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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
By email at:
TPSGC.PACCSGPN-APBWCDEMS.PWGSC@tpsgc-pwgsc.gc.ca
Please refer to the RFI

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
Special Projects Division (SPD)/Division de Projets Spéciaux (DPS)
Terrasses de la Chaudière 4th Floo
Terrasses de la Chaudière 4e étage
10 Wellington Street,
10 Wellington Street,
Gatineau
Québec
K1A 0S5

Title - Sujet RFI #3 for DEMS/Body Worn Cameras	
Solicitation No. - N° de l'invitation M7594-212120/D	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client M7594-212120	**Date** 2021-04-06
GETS Reference No. - N° de référence de SEAG PW-$$XU-005-39339	
File No. - N° de dossier 005xu.M7594-212120	**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 2021-04-13 Heure Avancée de l'Est HAE

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

Address Enquiries to: - Adresser toutes questions à: Mulligan, Kate	**Buyer Id - Id de l'acheteur** 005xu
Telephone No. - N° de téléphone (873) 353-9579 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
The Royal Canadian Mounted Police
1200 Vanier Parkway
Ottawa, ON K1A 0R2

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

Request for Information # M7594-212120/D

National Digital Evidence Management System (DEMS)

and Body Worn Cameras (BWC)

AMENDMENT #001

This Request for Information (RFI) amendment is issued to:

1. Extend the RFI closing date; and
2. Provide Industry with Annex A - Draft Overview and High Level Description of the Requirement.

The Request for Information (RFI) is hereby amended as follows:

1. On Page 1 of 1 of the RFI:

DELETE the following:

Solicitation Closes – L'invitation prend fin
At – à 02:00 PM
On – le 2021-04-09

INSERT the following in its place:

Solicitation Closes – L'invitation prend fin
At – à 02:00 PM
On – le 2021-04-13

2. At Annex A of the RFI:

DELETE the Annex A - Draft Overview and High Level Description of the Requirement and **INSERT** attached Annex A - Draft Overview and High Level Description of the Requirement.

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED.

ANNEX A

DRAFT OVERVIEW AND HIGH LEVEL DESCRIPTION

1. Background

1.1 The Royal Canadian Mounted Police (RCMP) is Canada's national police service and has policing mandates across the country at community, provincial, territorial and federal levels. The RCMP provides federal, provincial, territorial and municipal policing services to Canadians across 10 Provinces, 3 Territories, 150 municipalities, over 600 Indigenous Communities which includes providing both Federal Police Services and Specialized Police Services in support of hundreds of other police and public safety agencies across Canada.

1.2 The RCMP is a $5B organization with approximately 30,000 employees including 19,000 police officers. The RCMP has more than $1.3B in assets including 3,362 buildings and 14,749 vehicles across the country. The RCMP has made a decision to make body worn cameras (BWC) and a digital evidence management system (DEMS) a national standard for all front line and general duty police officers across the country, which is in the range of 10,000 - 15,000 officers. Many of these police officers work in rural and remote areas in approximately 750 detachments across Canada.

2. Key Driver for Change

2.1 The RCMP, and other police forces, are faced with increased public scrutiny of their interactions with the communities they serve. One key initiative to increase transparency and accountability is the national deployment of BWCs for RCMP police officers. Although not a universal solution, when BWCs have been used in other police forces around the world, they have been shown to increase transparency and reduce the time it takes to resolve complaints.

3. Use of Body Worn Cameras

3.1 Over the last 15 years, BWCs have been implemented around the world. In Canada, BWCs have been implemented, or are in various stages of implementation, in many of the larger police services including Calgary, Halifax, Toronto, and Peel.

3.2 The RCMP has been researching this technology for a number of years and has conducted BWC pilots. In 2017, the RCMP deployed twelve BWCs to the RCMP members who were serving in Happy Valley-Goose Bay and Cartwright in Newfoundland and Labrador (B Division) as a limited and temporary deployment of equipment to support police operations. This allowed the RCMP to assess the functionality of these devices in an operational environment.

3.3 After consulting with community members, stakeholders, and federal and territorial government officials, a limited pilot was launched in Iqaluit in the fall of 2020 to test draft operational procedures and guidelines and to determine resource requirements to support the

operations of the BWCs and the storage and management of video evidence. Information and data gathered from this pilot will be used to improve operational policy, procedures and training programs in support of the national Body Worn Camera and Digital Evidence Management System (BWC/DEMS) Program.

