

NCR15: The solution must provide secure access to non-web-based, on-premise GC applications, data and services for mobile users who are using a BYOD via RDP, SSH, and remote file system mounting (e.g. SMB).

NCR16: The solution must provide call quality information and reporting for Microsoft Teams calls, including network analytics (e.g. latency).

NCR17: The solution must differentiate between GC-approved, non-GC-approved and personal versions of public cloud-based applications and be capable of making access policy decisions associated with a user based on the device they are using. For example, on a Managed GC device, corporate cloud applications will be allowed but personal versions should be blocked.

NCR18: The solution must perform Data Loss Prevention (DLP) functions that include, at minimum:

a) pre-built Industry compliance policies (Canada PII, PCI-DSS);
b) built-in Canadian specific data identifiers (Health Card, Driver's Licence);
c) custom data identifiers;
d) regular expression (RegEx) support;
e) custom patterns and exact data matching;
f) ability to create custom DLP rules and profiles;

g) inspect within zip files;
h) inspect hidden fields; and
i) detect encrypted files.

NCR19: The solution must have Web Application and API Protection as a Service (WAAPaaS) capabilities.

NCR20: The solution must integrate with GC SOAR solutions using Extensible Markup Language (XML).

NCR21: The solution must provide the following User Experience capabilities for GC Managed and Non-GC Managed devices:

a) provide latency measurements on a hop-by-hop basis, showing the latency of all hops, from the user's endpoint to the destination;
b) determine destination public and private application availability, and response time to help determine if the application is responsible for poor user experience; and
c) include performance metrics for the end user's device, including CPU, memory, and Wi-Fi statistics.

NCR22: The solution must provide access for GC IoT and scientific devices located outside of a GC site to communicate and transmit data to other IoT and scientific devices and systems located outside of a GC site (e.g. OEM IoT systems to external research labs).

NCR23: The solution must perform authentication and authorization for users using an identity repository located within the CSS solution populated externally from GC authoritative sources.

NCR24: The solution must authenticate and authorize the end user's device prior to permitting access to applications, data, and services.

NCR25: The solution must scale to a minimum of 400,000 concurrent users.

NCR26: The solution must be able to implement a GC virtual network-based sensor to capture selective GC data, and send the captured data to GC sites for further analysis.

Personas

Persona Name

Dr. Abigail
Non GC users that need to access GC data (ie. educational institutions)

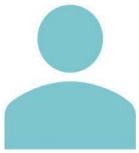
Demographics: Science

- Researcher at a university (could be an SME)
- Could be working on a masters or PhD or has a PhD

Goals • Scientists that need to access HPC to run algorithms • Easy and fast transfer of large quantities of data on and off the cluster – ie. Terabytes – the faster they are the more productive they will be • Easily access specific sites - Compute Canada or federated research data repository (FRDR) or other sites • Typically not real time traffic • Some could use streaming of traffic • Ability to have access on the fly (ie within 24 hours or less) • Provide access to and control of equipment (ie robots in the government labs) – still large amounts of data like high definition video or non-human / IoT/ Science devices (sensors streaming data in (automation needs to get data back into the facility to be analyzed)	**Challenges** • Some people using Linux environment – need to support multiple operating systems • Security tools – can reduce speed • Poor user experience, high latency • Security policies - How do we do identity management and how we do authentication • Users / scientists can't install software onto their computers • Not all types of access are at web browser or API driven • Access from outside Canada (global access requirement)
Values • Connection is simple (two factor authentication is sometimes pushed back on) • How they access will be similar to other systems they're familiar with	**Fears** • Extra hops – that may manipulate traffic and could slow it down • Fear of losing access - reliability and outages • Some research deals with sensitive data
Expectations • Once access is granted if performance is ok than they are ok • Once system is operational then how permissions are granted is done by researchers (within their department's control) – ie role based access and only permission will be given to which systems and whom (RBAC) • You get access to what you have access to and permissions to projects you have access to but not everything • 24 hour turn around – onboarding and offboarding collaborators • Look and feel is similar to what they're used to • Need High Availability • Ticketing system to support external users – support model for scientists for quick resolution (ITSM)	**Measures of Success** 1. Have fast and flexible connectivity for moving data (speed) 2. User experience – as seamless and with as few steps as possible 3. User logs once and they go through to what they need to access (only login once) – simplicity of use • Without installing new software • Failover

Persona Name

Penelope



ISO/SOC

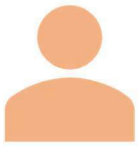
Demographics:

