Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St.,/11, rue Laurier
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

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

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

Comments - Commentaires

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

Issuing Office - Bureau de distribution
Shared Systems Division (XL)/Division des systèmes partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Title - Sujet National Cybercrime Solution Projec Solution nationale en matière de cybercriminalité	
Solicitation No. - N° de l'invitation M7594-205915/D	**Amendment No. - N° modif.** 003
Client Reference No. - N° de référence du client M7594-205915	**Date** 2021-05-10
GETS Reference No. - N° de référence de SEAG PW-$$XL-155-39352	
File No. - N° de dossier 155xl.M7594-205915	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-06-22 Heure Avancée de l'Est HAE

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à: Labossière, Jean-Claude	**Buyer Id - Id de l'acheteur** 155xl
Telephone No. - N° de téléphone (613) 858-7359 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**

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

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Canada

This Solicitation Amendment #003 is raised to:

1. Update Annex A – Statement of Work, Section 3.20, Web Content Accessibility Guidelines (WCAG), paragraph a)
2. Update Annex A – Statement of Work, Section 5.0, System Security Plan, paragraph 5.8
3. Post Questions and Answers

The Solicitation is amended as follows:

1. **Annex A – Statement of Work - Section 3.20 – Web Content Accessibility Guidelines (WCAG), paragraph a) is hereby DELETED in its entirety and REPLACED by the following;**

Web Content Accessibility Guidelines (WCAG)

a) The Solution must comply with the WCAG 2.0[1] level A and Government of Canada's Standard on Web Accessibility[2] as follows:

i) The Solution must be accessible using assistive technologies and various Web browsers, such as Internet Explorer, Firefox, Chrome, Safari and Edge.

ii) Information, structure, and relationships conveyed through presentation must be programmatically determined or are available in text.

iii) When the sequence in which content is presented affects its meaning, a correct reading sequence must be programmatically determined.

iv) All functionality of the content must be operable through a keyboard interface without requiring specific timings for individual keystrokes, except where the underlying function requires input that depends on the path of the User's movement and not just the endpoints.

v) If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface, and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the User is advised of the method for moving focus away.

vi) A mechanism must be available to bypass blocks of content that are repeated on multiple Web pages.

---

[1] https://www.w3.org/TR/WCAG20/

[2] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601

vii) When any user interface component receives focus, it must not initiate a change of context.

viii) Changing the setting of any user interface component must not automatically cause a change of context unless the User has been advised of the behavior before using the component.

ix) In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements must not contain duplicate attributes, and any IDs must be unique, except where the specifications allow these features.

x) For all user interface components (including but not limited to: form elements, links and components generated by scripts), the name and role must be programmatically determined; states, properties, and values that can be set by the User must be programmatically set; and notification of changes to these items must be available to User agents, including assistive technologies.

xi) Content must not restrict its view and operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential.

xii) Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages must occur in the same relative order each time they are repeated, unless a change is initiated by the User.

xiii) Components that have the same functionality within a set of Web pages must be identified consistently.

xiv) Any keyboard operable user interface must have a mode of operation where the keyboard focus indicator is visible.

2.0 Annex A – Statement of Work - Section 5.0 – System Security Plan, paragraph 5.8 is hereby DELETED in its entirety and REPLACED by the following;

5.0 **System Security Plan**

a) The Contractor must review and respond to all security requirements in Appendix E – Security Requirements Traceability Matrix (SRTM) with a proposed mechanism to address the requirement. In the event of any conflict between requirements in the entire RFP and the SRTM, the SRTM will take precedence.

b) The Contractor must address any risks identified by Canada's compliance processes such as audits, Security Assessment and Authorization (SA&A) Activities, Threat and Risks Assessments (TRAs), and Privacy Impact Assessments (PIAs).

c) The Contractor must allow Canada or its designees, at no cost to Canada to access the Contractors development and test environments within the RCMP Protected B Cloud Tenant to inspect and audit the Contractor's compliance with the privacy, security and information management requirements under the Contract and to have full access to all Personal Information and Records.

d) The Solution must allow Canada to install passive network tap(s), to enable a full sustained network capture of all Internet Protocol (IP) Layer network traffic and interactions between components within the NCS with the ability to inspect within encrypted traffic.

e) The Contractor must co operate with any security audits or inspections requested by Canada by providing the following evidence:

i) Data flow documentation, data protection description, data architecture and security descriptions as they pertain to work under the Contract;

ii) The Contractor's own PIAs, risk assessments, and risk treatment plans as they pertain to work under the Contract; and

iii) Interviews conducted by Canada of the Contractor's employees and third party consultants during normal working hours or other times as mutually agreed.