3.4 Pilots have been done previously, but have focused mostly on the BWC functions, limitations, operational impacts and policies. The RCMP maintains a small contingent of BWCs for limited use during major events.

4. Objectives and Business Outcomes

4.1 The RCMP is looking to procure the services of a Contractor to deliver "Services" that support the national rollout of BWCs along with the implementation of a national DEMS as detailed in sections 5.4.1 and 5.4.2. We are targeting to have a contractor in place by the summer of 2021. The first BWCs will be deployed in a phased manner leading to national implementation with full rollout, including a robust DEMS and related training, within 12-18 months of contract award.

4.2 As a result of implementing a national BWC/DEMS Program within the RCMP, Canadians can expect:

- Improved transparency and accountability for police leading to increased public trust and confidence in police;
- Increased lawful and respectful interactions between the public and the police;
- Improved evidence gathering and timely prosecutions; and
- Increased withdrawal or timely resolution of complaints due to video evidence.

4.3 The most tangible improvements are expected to be improved evidence collection, reductions in times to resolve complaints and increased transparency. The video evidence collected will provide an independent and objective way to capture incidents and interactions between police officers and the community.

4.4 Any resulting contract(s) may be available for use by other Canadian Federal Government departments and agencies, Canadian Municipal, Provincial and Territorial Government departments and agencies as well as by other Canadian provincial and municipal police forces.

5. Functional Scope

5.1 The Contractor that will be chosen among the Qualified Respondents, will be expected to provide and support a solution to deliver BWC equipment and a DEMS as a software as a service (SaaS) delivery model as a fully managed service.

5.2 This service will need to be adaptable to meet the unique RCMP requirements, meeting the needs of urban, rural and remote RCMP locations, and be able to deliver capabilities across multiple jurisdictions. The service must be scalable to support the needs of the RCMP, which is expected to equip up to 10,000 – 15,000 RCMP police officers with BWCs and DEMS as well as additional DEMS users across the RCMP.

5.3 The Contractor will need to consider the RCMP's unique challenges, such as the capture and storage of digital evidence in areas with limited data bandwidth, the ability for the BWC to operate under a wide range of temperatures given the diverse jurisdictions, and the automated activation and capture of digital evidence in emergency and high stress situations.

5.4 Using a competitive process to qualify Respondents, Canada will select a Contractor that will deliver as a Service the following components:

5.4.1 **BWCs**

The Contractor will be expected to provide Contractor owned and managed BWCs and associated equipment. Services which may be required, but are not limited to:

- provisioning;
- distributing;
- helpdesk support;
- training;
- maintenance and repair;
- secure disposal; and
- evergreening.

Associated equipment may include, but are not limited to the following:

- multiple uniform mounting options;
- mounting brackets and/or clips;
- associated docking stations and charging cables;
- Bluetooth trigger mechanisms (holster, conducted energy weapon, car); and
- hardware servers.

5.4.2 **DEMS**

The Contractor will be expected to provide a DEMS as a SaaS delivery model. Services which may be required are, but are not limited to:

- Configuration and testing;
- helpdesk support;
- training;
- implementation;
- deployment;
- onboarding;
- operations;
- maintenance; and
- evergreening.

The DEMS capabilities required may include, but are not limited to the following:

- secure and reliable data storage for Protected B data;
- upload of BWC video and other multi-media files from various sources;
- search and retrieval of digital evidence;
- integration capability in the form of a secure application programming interface (API);

- management, redaction and editing of captured information; and
- ability to share evidence internally and externally.

6. Functional Capabilities, Outcomes and Business Value

The following table reflects the business tools and capabilities Canada expects to implement as part of this initiative. This list of capabilities is intended to be used to create a functional project scope and detailed business requirements which will be outlined in future stages of the procurement process. This capability list itself may also evolve during the procurement process.

Functional Area	Capability	Business Value
Body Worn Cameras	• **Robust and easy to use**	• Can withstand the wear and tear that occurs throughout the course of a police officer's shift and does not compromise police officer safety • Easily activated with an ambidextrous single hand and avoid accidental de-activation
	• **Flexible and secure uniform mounting options**	• Ability to fit within the available space and visually blend in with the RCMP police officer uniforms • Compatible with multiple uniform mounting options that can support a variety of operational needs • Mount(s) that can be securely fastened to a police officer's uniform
	• **Operate in rural and remote areas**	• Can withstand the extremes of the Canadian winters and summers without affecting performance or compromising the ability to capture the events during a police officer's shift
	• **Automated uploading of digital evidence**	• Uploading processes that can be carried out in urban, rural and remote geographical areas that minimize additional work for police officers at the end of their shift • Ability to upload evidence from BWCs to DEMS where there may be limited bandwidth in remote locations (e.g. BWCs that connect directly to DEMS via cellular network)
	• **Battery life and storage capacity**	• Sufficient battery life and storage capacity to ensure that the police officer