- CS2 to CS4 both ISO and SOC

Goals • Ensure love and care of technology and infrastructure of the cloud solutions is taken care of • Incident response – augment incident response capabilities • Access management (ensure the right people have the right privileges)	**Challenges** • Staff to manage solution • Data quality – not getting adequate logging data • Data volume – data increases and collision of data if its not tagged properly • Getting the right people to do the work – hard to get SOC bilingual people – reskilling resources and training
Values • Having better visibility • Dealing with the disparate internet connections (not being monitored / insecure) • Better security	**Fears** • Would be duplicating other services that may be able to provide a different flavour of solution comparable to CBSS • By multiple options it creates more complexity and therefore more risk is introduced • How can we guarantee integrity of the services (so that they haven't been tampered with) – we don't manage the security control and how it will change over time and vulnerability management • Partners go around SSC to take control of their domain – will there be guard rails in place to prevent mistakes
Expectations • Would be nice to have a centralized place to manage tenants – to be able to access all tenants, like cyber events – if something needs to be replaced everywhere how fast can we reach them? (SSC, CRA, etc tenants) - Centralized cartography – observability • Global policy may impact every partner and specific policy for departments (parent/child multitenancy) • Integration with other security services for monitoring, observability, visibility • Pre-massage and prepare data to help with data quality and volume issues (so when data is corelated it makes sense) • Maintain / track source IP address • Ability to copy or apply settings to all tenants • Well architected RACI if this is a federated model – accountability of change needs to be in place • Solid change management (from baseline of global policy) • Availability of 99.999 and 7/24	**Measures of Success** 1. Have observability of entire infrastructure 2. Useful information – integration, easily available - actionable telemetry (not creating more work) – solution tells us where to look 3. Reduced effort to triage incidents 4. Increase security posture – ie. split tunneling may expose some part of the infrastructure – ie. when traffic not through VPN • Preserve log data *(integrity of logs, all logs are sent, and logs aren't lost)* • Properly architected – RBAC inclusion of two factor authentication • Ease of use – GUI and no need to engage professional services, no need to script • Global application of tenancy • Meet language and accessibility requirements

• A way to monitor health of environment – or access to staff that can help issues like performance and reliability	

Persona Name - Sierra



Department and SDA tenant admins

Demographics:

- RE5 to 6, CS4

Goals • Access to logs end to end – real time sharing of information (to mitigate incident) including SSC portions • IoT (non-human devices) – ie. camera with a 4G card uploading – any time, any place and any device – we want to protect and authenticate these devices • Integrating with partners, AD and PKI • Ease of use	**Challenges** • With security events, if some are managed by SSC it is hard to see and identify what has happened • What is in place for data residencies (does data stay in Canada?) • Decrypting data • Having enhanced reliability for data • TD5 threat profile – have additional security measures
Values	**Fears** • Poor performance (user experience) • Without clear RACI – there could be finger pointing – have everyone accountable for their portions (internal to government)

Expectations	Measures of Success
• Integration with existing security controls - Perimeter security infrastructure would work with CBSS • Flexibility to be able to tailor based on department needs – every department gets its own tenancy • Departmental admins would manage the department (ie. department maintains their own) • Global policy across all tenants • KPIs and reporting – executive reports – to showcase the security level to partners based on evidence and prove the information is secure, trends – to have their minds at ease that incidents were responded to quickly • For those with minimal IT teams, have more automation or machine learning to reduce management of system – as much as possible	1. Make us more secure 2. Automated action to mitigate the impact of incident 3. User experience – end user doesn't know it exists; they can just connect to what they need to connect to – don't need to worry about complexity of the network infrastructure • AI for unforeseen intrusion and malware • Uptime – no downtime • No latency – speed of accessing information from end user perspective • From operational /admin perspective have automated – no additional resources – don't want another system to support with same number of resources

Persona Name - Isabelle

GC Employees / Contractors – accessing remotely

Demographics:

- Everyone working remotely full time
- Located across Canada
- Significant increased use of cloud based services – due to remotely working and Government of Canada increasing cloud based services
- Accessing collaboration tools, office tools, corporate tools and government specific corporate and office tools
- Departmental specific applications on premises and in the cloud
- Accessing internal Government of Canada applications and cloud based
- Accessing mostly 9 am to 5 pm in their time zone

Goals	Challenges
• Accessing applications (and do it quickly) • Have application responsiveness (not wait 20 seconds after click) • Not have to go through unnecessary steps (ie no additional verification) • Common look and feel – do it the same way they do it in the office • Do our work and accomplish tasks without network/connectivity in the way – transparent/invisible • Privacy and confidentiality	• Capacity (of applications and network) to handle remote work • Can't have 12 people with their video turned on • Performance when accessing applications and their responsiveness (not as fast as in the office) • Particular application access may be difficult (ie. ESDC and others with more self-imposed policies)

Values • Privacy and security as an employee are maintained • Being able to do their job • Speed / responsiveness of applications that need to be access • Productivity (and ability to do job)	**Fears** • Congestion (too many people trying to get on the network at the same time) • Waking up to another lockdown – with a kids and everyone on the network at the same time,…. • Technical issues while working remotely, new solution or new process they have to follow (can't turn to person next to me for help or have someone come and help – and if it impacts collaboration tools, can't ask for anyone's help – leads to isolation) • Losing our work (networked applications don't save, network timeout, things crash) • Losing productivity and not being able to access what they need (and missing timelines)
Expectations • Single sign on • Remote access solution actually works • Invisible – connecting easily without many steps • Connecting on any device we have (ie things like email, Teams,…) • Support when it breaks (it just doesn't work, and don't know why) • More rapid adoption of new services • Quick internet browsing / access	**Measures of Success** 1. Quick response from applications being accessed 2. No disconnects / interruptions in the service 3. Ease of use – don't avoid using it – don't hate the service • Access what is needed, when it is needed • Low number of issues • Connection is simple and few (or one) steps

Attachment A1 - Cloud Security Requirements

Cloud Computing - Security Requirements

(Note to Offerors: in addition to the security requirements outlined in the section entitled Security Requirements, (CBSOS 1.9), a finalized Attachment A1 – Cloud Security Requirements will be set out in the Final Challenge-Based Standing Offer Solicitation.)

The Offeror must demonstrate compliance with the security requirements selected in the Canadian Centre for Cyber Security (CCCS) Annex B Cloud Control Profile – Medium of the Guidance on Security Categorization of Cloud-Based Services (ITSP.50.103) (https://www.cyber.gc.ca/en/guidance/guidance-security-categorization-cloud-based-services-itsp50103) for the scope of the Cloud Computing services provided by the Offeror.

The Offeror must ensure that Canada's Data, Offeror infrastructure (including any IaaS, PaaS or SaaS service provided to Canada) and service locations are secured with appropriate security measures that comply with the requirements set forth in the following certifications and audit reports by providing independent third-party assessment reports or certifications that addresses each service layer (e.g., IaaS, PaaS, SaaS) within the Cloud Computing services offered, including:

- ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Certification achieved by an accredited certification body; and
- ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for Cloud Computing services achieved by an accredited certification body;
- 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; and
- 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.

Each certification or audit report provided must:

- identify the legal business name of the Offeror or applicable Sub-processor;
- identify the Offeror's or Sub-processor's certification date and the status of that certification;
- identify the services included within the scope of the certification report. If there are any exclusions identified, or there is a need to separate a subservice organization such as data centre hosting, the subservice organization's assessment report must be provided.

Each audit will result in the generation of an audit report which must be made available to Canada. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Offeror must promptly remediate issues raised in any audit report to the satisfaction of the auditor.

Each SOC 2 Type II audit report must have been performed within the 12 months prior to ["the date of Solicitation/Offer Closing" or "the date of Contract/Standing Offer award" or "prior to Canada exercisingOption 1 - Deployment" or "prior to Work Segment 2 - Deployment"]. A bridge letter may be provided todemonstrate that the Contractor is in process of renewal where there is a gap between the service organization's report date and the user organization's year-end (i.e., calendar or fiscal year-end).

Cloud Computing - Security Assessment

Compliance will be assessed and validated through the Canadian Centre for Cyber Security (CCCS) CloudService 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), "centralized" or compliance will be assessed and validated through a local assessment departmental process "localized" with the support of the CCCS.

The Offeror must demonstrate that they participated in the process by successfully on-boarded, participated in, and completed the program. This includes providing the following documentation:

(i) a copy of the confirmation letter that confirms that they have on-boarded into the program;

(ii) a copy of the most recent completed assessment report provided by CCCS; and

(iii) a copy of the most recent summary report provided by CCCS.

The Offeror should contact the CCCS Client Services (https://cyber.gc.ca/en/) for any additionalinformation related to the CSP IT Assessment Program (centralized assessments).

It is the continuous obligation of the Offeror of the Cloud Computing services to notify CCCS (centralizedAssessments) or the department (localized assessments) when there are significant changes to its delivery of the IT Security services supporting the Offeror's Services and/or Work.

Security and Privacy Obligations

All terms set forth in the attached Schedule 1 - Security Obligations for Tier 2 (up to and including Protected B) SaaS, and the attached Schedule 2 - Privacy Obligations (unless otherwise specified herein) are incorporated by reference herein and shall be deemed to have the same force and effect as if set forth in full herein.