5.1 General Compliance Requirements

a) The NCS must be protected and secure in accordance with Government of Canada security policies and legislation. The Contractor must maintain the Security of the NCS in accordance with the ongoing Security requirements that follow:

5.1.1 Government of Canada Policy Compliance

a) The Contractor must comply with the following Government of Canada security policies and legislation related to Transport and Transmittal of Protected B information.

Transport/Transmittal: The physical exchange of sensitive information must follow the Contract. When a delivery service is used, it must offer proof of mailing, a record while in transit and of delivery.

Transport	Transport: to transfer sensitive information and assets from one person or place to another by someone with a need to know the information or need to access the asset.
Transmittal	Transmit: to transfer sensitive information and assets from one person or place to another by someone without a need to know the information or need to access the asset.

Note:

1. For Transport of Protected “B” information (travel to/from neutral locations for meetings and/or interviews): In place of a single envelope, a briefcase or other container of equal or greater strength may be used. Double envelope/wrap to protect fragile contents or to keep bulky, heavy or large parcels intact.
2. For Transmittal of Protected “B” information (by Canada Post or registered courier): Address in a nonspecific manner. Add "To Be Opened Only By" because of the need-to-know or need-to-access principles.

5.1.2 Third Party Assurance and Certifications

a) The Contractor must maintain the following valid and up-to-date industry certifications for the period of the Contract:

i) ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems Requirements;

ii ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls for cloud services;

iii) ISO/IEC 27018:2019 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors ; and

iv) AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, privacy and confidentiality - issued by an independent Certified Public Accountant.

b) Each certification or audit report provided must: (i) identify the legal business name of the Contractor or applicable Sub-processor; (ii) identify the Contractor's or Sub-processor's certification date and the status of that certification; (iii) identify the services included within the scope of the certification report. If the carved-out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

c) 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 Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor.

d) Each SOC 2 Type II audit report must have been performed within the 12 months prior to the Operations Ready Date. A bridge letter may be provided to demonstrate 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).

e) The Contractor is expected to maintain its certification of ISO 27001, ISO 27017, ISO 27018 and SOC 2 Type II for the period of the Contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

5.1.3 Cloud Service Provider (CSP) IT Security Assessment Program

a) If during the period of the Contract and following the approval of the Project Authority, the Contractor migrates the application and/or data from an on premise to a Cloud-based solution, the Contractor must demonstrate that the Cloud Service Provider:

i) Is compliant with the security requirements selected in the Government of Canada Security Control Profile for Cloud-Based Services for GC Services for Cloud Services that are leveraged for the NCS; and

ii) Has been assessed under the Canadian Centre for Cyber Security (CCCS) CSP Information Technology (IT) Security Assessment Process (ITSM.50.100).

b) Any Cloud Service Provider that has participated in the process must provide documentation to confirm that they have completed the onboarding process with (i) a copy of the most recent completed assessment report provided by CCCS; and (ii) a copy of the most recent summary report provided by CCCS.

5.1.4 Supply Chain Risk Management

a) The Contractor must maintain safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide services. This includes but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel including subcontractors within the supply chain.

b) The Contractor must maintain a Supply Chain Risk Management (SCRM) Plan that describes the Contractor's approach to SCRM and demonstrates how the Contractor's approach will reduce and mitigate supply chain risks.

c) The supply chain risk management approach must continue to be aligned with one of the following best practices:

i) ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); or

ii) NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

5.2 Conformance Review

a) Canada will—on an annual basis—conduct a GC approved audit and conformance review—paid for by the Contractor—that includes but is not limited to:

i) Ensuring that the Solution conforms to the NCS Security Requirements (see Appendix E - Security Requirements Traceability Matrix) and the RCMP Departmental Security Control Profile (DSCP) including a review of the Plan of Action and Milestones to ensure milestones are being reached;

ii) Ensuring that all Solution software has current and up to date security updates and patches for all known vulnerabilities;

iii) Ensuring that the Contractor is proactively monitoring for software vulnerabilities in NCS and implementing any required security patches and software releases to remedy such vulnerabilities; and

iv) Composition of Contractor's core team.

b) The Contractor must provide supporting evidence within ten (10) working days of a request by Canada, for any supporting evidence required for the conformance review.

c) If Canada deems that the supporting evidence does not support the conformity to the Contract, Canada will request a Plan from the Contractor to address the discrepancies identified by Canada with conformity to the terms and conditions of the Contract.

5.3 Security Validation

a) The Contractor must provide Canada with an SRTM that provides traceability for each NCS security assurance requirement marked for validation in the NCS Appendix E - Security Requirements Traceability Matrix). For each requirement, the SRTM must provide service documentation references within the service design specifications that describe the security safeguards to be implemented. The SRTM establishes assurance that the Solution design fully satisfies its security requirements.

b) All service documentation referenced in the SRTM must be provided to Canada with the SRTM and must describe the security safeguards in sufficient detail to allow Canada to confirm that the security safeguards satisfy the security requirements marked for validation in the NCS Appendix E - Security Requirements Traceability Matrix).

c) The Contractor must work collaboratively with the RCMP to assess the Solution against the RCMP DSCP via the SA&A process.

5.4 Security of Environment Systems and Data

5.4.1 Facility Security Clearance

a) The Contractor must, at all times during the performance of the Work, hold a valid Facility Security Clearance (FSC) to a Protected B level for all primary and secondary and Disaster Recovery sites hosting, storing or processing NCS data, in accordance with the Government of Canada Directive on Security Management .

5.4.1.1 Physical Security

a) The Contractor must maintain Physical Security measures for the protection of IT facilities and information system assets on which NCS data is stored and processed against all forms of unauthorized access, tampering, loss, damage, and seizure, and that is based on a prevent-detect-respond-recover approach to physical security. At a minimum, this must include:

i) Sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed service level agreement;

ii) Proper handling of IT media;

iii) Controlled maintenance of information systems and their components to protect their integrity and ensure their ongoing availability;

iv) Controlled access to information system output and storage devices to prevent unauthorized access to Canada's data;

v) Limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification;

vi) Escorting visitors and monitoring visitor activity;

vii) Maintaining audit logs of physical access;

viii) Controlling and managing physical access devices;

ix) Enforcing safeguarding measures for NCS data at alternate work sites (e.g. telework sites); and

x) Recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.

Reference: Government of Canada Directive on Security Management .

b) The Contractor's facilities must have physical protection measures that must be applied in accordance with practices in the Royal Canadian Mounted Police (RCMP) guidance and standards on physical security - G1-025 Protection, Detection and Response .

c) The Contractor must notify the Project Authority and the Industrial Personnel Security Services Directorate (formerly CISD) of any enhancements or changes made to the facilities managing the NCS.

5.4.2 Security Zoning

a) The Contractor must utilize security controls to ensure appropriate isolation of resources such that NCS data is not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Service's functionality and system administration. This includes access controls and enforcement of appropriate logical or physical segregation to support:

i) Separation between the Contractor's internal administration from resources used by its customers; and

ii) Separation of customer resources in multi-tenant environments in order to minimize one malicious or compromised consumer from affecting the service or data of another.

b) The Contractor must maintain Network security zoning aligned with:

i) Canadian Security Establishment (CSE) IT Security Guidance (ITSG) ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada; and

ii) Canadian Security Establishment (CSE) Network Security Zoning - Design Considerations for Placement of Services within Zones (ITSG-38).

c) The Contractor must monitor and maintain Network security zoning to ensure:

i) Strict control of all Public Zone interfaces, including all external uncontrolled networks such as the Internet, at a defined security perimeter; and

ii) Perimeter defence safeguards (e.g. firewalls, routers) which mediate all traffic and to protect servers that are accessible from the Internet.

d) Any planned or unplanned changes to the environment, throughout the period of the Contract, must be documented and updated in accordance with the Change Management Plan and Process.

5.4.3 Solution Design Review

a) The service design for the NCS must be reviewed and approved by Canada. This includes providing Canada with a copy of the proposed architecture of the NCS that will enable Canada to perform:

i) a review of the proposed security safeguards and security components that will be implemented as part of the NCS; and

ii) a review of the security configuration of all security devices.

5.4.4 Malware Protection

a) The Contractor must protect IT components used to deliver and manage the solution from cyber threats, including monitoring devices, servers, peripheral devices, and desktop workstations, and must protect and prevent penetration by external sources;

b) The network protection must be implemented and maintained to detect and eliminate malicious software and/or unauthorized external connection attempts on the network; and

c) The Contractor must scan the Contractor environment supporting the NCS for the presence of malware. There must be active host-protection mechanisms on servers that performs:

i) On access scans for malware; and

ii) Scheduled active scanning of malware at a minimum of once a month.

5.4.5 Security Updates

a) The Contractor must apply Security Updates on regular Operating Systems and Applications to patch vulnerabilities utilizing a risk based approach aligned to the methodology set out in Canadian Security Establishment (CSE) Security Vulnerabilities and Patches Explained - IT Security Bulletin for the Government of Canada (ITSB-96) .

5.4.6 Patch and Vulnerability Management

a) The Contractor must perform patch management including, at a minimum:

i) Ensuring a current supported version of applications and operating systems are used;

ii) Ensuring that vulnerabilities are evaluated, and vendor-supplied security patches are applied in a timely manner;

iii) Prioritizing critical patches and service packs using a risk- based approach; and

iv) Testing and verifying to ensure that patches have been implemented properly.

5.4.7 Privilege Management

a) The Contractor must manage and monitor privileged access to the NCS to ensure that all service interfaces are protected from unauthorized access. This process must include, at a minimum:

i) Enforce and audit authorizations for access to NCS data;

ii) Restrict and minimize access to only authorized devices, users, and administrators with an explicit need to have access;

iii) Constrain all access to service interfaces that host NCS data to uniquely identified, authenticated and authorized individuals;

iv) Implement multi-factor authentication mechanisms to authenticate users with privileged access;

v) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to NCS data;

vi) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles;

vii) Adhere to the principles of least privilege and need-to-know when granting access to employees and contractors;

viii) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of services and infrastructure;

ix) Implement an automated or manual process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions. If a manual audit process is used, a policy or procedure for this activity must be documented and shared with Canada; and

x) Upon termination of employment or contract, terminate or revoke authenticators and access credentials associated with the employee or subcontractor.

5.4.8 Secure Data Migration and Exchange

a) The Contractor must maintain data migration practices to support implementation of the NCS as follows:

i) Between the Contractor and their subcontractors

The Contractor must leverage the Government of Canada approved Managed Secure File Transfer (MSFT) solution for Secure Data Migration and Exchange between themselves and their subcontractors (if applicable) that supports Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol over Secure Socket Layer (FTPS) and File

Transfer Protocol over Secure Shell (SFTP) and provide data encryption compliant to the Federal Information Processing Standards (FIPS) 140-2 cryptography requirements.

ii) Between the Contractor and Canada

- The Contractor must establish secure network connections that implement TLS 1.2, or subsequent versions, and uses supported cryptographic algorithms and certificates, accepted by the CSE as follows:
- Canadian Security Establishment (CSE) Guidance on Securely Configuring Network Protocols (ITSP.40.062) Section 3.1 for AES cipher suites
- Canadian Security Establishment (CSE) Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information (ITSP.40.111)

The Contractor must update its secure network connection in accordance with the above CSE requirements as those CSE requirements evolve during the period of the Contract.

iii) Between the Contractor and third party

Upon the Project Authority Approval and Personnel Security Screening Division (PSSD) (formerly CISD) clearance, the Contractor must provide a Secure data transfer tool or methodology that allows the Contractor to transfer data to an approved third party to facilitate external audits and other Government initiated projects.

5.4.9 Cryptographic Protection

a) The Contractor must use, and update if deemed necessary in discussion with Canada, cryptography protection to maintain confidentiality or integrity safeguards or as part of the authentication mechanism (e.g. VPN solutions, TLS, software modules, PKI, and authentication tokens, where applicable) in use for the Service.

b) The Contractor must use the following approved cryptographic algorithms and cryptographic key sizes and crypto periods:

i) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSE and validated by the NIST Cryptographic Algorithm Validation Program and are specified in ITSB-111 or in a subsequent version; and

ii) Be implemented and operated in an approved mode in a Cryptographic Module, validated by the NIST Cryptographic Module Validation Program to at least NIST Security Requirements for Cryptographic Modules (FIPS 140-2)

validation at Level 1. At a minimum, FIPS 140 compliant/validated cryptography must be employed at perimeter protection devices or anywhere else encryption is required.

5.4.10 Security of Electronic Data Interchange

a) The Contractor must ensure that NCS data submitted or exchanged between the NC3 and Partners via EDI or other Digital Services comply with all established NCS security requirements;

b) The Contractor's Solution must facilitate secure transmission of information using EDI between Partners and the NC3;

c) The Contractor's Solution must safeguard the integrity and authenticity of all NCS data at rest and in transit, from corruption and inadvertent or malicious changes by employing hashing, digital certificates, or similar technology, in accordance with 5.4.10 Cryptographic Protection; and

d) The Contractor must ensure that security and privacy of information is maintained throughout any data conversion or loading exercise.

5.4.11 Data Storage and Retention

a) The Contractor must store all NCS back-up data in accordance with NC3 Information retention requirements and the following:

i) All handling of any removable media that may be used with the system must meet with the requirements for proper labelling, destruction and handling, and storage of these types of assets in accordance with Secure use of portable data storage devices within the Government of Canada Secure use of portable data storage devices within the Government of Canada (ITPIN 2014-01) ;

ii) All back-up data must be stored in a secure, fire and flood protected area;

iii) Data storage protection must meet Advanced Encryption Standards (AES), with key lengths of 128 bits, to protect the confidentiality and integrity of backup information at the storage location;

iv) The Contractor must assess the viability of whether storage media can be securely reused based on the CSE Guidelines on IT Media Sanitation (ITSP.40.006) ; and

v) The Contractor must pay for any costs associated with the destruction of data initiated by the Contractor and approved by the Project Authority.

5.4.12 Data Extraction

a) The Contractor must provide the tools and services that allow Canada to:

i) Extract all online, near line, and offline Canada's data, including, at a minimum, databases, object and file storage, system configurations, cloud activity logs, source code hosted in a Canada code repository, and network configurations such that any Canada End User can use these instructions to migrate from one environment to another environment; and

ii) Securely transfer all Canada's data, including content data and associated metadata, in a machine-readable and usable format, including CSV format, and in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value .

5.4.13 Data Destruction

a) At the end of the contract period (i.e. at contract expiration or termination) or upon request by the Project Authority, the Contractor must follow the CSE Guidelines on IT Media Sanitation (ITSP.40.006) that contained NCS data;

b) The Contractor must provide reported evidence, such as a certificate, to attest to the destruction of all user data related to the NCS; and

c) All costs associated with the destruction of media that contained or hosted NCS Protected B Information is to be borne by the Contractor.

5.4.14 Data Transportation

a) In the event that data on paper must be physically transported, the Contractor must adhere to RCMP G1-009 Transport and Transmittal of Protected and Classified Information and the Contract Security Manual – Chapter 6: Handling and safeguarding of classified and protected information and assets;

b) The Contractor must mark all hard copy documents and other media with the highest appropriate security classification as provided by the Project Authority; and

c) The Contractor must obtain Project Authority approval prior to moving data in or out of Protected B physical domain.

5.5 Secure Access Controls

5.5.1 Personnel Security Clearance

a) The Contractor must ensure that all individuals handling, viewing, managing, or who may come in contact with, NCS data or who have access to the NCS designated facilities, have a valid security clearance at the level of Reliability or higher based on the levels of security requirements as per Government of Canada Levels of security . The Contractor must ensure that any new personnel including subcontractors have appropriate clearances and that clearances are maintained throughout the period of the Contract; and

b) The Contractor must ensure personnel screening measures are applied in accordance with the definition and practices in the Government of Canada's Standard on Security Screening to ensure the adequate protection of Protected B Information.

5.5.2 Access Controls

a) The Contractor must provide role-based access control as follows:

i) The Contractor must implement Access Controls based on roles defined in the NCS, where each role is assigned capabilities and access according to the least privilege required for that role, and a need-to-know;

ii) The Contractor must implement a process to manage a unique user account for each of the Project Authority identified users of the NCS solution Protected B data, including at a minimum, the Police and Partner Portal (P3) and NCS Interfaces; and

iii) The Contractor must apply identified changes to user access profiles within three Days of receipt of information from the Project Authority;

b) The Contractor must implement multi-factor authentication mechanisms for users and privileged accounts;

c) The Contractor must ensure passwords comply with CSE's User Authentication Guidance for Information Technology Systems (ITSP.30.031) ;

d) The NCS solution should notify users, upon successful logon, of the date and time of the last successful logon;

e) Any change to a user account must be accompanied by an audit record indicating what was changed, which user account made the change, on what date and time and by whom;

f) The Contractor must ensure Contractor user access and controls are kept current with all changes or updates to Contractor staff and also provide notification of such changes to the Project Authority.

5.5.3 Account Protection

a) The Contractor must maintain controls to issue and update existing account passwords in accordance with either:

i) CSE's User Authentication Guidance for Information Technology Systems (ITSP.30.031) ; or

ii) Other industry best practices such as ISO 27001 or NIST.

5.5.4 Security Awareness and Training

a) The Contractor must provide a security awareness training or briefing session to ensure that all personnel including subcontractors handling NCS Protected B Information understand their role and responsibilities in managing information security, prior to commencing work on the NCS.

5.6 Security Testing

a) The Contractor must provide Canada with a Security Testing Plan that documents the test cases to verify each NCS Production Environment (NCS PE) security assurance requirement, marked for Security Testing in the Appendix E - Security Requirements Traceability Matrix).

b) The Contractor must perform the Security Testing Plan for each security safeguard and provide Canada with a Security Testing Report that satisfies one or more of the security requirements marked for security testing in Appendix E - Security Requirements Traceability Matrix) :

i) The Security Testing procedure must confirm that the security safeguard is implemented correctly and satisfies applicable standards as specified in the service design specifications;

ii) The expected and actual results for each Security Testing procedure;

iii) For each deviation from the expected result that could be corrected at the time of verification, a description of the corrective measure(s) that were implemented in the NCS PE; and

iv) For each deviation from the expected result that could not be corrected at the time of verification (e.g., due to more significant changes), a Change Request reference.

c) The Contractor must update the SRTM to include the tracing between the security requirements marked for Security Testing and the Security Testing procedures.

d) The Contractor must allow Canada to witness the Security Testing that includes the ability to observe Contractor representatives while they execute the Security Testing procedures or the ability to observe the test log results where the security testing is automated.

5.7 Security Controls Assessment Methods

a) The Contractor must use the following Security Controls Assessment Methods in the Security Test and Evaluation Report:

i) ASSESSMENT METHOD: Examine:

(1) ASSESSMENT OBJECTS:

a) Specifications (e.g., policies, plans, procedures, system requirements, designs);

b) Mechanisms (e.g., functionality implemented in hardware, software, firmware); and

c) Activities (e.g., system operations, administration, management; exercises).

(2) DEFINITION: The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time; and

ii) ASSESSMENT METHOD: Test:

(1) ASSESSMENT OBJECTS:

a) Mechanisms (e.g., hardware, software, firmware); and

b) Activities (e.g., system operations, administration, management; exercises).

(2) DEFINITION: The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

5.8 VULNERABILITY ASSESSMENT

a) The Contractor is responsible for internal and external Vulnerability Assessment testing on an as and when required basis, to be performed by the Contractor or a third party agreed upon by Canada. This testing must be conducted at a minimum on a yearly basis and aligned to the Vulnerability Management controls in the DSCP. The Contractor must determine the assignment of responsibility for supporting Vulnerability Assessment testing.

b) The Contractor must make provisions to allow Canada, or a third party acting on behalf of Canada, to perform internal and external Vulnerability Assessment testing on an as and when required basis.

c) Where Canada has requested that Canada, or a third party acting on behalf of Canada, perform Vulnerability Assessment testing, the Contractor must provide:

i) Logical access to the RCMP Protected B Cloud Tenant subscription where the NCS Test Environment (NCS TE) infrastructure is located and operated for;

ii) Network access or accesses to the NCS TE to allow for the scanning of network and host devices; and

iii) Assistance for the duration of any portion of the Internal Vulnerability Assessment of at least one (1) technical resource who is familiar with the technical aspects of the NCS TE (i.e., the software and network products and their configuration).

d) Where the Contractor, or third party on behalf of the Contractor, conducts its own Internal Vulnerability Assessment testing, the Contractor must:

i) Submit a Vulnerability Assessment Plan to Canada for its prior approval;

ii) Include within the scope of the plan, the scanning of all network and host devices deployed in the NCS TE;

iii) Conduct the vulnerability assessment testing in the NCS TE; and

iv) Provide the results to Canada for review and analysis. Canada may require implementation of Contractor initiated changes based on review and analysis.

e) In response to any source of Vulnerability Assessment testing, within ten (10) business days, the Contractor must provide Canada with a Vulnerability Mitigation Report that includes:

i) A list of vulnerabilities for which Canada is recommending the implementation of corrective measures;

ii) A list of vulnerabilities for which the Contractor is recommending the implementation of corrective measures if the Contractor has chosen to conduct its own Internal Vulnerability Assessment testing;

iii) A description of the corrective measures to be implemented including expected time frames; and

iv) Service documentation referenced in the SRTM that must be updated as a result of the implementation of the corrective measures.

f) The Contractor must implement the corrective measures identified in the approved Vulnerability Mitigation Report within the time frame established in the Vulnerability Mitigation Report.

2.) **Questions and Answers:**

Question #	Question	Response
10	**Section 7.8(c) of the RFP Translation Rights states:** "The Contractor agrees that Canada may translate any written deliverable, including the Solution Documentation or Training Materials into English or French." However Section 3.10.2 Training Material (a) in the SoW states that the "Contractor must provide English and French electronic copies of operating manuals, technical manuals, and other relevant user documentation that is required in order to learn, use, and maintain the Solution" etc, Can the Crown please clarify whether there is a requirement for operating manuals, technical manuals and all training materials to be translated by the Contractor?	Canada requires that the Contractor provide English and French electronic copies of operating manuals, technical manuals, and other relevant user documentation that is required in order to learn, use, and maintain the Solution.

11	**Section 3.4.b.ii of the SOW indicates that SA&A is part of Phase 2.** Can Canada confirm that SA&A controls for Phase 1 do not need to be implemented and will only be required if Canada invokes their option to begin Phase 2?	The SA&A is only required after Canada has selected a Contractor to deliver Phase 2.
12	**Section 3.18 Performance Metrics, Table 3-1 of the SOW specifies maximum response time metrics.** Is it Canada's intent to measure these from the browser or are they to be measured from the point they leave the Contractor controlled network endpoint?	Canada intends to measure the indicated metrics from the browser (end-user interface). However, the Contractor will not be held accountable for delays that occur outside the Contractor controlled network endpoint.
13	**Section 3.20 Web Content Accessibility Guidelines (WCAG) of the SOW references WCAG 2.0 but does not specify the level (e.g., A, AA) that must be achieved.** Capability 5.13.2.2 in Appendix C specifies WCAG 2.0 A. Mandatory Criteria MC-47 in Annex J aligns with Section 3.20 from the SOW. Can Canada confirm that WCAG 2.0 level A is the requirement?	See amendment to Annex A – Statement of Work, Section 3.20, Web Content Accessibility Guidelines (WCAG), paragraph a)
14	**Section 4.3 Interoperability of the SOW, subsections a. iv, v, vi, vii, xiv, and xi refer to various interfaces.** Can Canada confirm that all these interfaces, that are API based, support REST JSON or XML?	Canada confirms that these API based interfaces, support protocols including but not limited to: Representational State Transfer (REST) using JavaScript Object Notation (JSON) or Extensible Markup Language (XML).
15	**Section 4.3.b.i of the SOW talks about the Public Reporting Web Site queuing service.** Can Canada provide information on the Public Reporting Web Site queuing service that has been	As described in SOW section 4.4, the architecture and design of a message queuing interface to ingest reports from Canada's Public Reporting Web Site into the NCS is expected to be included as part of the Contractor's solution.

	selected? This service does not appear on Canada's architecture diagram in Appendix D.	No implementation currently exists for the Public Reporting Website.
16	**Sections 4.6.a, 3.12, 3.14 of the SOW do not appear to be fully aligned on the transition to Canada of the full solution.** Section 3.12 Transition Plan of the SOW suggests that the Transition Plan is for a full transition to Canada assuming the use of the RCMP Protected B Cloud Tenant. 4.6.a specifies three options that include the RCMP Protected B Cloud Tenant. Can Canada clarify how the Transition Plan should accommodate the three options discussed in section 4.6.a?	Canada requires a Transition Plan that aligns to the Bidder's Solution Architecture. SOW sec 4.6 Cloud Deployment outlines Canada's requirements related to the architecture as it relates to the Solution Cloud Service Delivery Model (CSDM). The Transition Plan requirements in the SOW do not intend use of the RCMP Protected B Cloud if this does not align with the Bidder's Solution (e.g. if the Solution is a SaaS or Public PaaS solution).
17	**Section 4.7.a.iv of the SOW specifies that:** Development of updates and new features must be performed on the RCMP Protected B Cloud Tenant in a development environment. How does this requirement reconcile with section 4.6.a where three options are described?	Section 4.7 Source Code and Development does not apply to SaaS or Public PaaS components of a solution. For IaaS and private PaaS components of a Solution that involve custom code development and custom configuration, Canada requires the Contractor to provide an integration team to work collaboratively with the RCMP, as specified in section 4.7.
18	**Section 4.8 of the SOW requires the use of Azure AD for administrative access.** Note that section 4.6.d.iv of the SOW only specifies Azure AD is to be used for internal RCMP and external Partner users. Which section is correct?	The Solution must use Azure AD (Active Directory) functionality for Identity and Access Management for all Users of the Solution (including administrative access).
19	**Section 5.6. a of the SOW states that:** The Security Testing Plan must address the security assurance requirements in Appendix E that are marked for Security Testing. Section 5.7 of the SOW	Section 5.7 provides the methodologies acceptable for testing, but the Contractor will be granted the flexibility to assign a test methodology for a given control that they find

	provides information on the assessment method for controls of Examine or Test. A review of Appendix E does not identify which security requirements are "marked for testing" vs "examine". Will Canada be providing an updated Appendix E that highlights which security requirements are "marked for testing"?	most appropriate, subject to review by the Canada during the SA&A process. As such, Canada will not be providing an updated Appendix E, but rather will be expecting the vendor to make a determination of the appropriate assessment methodology for each security assurance requirement in the Security Testing Plan it will deliver to Canada.
20	**Section 5.8 Vulnerability Assessment of the SOW:** States this is an optional service as outlined below: 5.8 b) states: "If the Contractor selects to allow Canada to perform the Internal Vulnerability Assessment testing, the Contractor must provide **….."** and 5.8 c) states "If the Contractor (or third party on behalf of the Contractor) chooses to conduct its own Internal Vulnerability Assessment testing, the Contractor must:….." Proponents can therefore elect to perform themselves, or have Canada perform the Assessment. How will Canada ensure the financial evaluation is fair and equitable , between proponents who have elected to include or exclude these costs?	See amendment to Annex A – Statement of Work, Section 5.0, System Security Plan, paragraph 5.8
21	**Section 7.1.d of the SOW states that:** Phase 2 begins on the date Canada exercises their option to deliver Phase 2. Is it Canada's intention that Phase 2 should: a. Follow Phase 1 immediately with no gap in service between the end of Phase 1 and the start of Phase 2?	Canada intends to initiate Phase 2 immediately after completion of Phase 1.

	b. Proceed after Phase 1 is completed but with a gap of several weeks or months between the end of Phase 1 and the start of Phase 2? c. Overlap with Phase 1 schedule? If yes, by how many weeks or months?	
22	**Appendix C – NCS Business Capability Model of the SOW, capability 2.1.2.4 requires exchange rates.** Is Canada providing access to an API that will provide these exchange rates to NCS?	The Contractor's Solution must provide a currency conversion Solution per the stated requirement in the BCM. Canada will not commit to providing an API that will provide exchange rates.
23	**Capability 5.2.2.5 in Appendix C specifies MS Outlook integration as a requirement.** Capability 5.7.1.3 specifies NCS must integrate to the RCMP corporate email system. Is MS Outlook the corporate email system and is it missing from Table 4.1 Mandatory RCMP Components?	MS Outlook is the RCMP's corporate email system.
24	**Annex J Mandatory Criteria MC-55 specifies that:** Evidence must be provided confirming successful integration between the proposed CSP and GoC networking using SCED infrastructure. Can Canada confirm that, for the purpose of Phase 1, this integration must exist as of the bid closing date of this RFP? If yes, please provide a list of CSPs that meet this requirement, and that Bidders intending to use any other Cloud will be non compliant?	Canada confirms that, integration between the proposed CSP and GoC networking using SCED infrastructure must exist as of the bid closing date of this RFP. A list of CSPs that meet these requirements is available by contacting the GC Cloud Brokering Services.

25	**Mapping of Annex J Mandatory / Rated Criteria to Appendix C Capabilities:** Can Canada provide a traceability mapping of the Mandatory and Rated Criteria in Annex J to the corresponding Capabilities in Appendix C? This traceability is required to document the gap between Phase 1 and Phase 2 capabilities to be delivered post Phase 1, and to ensure all Bidders are pricing the same solution.	Canada will not provide a traceability mapping. Canada expects Bidders to meet the requirements as stated in Appendix C. Any gaps between Phase 1 and Phase 2 capabilities will be addressed during Phase 2.

ALL OTHER TERMS AND CONDITIONS OF THE BID SOLICIATION REMAIN UNCHANGED.