		is able to capture all required recordings for the entire duration of the shift
	• **Equipment Management**	• The secure supply, distribution, maintenance, repair, replacement, upgrade, and disposal of BWCs and all related equipment
DEMS	• **Cloud based storage of digital evidence**	• Accommodate the secure uploading of digital evidence from the BWCs and other multi-media files to a cloud-based storage solution. • Provide a solution that supports rural and remote areas that have low bandwidth.
	• **Management of evidence**	• Allow Canada to store and organize the digital media in a way that facilitates the organization and retrieval of data and considers the mobility of resources who will move between detachments within a single division and move from one division to another over time • Provide a service that is available in both of Canada's official languages (English and French) and meets Government of Canada Accessibility standards as outlined in section 7.1.
	• **Redaction and Editing**	• Include tools that are secure and easy to use and support the redaction and editing of digital media for disclosure. Tools that support automation and reduce the number of manual interventions through the use of robotic process automation features are desirable
	• **Disclosure**	• Accommodate the easy disclosure of evidence to a variety of external stakeholders in multiple jurisdictions across the country
	• **Reporting**	• Support the reporting of information at various levels including geographic based reporting • Support a variety of reporting needs (e.g. administrative, audit, performance, etc.)
	• **Privacy and Security**	• Ensures compliance to federal privacy legislation and security standards and

		provides tools to manage and control user access • Must meet cloud Protected B security requirements for the Government of Canada • The DEMS Solutions and Services must be hosted by a "qualified" Cloud Service Provider that has completed the CCCS Assessment Program (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technologysecurity-assessment-process-itsm50100) and has met all of the requirements of Shared Services Canada's Invitation to Qualify for Government of Canada Cloud Service Procurement Vehicle (GC Cloud) (https://buyandsell.gc.ca/procurement-data/tender-notice/PW-18-00841719).
	• **Interfaces and Integration**	• Digital evidence can be integrated to RCMP source systems for the purposes of operational records management
	• **User Access Management**	• Ability for the RCMP to set role-based access controls • Ability to use federated identities for user access management
Cross-Functional Services	• **Training**	• Provision of training materials to support training of all RCMP police officers and end-users of the BWC and DEMS in both official languages of Canada
	• **Helpdesk Support**	• Provision of 24/7 support in both official languages of Canada for both the use of the BWCs and the use of the DEMS with a set of service standards that are adhered to.
	• **Fault and performance reporting and resolution**	• Provision of a service that must monitor and report faults or errors and must provide resolutions to faults and errors within a set of service standards. • Ability for end-users to access reports on a variety of performance information and service usage data

	• **Availability / Business Continuity**	• Ability for end-users to continue to record and store events during major disruptions (e.g. power failure, loss of telecommunications, etc.) • Ability for end-user's information to be stored and protected at rest, including data in backups or maintained for redundancy purposes within the geographic boundaries of Canada

7. Anticipated Mandatory Requirements

It is anticipated that any future bid solicitation will include the following MANDATORY requirements. These pertain to the Contractor's capacity to develop and deploy a BWC/DEMS Program solution . The full list of requirements to be delivered as part of the BWC/DEMS Program solution are under development and will be supplied further in the procurement process.

7.1 Accessibility

The system solution must ensure AA compliance to Web Content Accessibility Guidelines (WCAG) 2.1 standards as described at the following link: https://www.w3.org/TR/WCAG21/

These standards include but are not limited to:

- Correct use of semantic/hierarchical markup (essential for screen readers);
- Alt-text for all information-bearing images (null alts for decorative images);
- Users must be able to tab to all features (complete functionality without a mouse);
- Links must open in the same browser window (no new tab/new window);
- Tables must conform to WCAG specifications.

Any accommodations and points of interest presented visually on a map must also be presented in an accessible text format.

The system solution must conform to the Government of Canada Standard on Accessibility as described at the following link: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601

7.2 Security Obligations

The following areas are a subset of the larger set of security requirements which are being developed and is not an exhaustive list. Organizational Data is defined as all data created and/or processed by the RCMP and/or its Police Partner Agencies and/or Canada within the Cloud Service. Organizational Data includes any and all metadata and logs derived from or related to Organizational Data.

7.2.1 Third-Party Assurance: Certifications and Reports

The Contractor must ensure that Organizational Data, Contractor's 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 Contractor's security practices and policies.

The Contractor must demonstrate that the measures 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 Service offering, including:

a) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Certification achieved by an accredited certification body; **AND**
b) 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.

Other Certifications which may be reviewed and/or considered are:

a) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services achieved by an accredited certification body;
b) ISO/EIC 27018:2019 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors; **AND**
c) Cloud Security Alliance (CSA) Level 2 CSA Star Certification and Attestation.

Each certification or audit report provided must:

a) Identify the legal business name of the Contractor or applicable Sub-processor;
b) Identify the Contractor's or Sub-processor's certification date and the status of that certification; and
c) 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.

7.2.2 IT Security Assessment and Authorization Process

Compliance will be assessed and validated by Canada utilizing the RCMP Security Assessment and Authorization Process or through a third-party process determined by Canada.

In the situation where the Contractor has been assessed and validated through the Canadian Centre for Cyber Security (CCCS) Cloud Security Provider (CSP) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-

security-assessment-process-itsm50100). The Contractor must demonstrate that they participated in the process by successfully on-boarding, participating in, and completing the program. This includes providing the following documentation to the RCMP:

a) A copy of the confirmation letter that indicates they have on-boarded into the program;
b) A copy of the most recent completed assessment report provided by CCCS; and
c) A copy of the most recent summary report provided by CCCS.

7.2.3 **Removable/Portable Media**

All BWC and other portable/removable media must be FIPS 140-2 Level 1 validated/compliant

7.2.4 **Data Location**

As per the guidance found at: https://www.canada.ca/en/government/system/digital-government/guideline-service-digital.html#ToC4_4

The Contractor must store and protect Organizational Data, at rest, including data in backups or maintained for redundancy purposes. This includes the ability to isolate data within the geographic boundaries of Canada in one of the approved cloud service providers (CSP) on the list found at: https://cloud-broker.canada.ca/s/central-provider-page-v2?language=en_US

The Contractor must have the ability for the RCMP to isolate Organizational Data hosted in Cloud Services in approved CSPs that are geographically located in Canada.

Upon request of Canada, the Contractor must:

a) Provide Canada with an up-to-date list of the physical locations, including city, which may contain Organizational Data for each CSP that will be used to provide the Cloud services; and
b) Identify which portions of the Cloud Services are delivered from outside of Canada, including all locations where data is stored and processed and where the Contractor manages the service from.

It is the continuous obligation of the Contractor of the proposed Cloud Services to notify Canada when there are updates to the list of physical locations which may contain Organizational Data

7.2.5 **Backup and Recovery**

Backups are to be stored in data centres that are geographically separated by at least 200km to protect from natural and man-made disasters and are operate on differing power grids to ensure protection from prolonged loss of power in a specific geographical region.

7.2.6 **Incident Management**

The Contractor's Security Incident response process for the Cloud Services must encompass IT security incident management lifecycle and supporting practices for preparation, detection, analysis, containment, and recovery activities. This includes:

a) A published and documented Security Incident Response Process for review by Canada that is aligned with one of the following standards:
   i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; OR
   ii) NIST SP800-612, Computer Security Incident Handling Guide; OR
   iii) GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/treasury-board-secretariat/services/accessinformation-privacy/security-identity-management/government-canada-cybersecurity-event-management-plan.html); OR
   iv) other best practices from industry standards, if Canada determines, in its discretion, that they meet Canada's security requirements.
b) Documented processes and procedures of how the Contractor will identify, respond, remediate, report, and escalate Security Incidents to Canada, including:
   i) The scope of the information security incidents that the Contractor will report to Canada; The level of disclosure of the detection of information security incidents and the associated responses; The target timeframe in which notification of information security incidents will occur;
   ii) The procedure for the notification of information security incidents;
   iii) Contact information for the handling of issues relating to information security incidents; AND
   iv) Any remedies that apply if certain information security occur.

The Contractor must have procedures to respond to requests for potential digital evidence or other information from within the Cloud Services environment and includes forensic procedures and safeguards for the maintenance of a chain of custody.

If required by Canada, the Contractor must:

a) Work with Canada's Security Operations Center(s) (e.g. CCCS, RCMP SOC) on Security Incident containment, eradication and recovery in accordance with the Security Incident Response process.
b) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data or the service; and
c) Track, or enable Canada to track, disclosure of Organizational Data, including what data has been disclosed, to whom, and at what time.

7.2.7 **Cryptographic Protection**

A minimum of FIPS 140.-2 Level 1 validated cryptography is employed when encryption is required for the Digital Evidence Management System.

7.2.8 External Application Programming Interfaces (API)

Take reasonable measures to protect external APIs through secure authentication methods. This includes ensuring that all externally exposed API queries require successful authentication before they can be called and providing the ability for Canada to meet the Government of Canada (GC) standards on API (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html).

7.2.9 Identity and Access Management

The Contractor must have the ability for Canada to support secure access to Cloud Services including ability to configure:

a) Multi-factor authentication in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3) using GC-approved credentials;
b) Role-based access;
c) Access controls on objects in storage; and
d) Granular authorization policies to allow or limit access.

The Contractor must have the ability to establish organization-wide defaults to manage tenant-wide policies.

7.2.10 Federation

The Contractor must have the ability for Canada to support federated identity integration including:

a) Support for open standards for authentication protocols such as Security Assertion Markup Language (SAML) 2.0 and/or OpenID Connect 1.0, or subsequent versions, where the End User credentials and authentication to cloud services are under the sole control of Canada; **and**
b) Ability to associate Canada's unique identifiers (e.g. an end-user unique ID, an end-user email address, etc.) with the corresponding Cloud Service user account(s).

7.2.11 Location of Employees - Remote Service Management

The Contractor must manage and monitor remote administration of the Contractor's Cloud Service that is used to host Organizational Data including, but not limited to the following measures:

a) Implementing multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);
b) 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

Cloud Services and Contractor Infrastructure;

Upon Canada's request, the Contractor must provide a document that describes the Contractor's approach and process for managing and monitoring remote administration of the Cloud Service(s).

7.2.12 **Logging and Auditing**

The Contractor must allow Canada to centrally review and analyze audit records from the Subscription Service components that include, but not limited to the following:

a) Forwarding Canada tenant events and logs to an RCMP and/or GC-managed centralized audit log system using standardized reporting interfaces, protocols, and data formats (e.g. Common Event Format (CEF), syslog, or other common log formats) and APIs that support log data remote retrieval (e.g. via a database interface using SQL, etc.).
b) The Contractor must provide Application Programming Interface(s) for the Subscription Service that allows Canada to:
    i) Inspect and interrogate data at rest; and
    ii) Export security event logs for the Solution(s); and
    iii) Assess events stored in application logs. This includes, but is not limited to events such as user access and behaviour, administrator access and behaviour, and changes to third-party API access, stored in application logs.

7.2.13 **Information Spillage**

The Contractor's Information Spillage process must include, at a minimum:

a) A process for notifying Canada of the potential for Information Spillage;
b) A process for identifying the specific data elements that is involved in a System's contamination;
c) A process to isolate and eradicate a contaminated System; and
d) A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination.

Upon Canada's request, the Contractor must provide a document that describes the Contractor's Information Spillage Response Process.

7.2.14 **Security Testing and Validation**

The Contractor must allow Internal Vulnerability Assessment testing to be conducted on an as and when required basis by Canada or a third party selected by Canada. This testing must be conducted at a minimum on a yearly basis and aligned to the Vulnerability Management controls in the RCMP Departmental Security Control Profile (RDSCP). The Contractor and Canada must agree on the assignment of responsibility for supporting Vulnerability Assessment testing.

7.2.15 **Background Checks/Personnel Security Screening**

The Contractor and its subcontractors and sub-subcontractors shall work with Canada or any authorized third-party, to identify roles within the Contractor's organization with elevated rights of access. Personnel occupying those roles may be subject to additional RCMP Personnel Security Screening processes. If Contractor employees with elevated rights of access do not qualify for appropriate RCMP Personnel Security Clearance levels identified, then the Contractor must provide the RCMP a plan for staffing the identified roles with personnel qualified to meet the identified RCMP Personnel Security Clearance thresholds.

7.2.16 Supply Chain Risk Management

In the situation where the Contractor is a Software as a Service (SaaS) provider using a GC-approved Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) provider that already complies with the Section 38 - Supply Chain Risk Management requirements, within 90 days of contract award, the SaaS provider using the GC-approved IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed in the GC-approved IaaS provider environment for a Supply Chain Integrity (SCI) review.

7.2.17 Ongoing Supply Chain Integrity Process

Addressing Security Concerns
Despite the previous sub-section, if Canada decides in its discretion that the identified security concern represents a threat to national security that is both serious and imminent, the Contracting Authority may require that the Contractor immediately cease deploying the identified Service(s) and/or Product(s) from the Contract according to a schedule determined by the Canada. However, prior to making a final determination in this regard, Canada will provide the Contractor with the opportunity to address the security concerns within 48 hours of receiving notice from the Contracting Authority. The Contractor may propose, for example, mitigation measures for Canada's consideration. Canada will make the final determination.

7.2.18 Industrial Security Program – Security Requirement for Canadian Suppliers

The Contractor must comply with the provisions of the:

a) Security Requirements Check List and security guide (if applicable);
b) Industrial Security Manual (Latest Edition);
c) OSS website: Security requirements for contracting with the Government of Canada, located at www.tpsgc-pwgsc.gc.ca/esc-src

7.3 Service Work Streams

7.3.1 Overview

The following work streams will be key responsibilities of the Contractor in the start-up, deployment, and operationalization of the BWC/DEMS Program:

- Onboarding planning
- Planning and implementation

- Training and organizational change management
- Deployment
- Operating phase
- Innovation and solution improvements
- Additional services

An overview of the work streams is provided in the sections below.

Further descriptions, scope, roles, responsibilities, current state information and requirements will be reviewed and refined with the ITQ Qualified Suppliers during the RFP phase.

7.3.2 **Onboarding planning**

It is expected that the Contractor will provide professional services to Canada to determine the most appropriate way to deploy the BWC and the DEMS nationally. This includes key considerations for the deployment to ensure optimal success and management risk. This should be drawn from experience in managing deployments of similar scope and scale to the deployment required by Canada. Included in the planning is support in defining the number of Canada resources required to support the successful onboarding process and the number of resources required on an ongoing basis to support the management of equipment, redaction and editing of digital information, and disclosure. Any associated deliverables will be further defined the any resulting bid solicitation, as applicable.

7.3.3 **Planning and implementation**

It is expected that the Contractor will provide implementation services including project management and planning; system, data and process design; solution implementation; configuration; linkages to Canada systems; and, testing and deployment. Also included in planning and implementation is support for business continuity planning and disaster recovery planning to ensure continuity of service during major disruptions (e.g. Power failure, loss of telecommunications, loss of internet connectivity, failure or disruption of key services, etc.).

7.3.4 **Training and organizational change management support**

It is expected that the Contractor will provide the expertise and resources to support the development of a change management and training plan based on experience with other similar sized solutions. This includes an overview of the key steps each division and detachment should undertake to prepare for the onboarding and check lists or readiness assessment to be completed prior to onboarding. It is also expected that the Contractor provides input to draft policies and procedures that are currently being used for BWCs and the management of digital evidence to align policies and procedures with industry leading practices where applicable. It is also expected that the Contractor will provide BWC and DEMS training tools and material that can be integrated into the broader officer training programs.

7.3.5 **Deployment**

7.3.5.1 **Initial deployment**

It is expected that the Contractor will support an initial deployment of BWCs to a rural, a remote, and an urban centre. This will include testing a number of elements including the BWCs, the DEMS, as well as the policies and procedures for how the BWC/DEMS is to be used. It is also expected that this initial deployment will test the organizational change management and training plans and tools that are developed.

7.3.5.2 **Adjustments based on initial deployment**

It is expected that a formal assessment will be completed by Canada of the initial deployment and that the Contractor will support any updates and changes required to the BWC/DEMS, procedures and training tools and material.

7.3.5.3 **Phased deployment**

It is expected that the Contractor will support a phased deployment of BWCs and DEMS across the country. The Contractor is expected to support the planning of this phased deployment and provide advice and guidance about the sequence and scale of each phase of deployment based on the learning from the initial deployment.

7.3.5.4 **Operating phase**

The Contractor will be expected to manage and support the BWC/DEMS services after each phase of the deployment, which will include a set of responsibilities that are outlined in the contract and a set of service standards that are also outlined in the contract.

7.3.5.5 **Innovation and service improvements**

It is expected that the Contractor will provide services to and work collaboratively with Canada to innovate and make improvements to the Service provided by the Contractor. This will include proposing new technologies or processes to improve Canada’s usage and benefits of the BWC and DEMS capabilities.

7.3.5.6 **Additional services**

The Contractor may be asked to provide additional services to the BWC/DEMS Program to address evolving requirements (e.g., professional services working with Canada to accommodate additional streams of evidence).

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED.