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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet RFI #3 for DEMS/Body Worn Cameras	
Solicitation No. - N° de l'invitation M7594-212120/D	**Date** 2021-04-01
Client Reference No. - N° de référence du client M7594-212120	**GETS Ref. No. - N° de réf. 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 2021-04-09 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

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée See Herein – Voir ci-inclus	**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**

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

Canada

REQUEST FOR INFORMATION No. 003

FOR

A NATIONAL DIGITAL EVIDENCE MANAGEMENT SYSTEM

AND

BODY WORN CAMERAS

FOR

THE ROYAL CANADIAN MOUNTED POLICE

M7594-212120/D

Request for Information No. 003 for

A National Digital Evidence Management System and

Body Worn Cameras

for

The Royal Canadian Mounted Police

TABLE OF CONTENTS

Request for Information No. 003

A National Digital Evidence Management System and

Body Worn Cameras for

The Royal Canadian Mounted Police

1. BACKGROUND AND PURPOSE

Public Works and Government Services Canada (PWGSC) has issued this third Request for Information (RFI), on behalf of the Royal Canadian Mounted Police (RCMP). The purpose of this RFI is to solicit feedback from Industry on draft Overview and High Level Description of the Requirement and evaluation criteria that will be included within the formal ITQ which will be published to qualify suppliers who will be able to bid on a future solicitation to acquire a National Digital Evidence Management System (DEMS) and Body Worn Cameras (BWC).

On October 20, 2020, PWGSC issued RFI #M7594-212120/A and on February 22, 2021, issued RFI #M7594-212120/B on behalf of the RCMP seeking industry feedback on a National Digital Evidence Management System and Body Worn Cameras. Canada also sought feedback on other evidence-gathering capabilities from suppliers who currently offer these important products, systems and services. As part of RFI process #M7594-212120/A, Canada held an Industry Engagement Information Session as well as one-on-one vendor demonstrations with industry.

RFI #M7594-212120/B was issued to seek additional feedback on a managed service approach for BWC and DEMS, costing methodologies and basis of payment structure, provision of services from Indigenous businesses, security considerations, accessibility requirements and other relevant questions. Responses and feedback received in response to both RFIs are being reviewed and summarized in Summary of Feedback and Outcomes Reports and will be published on BuyandSell.gc.ca as soon as they are finalized.

Notice #M7594-212120/C was issued on March 26, 2021 to inform the Industry that Canada intends to move forward with the issuance of an Invitation to Qualify (ITQ), which will be the first phase of the competitive procurement process.

2. RCMP MANDATE

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.

3. NATURE OF THIS REQUEST FOR INFORMATION

This RFI is a consultative initiative. Industry is requested to submit feedback and raise any concerns on the draft Overview and High Level Description of the Requirement and evaluation criteria found herein at Annex A and Annex B, respectively.

The draft Overview and High Level Description of the Requirement contains a broad description of the requirements, business tools and capabilities to be implemented, business outcomes and anticipated requirements to be included in the Request for Proposal (RFP). The draft ITQ evaluation criteria includes the

proposed ITQ mandatory requirements that will permit Canada to qualify suppliers that have the required experience and high level capacity to provide Canada with a software-as-a-service National Digital Evidence Management System and Body Worn Cameras as a managed service that will comply with Canada's requirements.

This RFI is neither a call for tender nor a Request for Proposal (RFP). No agreement or contract will be entered into directly pursuant to this RFI. The issuance of this RFI is not to be considered in any way a commitment by Canada, nor as authority to potential respondents to undertake any work that could be charged to Canada. This RFI is not to be considered as a commitment by Canada to issue a subsequent RFP or award contract(s) for the work described herein.

Participation in this RFI is encouraged, but is not mandatory. There will be no short-listing of potential firms for the purposes of undertaking any future work as a result of this RFI. Similarly, participation in this RFI is not a condition or prerequisite for the participation in any potential subsequent RFP, or other type of solicitation.

4. NATURE OF AN ITQ PROCESS (FOR INFORMATION)

An ITQ will be neither a call for tenders nor a solicitation. No contract will result from an ITQ. The ITQ is the first phase of the procurement process. Suppliers will be invited to pre-qualify in accordance to terms and conditions including mandatory requirements that will be contained in the ITQ in order to become Qualified Respondents (QR) for any later procurement phases. Only QRs will be permitted to bid on any subsequent solicitation issued under this procurement process. The issuance of an ITQ is not to be considered in any way a commitment by Canada or as authorization to potential participants to undertake any work, which could be charged to Canada. An ITQ may be partially or completely cancelled by Canada at any time, and therefore there is no guarantee of a subsequent procurement phase. Because an ITQ is not a tender, respondents and QR may withdraw from this procurement phase at any time. Respondents who meet all the ITQ mandatory criteria and requirements and terms and conditions will be considered a QR.

5. POLICIES, ACTS AND KEY INFORMATION

Annex C outlines policies, acts, and other key information that may be applicable under a competitive procurement process for National DEMS and BWC.

6. ACCESSIBLE PROCUREMENT

PWGSC's goal is to ensure that the goods and services the Government of Canada buys are inclusive by design and accessible by default. Considering accessibility in public procurements is now an obligation in the Treasury Board Contracting Policy and accessibility criteria must be included in the requirements for goods and services, where appropriate. For additional information, please refer to Annex C.

7. SECURITY REQUIREMENTS

The Royal Canadian Mounted Police (RCMP) (herein referred to as the client) has an immediate requirement for the provision of BODY WORN CAMERAS AND DIGITAL EVIDENCE MANAGEMENT SYSTEM. The requirement calls for a turnkey solution where the service provider will be required to provide the necessary hardware and cloud service as a software in a Government of Canada approved Protected B space for the retention and management of electronic evidence. The information that will be collected by RCMP agents via the solution is expected to be up to PROTECTED B level. As the CSP has not received a completed SRCL for this procurement, we are providing the attached draft security clauses based on our current understanding of the security requirement and may be subject to further change post ITQ. It is understood that supply chain integrity assessments will be conducted by

the Communications Security Establishment (CSE). The CSE will provide, directly to the client and the contract authority, the relevant clauses to cover this aspect in the procurement documents.

Prior to Contract Award:

Supply Chain Integrity and Ownership Assessment:

The Government of Canada reserves the right to conduct a supply chain integrity and ownership assessment on a supplier, requiring the supplier to provide information on their corporate structure, supply chain and financial information. In light of the national security sensitivity on this particular file, it has been determined that the Communications Security Establishment (CSE) will conduct a Supply Chain Integrity Assessment on those organizations who submit a bid in response to the Request for Proposal (RFP).

The PSPC Contract Security Program (CSP) and RCMP may also conduct assessments to ensure the protection of sensitive information and assets from unauthorized access which could compromise national security.

Cloud Software as a Service - IT Assessment Program:

To initiate the on-boarding process, the Supplier should contact the CCCS Client Services to receive a copy of the onboarding submission form and any additional information related to the CSP IT Assessment Program.

The Supplier must provide documentation that lists information on any third parties that could be used to perform any part of the supply chain that would provide Canada with the proposed Commercially Available Software as a Service whether they would be (i) subcontractors to the Supplier, or (ii) subcontractors to subcontractors of the Supplier down the chain, OR (iii) any subsidiaries or third parties.

After Contract Award:

Subcontracting and third party involvement:

For information purposes, should a prime supplier have a requirement to subcontract, please note that the security requirements on the subcontracting SRCL can be the same as the prime SRCL or lower when appropriate, but not higher.

When a security requirement exists, ***prime contractors wishing to subcontract or involve a third party must contact the CSP prior to issuing a subcontract*.**

Please consult Annex D for the draft security clauses.

National Security Exception: RCMP is in the process of requesting that the national security exceptions provided for in the trade agreements to which Canada is a party, current and future, be invoked with respect to this procurement. Therefore, if invoked, this procurement will be excluded from all of the obligations of the trade agreements, for each and all purposes.

8. HIGH LEVEL ACTIVITIES

These activities are provided to give industry an idea as to the previous and envisioned steps in the process.

Publication of RFI #1 – closed November 27, 2020
Publication of RFI #2 – closed March 17, 2021
Publication of Notice to Industry – published March 26, 2021
Publication of RFI #3 – this document

Publication of Formal ITQ – Spring 2021
Publication of Draft RFP – Summer 2021
Publication of RFP – Summer 2021
Contract Award – Summer 2021

9. RESPONSE COSTS

Canada will not reimburse any respondent for any expenses incurred in responding to this RFI.

10. TREATMENT OF RESPONSES

a) Use of Responses: Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify procurement strategies or any draft documents contained in this RFI. Canada will review all responses received by the RFI closing date. Canada may, in its discretion, review responses received after the RFI closing date.

b) A review team composed of representatives of the RCMP and PWGSC will review the responses. Canada reserves the right to hire any independent consultant, or use any Government resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

c) Canada may, in its discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response.

d) Responses and feedback received will may or may not be summarized in a Summary of Feedback and Outcomes Report and published on BuyandSell.gc.ca upon the completion of the RFI consultation activities.

e) Early responses will be considered and are encouraged.

f) Each respondent is solely responsible for ensuring its response is delivered on time, to the correct location.

g) Each respondent should ensure that its name, return address, the solicitation number and the closing date appear legibly on the outside of the response.

h) Responses to this RFI will not be returned.

11. CONFIDENTIALITY OF SUPPLIER RESPONSES

Although the information collected may be provided as commercial-in-confidence (and, if identified as such, will be treated accordingly by Canada), Canada may use the information to assist in drafting future solicitation or contract documents.

Respondents are encouraged to identify, in the information they share with Canada, any information that they feel is proprietary, third-party or personal. Please note that Canada may be obligated by law (e.g. in response to a request under the *Access of Information and Privacy Acts*) to disclose proprietary or commercially-sensitive information concerning a respondent.

Respondents should mark any portions of their response that they consider proprietary or confidential. Canada will handle the responses in accordance with the *Access to Information Act*.

12. FORMAT OF RESPONSES

Respondents are requested to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this RFI could be satisfied. Respondents are also invited to provide comments regarding the content, format and/or organization of any draft documents included in this RFI. Respondents should explain any assumptions they make in their responses.

Cover Page: If the response includes multiple volumes, respondents are requested to indicate on the front cover page of each volume the title of the response, the solicitation number, the volume number and the full legal name of the respondent.

Title Page: The first page of each volume of the response, after the cover page, should be the title page, which should contain:

- the title of the respondent's response and the volume number;
- the name and address of the respondent;
- the name, address and telephone number of the respondent's contact;
- the date; and
- the RFI number.

Numbering System: Respondents are requested to prepare their response using a numbering system corresponding to the one in this RFI. All references to descriptive material, technical manuals and brochures included as part of the response should be referenced accordingly.

13. ENQUIRIES AND SUBMISSION OF RFI RESPONSES

All enquires on this RFI must be directed to the PWGSC Contracting Authority.

Interested suppliers must note that all communication pertaining to the subject matter of this RFI shall exclusively be directed to the PWGSC Contracting Authority. Interested suppliers must refrain from communicating directly with RCMP stakeholders or with other Government of Canada representatives, regarding any aspect of this procurement process, including the subject matter described herein.

PWGSC Contracting Authority:

Kate Mulligan
Public Works and Government Services Canada
Email: TPSGC.PACCSGPN-APBWCDEMS.PWGSC@tpsgc-pwgsc.gc.ca

Time and Place for Submission of Responses: Suppliers interested in providing a response must deliver it by email to the PWGSC Contracting Authority email address identified above, by the time and date indicated on the information cover page of this RFI.

14. FAIRNESS MONITOR

The Government of Canada has engaged RFP Solutions Inc. as a Fairness Monitor (FM) for this procurement. The FM will, for example, observe the procurement process to ensure that PWGSC has acted in a fair and consistent manner during the entire process. The FM is under obligations pursuant to its contract with the Government of Canada to maintain the confidentiality of all information received as a result of its participation in this

procurement process. For the purpose of carrying out its FM-related obligations, the FM will be granted access to documentation generated and received by Canada pursuant to this RFI and any subsequent procurement activities undertaken during the procurement process.

15. QUESTIONS TO INDUSTRY

This RFI contains specific questions addressed to industry. Respondents are requested to answer the questions directly, and in a concise manner.

15.1 Please provide comments on the draft Overview and High Level Description of the Requirement at Annex A and advise Canada of any concerns or show-stoppers.

15.2 Please provide comments on the draft ITQ Evaluation Criteria at Annex B and advise Canada of any concerns or show-stoppers.

15.3 Please provide any additional comments not previously addressed.

ANNEX A

DRAFT OVERVIEW AND HIGH LEVEL DESCRIPTION OF THE REQUIREMENT

Content will be provided via an amendment to the RFI.

ANNEX B

DRAFT ITQ EVALUATION CRITERIA

1. Mandatory Requirements

1.1 Respondents must meet all of the mandatory requirements. In accordance with the ITQ, Canada may contact the customer reference for the referenced project(s) to validate Respondent's responses. Only the capabilities and experience of the Respondent will be considered when evaluating the response submitted to this ITQ.

2. Substantiation of Technical Compliance – Mandatory Evaluation Criteria

2.1. Respondents must respond to the corresponding mandatory requirements explaining, demonstrating, substantiating and justifying their experience and qualifications. Respondents are requested to utilize the unique number and associated title of each mandatory requirement in their responses. Respondents are requested to indicate where each mandatory requirement is met in their response by entering a reference to where it is located in their response (e.g. volume/binder number, page number, etc.). Respondent's responses to the mandatory requirements will be evaluated in accordance with the ITQ. The Phased Bid Compliance Process will apply to all mandatory technical criteria.

2.2. Respondents must only provide the required number of reference project(s) as indicated in each mandatory requirement. If more than the required number of reference project(s) is provided, Canada will decide in its discretion which projects will be evaluated.

Note to Industry:

For the purposes of obtaining feedback from industry on the draft ITQ mandatory evaluation criteria, the term Respondent is defined as:

- the person or entity (or, in the case of a joint venture, the persons or entities) submitting a Response perform a contract for goods, services or both. It does not include the parent, subsidiaries or other affiliates of the Respondent, or its subcontractors.

Criteria	Mandatory Technical Criteria	Evaluation	Proof Required
M1	**Body Worn Camera (BWC) Experience** The response must provide proof that the Respondent has been providing each of the following BWC services for each project reference, as of the closing date and time of the ITQ: 1) Supply and Distribution of BWCs 2) Support and Maintenance Services for the following: a) 24/7 Support/help response service (call, email or online) for equipment non-performance, errors or defects; 3) Training Services for both of the following: a) Train-the-trainer training b) Development of training aids such as online courses or reference materials The Respondent must have provided at least 7,000 BWCs for each project to a law enforcement organization.	Met/Not Met	To demonstrate they meet this requirement, the Respondent must provide a minimum of two (2) project examples, with one client reference per project where BWC services were provided for at least one (1) year* within the past five (5) years from the date of ITQ closing. Client references must include: • Name of organization • Contact information for reference person within organization • Description of services provided • Dates and period of time the services were provided *A year is defined as a twelve (12) month consecutive period ending on or before the closing date of the ITQ.
M2	**Digital Evidence Management System (DEMS) Experience** The response must provide proof that the Respondent has been providing each of the following DEMS services and capabilities for each project reference, as of the closing date and time of the ITQ: 1) Deployed as a SaaS model; 2) Capable of storing uploaded body worn camera audio and video; 3) Search and retrieval of digital evidence; 4) Redaction capability; 5) Implementation Services demonstrating how the Respondent supported the client with all of the following tasks: a) planning, b) configuration, c) testing and d) production rollout 6) Training Services for both of the following: a) Train-the-trainer training b) Development of training aids such as online courses or reference materials 7) Maintenance and Support Services for each of the following:	Met/Not Met	To demonstrate they meet this requirement, the Respondent must provide two (2) project examples, with one client reference per project where DEMS services were provided for at least one (1) year within the past five (5) years from the date of ITQ closing. • Client references must include: • Name of organization • Contact information forreference person within organization • Description of services provided • Dates and period of time the services were provided Note: Client references may be the same as those used for M1, but must respond to the requirements as described in M2.

	a) 24/7 support/help response service (call, email or online) for application performance issues, errors and defects; b) application corrective measures (e.g. bug fixes) and/or patches; and c) provision of ongoing application upgrades. The Respondent must have provided the DEMS services above to a minimum of 7,000 users for each project within a law enforcement organization.		
M3	**Integrated BWC and DEMS Service** The response must provide proof that the Respondent has been providing both BWCs and a DEMS to the same client as an integrated service as described below as of the closing date and time of the ITQ: 1) Automated upload of the body worn camera, audio and video, from the docking station to the DEMS must be supported. The Respondent must have provided this integrated service to a law enforcement organization with a minimum of 3,000 BWC and DEMS users.	Met/Not Met	To demonstrate they meet this requirement, the Respondent must provide one (1) project example, with one client reference where both BWC and DEMS services were provided for at least one (1) year* within the past five (5) years from the date of ITQ closing. Client references must include: • Name of organization • Contact information for reference person within organization • Description of services provided • Dates and period of time the services were provided *A year is defined as a twelve (12) month consecutive period ending onor before the closing date of the ITQ.
M4	The Respondent (or in the case of a joint venture, one of the persons or entities) must own the intellectual property for the proposed DEMS component necessary for the performance of the proposed service (excluding add-ons and extensions) to Canada, in order to allow for the Respondent to introduce and support product enhancements into the main commercial product to align with Government of Canada (GC) needs.	Met/Not Met	To demonstrate they meet this requirement, the Respondent must provide, in less than one page, a brief description of how they meet criteria.
M5	The Respondent must provide a roadmap to demonstrate that the BWC/DEMS service will be available in both of Canada's official languages (English and French).	Met/Not Met	To demonstrate they meet this requirement, the Respondent must provide a high level roadmap that contains the timelines for delivering key product features and capabilities in both of Canada's official languages

			(English and French) including technical support, user interface for DEMS, user interface for BWC, training, and product documentation.
M6	The Respondent must demonstrate that the DEMS component of the proposed service is offered through a Software as a Service (SaaS) model as defined by National Institute of Standards and Technology special publication 800-145.	Met/Not Met	To demonstrate they meet this requirement, the Respondent must provide, in less than one page, a brief description of how they meet criteria.
M7	The Respondent must demonstrate that they have read and understand the accessibility requirements as outlined in the following: • Web Content Accessibility Guidelines (WCAG) 2 standards as described at the following link: https://www.w3.org/TR/WCAG21/ • Government of Canada Standard on Web Accessibility as described at the following link: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601 • Accessibility Strategy for the Public Service of Canada as described at the following link: https://www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/diversity-inclusion-public-service/accessibility-public-service/accessibility-strategy-public-service-toc.html	Met/Not Met	To demonstrate they meet this requirement, the Respondent must acknowledge that they have read and understand the accessibility requirements as outlined in the Web Content Accessibility Guidelines (WCAG) 2 standards, Government of Canada Standard on Web Accessibility, and the Accessibility Strategy for the Public Service of Canada.
M8	The Respondent must demonstrate that the DEMS component of the proposed service can be deployed on 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	Met/Not Met	To demonstrate they meet this criteria, the Respondent must provide a description of how they are currently deployed on one of the approved CSPs or provide a roadmap showing how they will onboard to one of the approved CSPs by contract award.

ANNEX C

POLICIES, ACTS AND KEY INFORMATION

This following section highlights the various policies, acts and key information that may need to be taken into consideration.

1. Resulting Contract

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.

2. Digital Standards and Policy

a) Government of Canada Digital Standards (https://www.canada.ca/en/government/system/digital-government/government-canada-digital-standards.html) form the foundation of the government's shift to becoming more agile, open, and user-focused. They guide teams in designing digital services in a way that best serves Canadians.

b) The Policy on Service and Digital (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603) - Serves as an integrated set of rules that articulate how GC organizations manage service delivery, information and data information technology, and cyber security in the digital era.

3. Interoperability Standards

Standards on Application Programming Interfaces (APIs) (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html) - The standards govern how APIs are to be developed within and for the GC to better support integrated digital processes across departments and agencies.

4. Cloud Computing and Data Sovereignty

Government of Canada White Paper: Data Sovereignty and Public Cloud (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html) - The purpose of this paper is to provide an overview of the risks to data sovereignty that is associated with using commercial public cloud environments. The risks to data residency and security are also discussed. These risks are examined in the context of the GC's cloud-first strategy. By the end of this paper, the reader will understand these risks and the associated mitigation measures. The reader will also understand how cloud services can help the GC address other risks, such as: aging IT, current security gaps and not benefiting from emerging technology.

5. Privacy

a) Interim Policy on Privacy Protection (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510) - The objectives of this interim policy are as follows: to facilitate statutory and regulatory compliance, and to enhance effective application of the Privacy Act and its Regulations by government institutions; to ensure consistency in practices and procedures in administering the Act and Regulations; and to

ensure effective protection and management of personal information and mitigating privacy risks in government programs and activities.

b) Access to Information (https://laws.justice.gc.ca/eng/acts/A-1/index.html) An Act to extend the present laws of Canada that provide access to information under the control of the Government of Canada

c) Privacy Act (https://laws.justice.gc.ca/eng/acts/P-21/index.html) - An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to personal information about themselves.

6. Security Policy

Policy on Government Security (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578) - Provides direction to manage government security in support of the trusted delivery of GC programs and services, the protection of information, individuals and assets, and provides assurance to Canadians, partners, oversight bodies and other stakeholders regarding security management in the GC.

7. Accessibility

a) Standard on Web Accessibility (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601) The objective of this standard is to ensure a high level of Web accessibility is applied uniformly across Government of Canada websites and web applications.

b) Accessibility Strategy for the Public Service of Canada (https://www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/diversity-inclusion-public-service/accessibility-public-service/accessibility-strategy-public-service-toc.html) - The Strategy outlines how the vision of the GC being the most accessible and inclusive public service in the world and how the guiding principles of Nothing without us, collaboration, sustainability, and transparency are to be implemented.

c) Accessible Canada Act (https://www.parl.ca/DocumentViewer/en/42-1/bill/C-81/royal-assent) – The Accessible Canada Act was enacted into law in order to enhance the full and equal participation of all persons, especially persons with disabilities, in society. This is to be achieved through the realization, within the purview of matters coming within the legislative authority of Parliament, of a Canada without barriers, particularly by the identification, removal and prevention of barriers.

d) Web Content Accessibility Guidelines (http://www.w3.org/TR/WCAG21/) – The Web Content Accessibility Guidelines (WCAG) 2.1 covers a wide range of recommendations for making Web content more accessible. Following these guidelines will make content more accessible to a wider range of people with disabilities, including accommodations for blindness and low vision, deafness and hearing loss, limited movement, speech disabilities, photosensitivity, and combinations of these, and some accommodation for learning disabilities and cognitive limitations; but will not address every user need for people with these disabilities. These guidelines address accessibility of web content on desktops, laptops, tablets, and mobile devices.

e) Guideline on Making Information Technology Usable by All (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32620) - This guideline supports the Government of Canada's direction to ensure that departments, agencies and organizations consider accessibility in the acquisition or development of information technology (IT) solutions and equipment to make IT usable by all.

8. Official Languages

The Official Languages Act (OLA) (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26160) reaffirms the equality of the status of English and French as the official languages of Canada and establishes equal rights and privileges as to their use in institutions. The policy's objective is to facilitate compliance with and ensure effective implementation of the OLA and its Refutations by institutions.

9. Nunavut Settlement Area (NSA)

The Directive on Government Contracts, Including Real Property Leases, in the Nunavut Settlement Area (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32610) ensures that government contracting in the Nunavut Settlement Area will meet the Government of Canada's obligations under Article 24 of the Nunavut Agreement.

10. Comprehensive Land Claim Agreements

Modern treaties, also known as Comprehensive Land Claim Agreements (CLCAs), (https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/9#section-9.35) are typically tripartite, including Indigenous organizations or nations, the Crown, and provincial/territorial governments as signatories. They provide clarity and predictability with respect to land and resource rights, ownership, and management. Modern treaties/CLCAs also seek to ensure fair treatment of Indigenous interests with respect to cultural, social, political and economic rights, including rights to lands, and to fish and hunt and practice their own cultures. The rights defined in them are constitutionally protected within section 35 of the *Constitution Act*, 1982.

ANNEX D

DRAFT SECURITY REQUIREMENTS

DOMESTIC SUPPLIER CLAUSES:

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER:
PWGSC FILE No. BODY WORN CAMERAS AND DIGITAL EVIDENCE MANAGEMENT SYSTEM

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid **Designated Organization Screening (DOS)** with approved Document Safeguarding at the level of **PROTECTED B**, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

2. The Contractor/Offeror personnel requiring access to **PROTECTED** information, assets or sensitive site(s) must EACH hold a valid personnel security screening at the level of **RELIABILITY STATUS or, as required**, **SECRET,** granted or approved by the CSP, PWGSC.

3. The Contractor **MUST NOT** utilize its Information Technology systems to electronically process, produce or store **PROTECTED** information until the CSP, PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of **PROTECTED B**.

4. The prime Contractor/Offeror may subcontract or use third parties in the performance of the Work, provided that (a) the Contractor obtains the Contracting Authority's prior written consent, (b) written permission is provided from the CSP, PWGSC, (c) the subcontractor or third party provider is bound by the terms of this Contract, (d) the Contractor remains liable to Canada for all the Work performed by the subcontractor or third party subcontractor/Offeror.

5. Any Contractor/Offeror/sub-contractor or third party delivering Cloud services must be approved by the Government of Canada and comply with the security requirements in the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM) for the scope of the proposed Commercially Available Software as a Service provided. Compliance will be validated and verified through the Canadian Centre for Cyber Security (CCCS) Cloud Service Provider (CSP) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100). Any Supplier that has participated in the process must provide documentation to confirm that they have completed the on-boarding 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. This will accelerate the qualification process and at the same doesn't require the Supplier to demonstrate the compliance.

6. The Contractor/Offeror must comply with the provisions of the:

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

NOTE: There are **multiple levels of personnel security screenings** associated with this file. In this instance, a Security Classification Guide must be added to the SRCL clarifying these screenings. The Security Classification Guide is normally generated by the organization's project authority and/or security authority.

FOREIGN SUPPLIER CLAUSES:

Note: For Cloud software as a service up to Protected B level, the infrastructure has to reside entirely within Canada.

SECURITY REQUIREMENTS FOR FOREIGN SUPPLIER:

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation:

The Canadian Designated Security Authority (Canadian DSA) is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD). The Canadian DSA is the authority for confirming **Contractor/Subcontractor** compliance with the security requirements for foreign suppliers. The following security requirements apply to the foreign recipient **Contractor/Subcontractor** incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing outside of Canada the Work described in the Cloud Solutions, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified in the Section entitled Protection and Security of Data Stored in Databases.

1. The Foreign recipient **Contractor/Subcontractor** must be from one of the following countries: Australia, New Zealand, United Kingdom and the United States. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.
2. The Foreign recipient **Contractor/Subcontractor** must at all times during the performance of the **contract/subcontract** be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country(ies) in which it is incorporated or operating and authorized to do business. The Foreign recipient **Contractor/Subcontractor** must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and the Canadian DSA, and identify the relevant national Privacy Authority. For European **Contractors/ Subcontractors**, this will be the national Data Protection Authority (DPA).
3. The Foreign recipient **Contractor/Subcontractor** must, at all times during the performance of the **contract/subcontract**, hold an equivalence to a valid Designated Organization Screening (DOS), issued by the Canadian DSA as follows:

i. The Foreign recipient **Contractor/Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.

ii. The Foreign recipient **Contractor/Subcontractor** must not begin the work, services or performance until the Canadian Designated Security Authority (DSA) is satisfied that all contract security requirement conditions have been met. Canadian DSA confirmation must be provided, in writing, to the foreign recipient **Contractor/Subcontractor** in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.

iii. The Foreign recipient **Contractor/Subcontractor** must identify an authorized Contract Security Officer (CSO) and an Alternate Contract Security Officer (ACSO) (if applicable) to be responsible for the

overseeing of the security requirements, as defined in this contract. This individual will be appointed by the proponent foreign recipient **Contractor's/Subcontractor's** Chief Executive officer or Designated Key Senior Official, defined as an owner, officer, director, executive, and or partner who occupy a position which would enable them to adversely affect the organization's policies or practices in the performance of the contract.

iv. The Foreign recipient **Contractor/Subcontractor** must not grant access to **CANADA PROTECTED** information/assets, except to its personnel subject to the following conditions:

a. Personnel have a need-to-know for the performance of the **contract/subcontract**;

b. Personnel have been subject to a Criminal Record Check, with favourable results, from a recognized governmental agency or private sector organization in **their country** as well as a Background Verification, validated by the Canadian DSA;

c. The Foreign recipient **Contractor/Subcontractor** must ensure that personnel provide consent to share results of the Criminal Record and Background Checks with the Canadian DSA and other Canadian Government Officials, if requested; and

d. The Government of Canada reserves the right to deny access to **CANADA PROTECTED** information/assets to a foreign recipient **Contractor/Subcontractor** for cause.

4. **CANADA PROTECTED/PERSONAL** information/assets, provided to the foreign recipient **Contractor/Subcontractor** or produced by the Foreign recipient **Contractor/Subcontractor**, must:

a. not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the **contract / subcontract**, without the prior written consent of Canada. Such consent must be sought from its national DPA, the Contracting Authority (in collaboration with the Canadian DSA); and

b. not be used for any purpose other than for the performance of the **contract/subcontract** without the prior written approval Canada. This approval must be obtained by contacting its national DPA, the Contracting Authority (in collaboration with the Canadian DSA).

5. The Foreign recipient **Contractor/Subcontractor** MUST NOT remove **CANADA PROTECTED** information/assets from the identified work site(s), and the foreign recipient **Contractor/ Subcontractor** must ensure that its personnel are made aware of and comply with this restriction.

6. The Foreign recipient **Contractor/Subcontractor** must not use the **CANADA PROTECTED** information/assets for any purpose other than for the performance of the **contract/subcontract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

7. The Foreign recipient **Contractor/Subcontractor** must, at all times during the performance of the **contract/subcontract** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED B**.

All **CANADA PROTECTED** information/assets, furnished to the foreign recipient **Contractor/Subcontractor** or produced by the foreign recipient **Contractor/Subcontractor**, must also be safeguarded as follows:

8. The Foreign recipient **Contractor/Subcontractor** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information/ assets pursuant to this **contract/subcontract** has been compromised.

OR

9. The Foreign recipient **Contractor/Subcontractor** must immediately report to its respective national DPA and the Contracting Authority (in collaboration with the Canadian DSA), all cases in which it is known or there is reason to suspect that any Personal Information provided or generated pursuant to this **contract/subcontract** have been lost, or in contravention of these security requirements, accessed, used or disclosed to unauthorized persons.
10. The Foreign recipient **Contractor/Subcontractor** must not disclose **CANADA PROTECTED** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent must be sought through the Canadian DSA.
11. The Foreign recipient **Contractor/Subcontractor** must provide the **CANADA PROTECTED** information/ assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the Canadian DSA.
12. Upon completion of the Work, the foreign recipient **Contractor/Subcontractor** must return to the Government of Canada, all **CANADA PROTECTED** information/assets furnished or produced pursuant to this **contract/subcontract**, including all **CANADA PROTECTED** information/assets released to and/or produced by its subcontractors.
13. The Foreign recipient **Contractor/Subcontractor** requiring access to **CANADA PROTECTED** information/assets or Canadian restricted sites, under this contract, must submit a Request for Site Access to the Chief Security Officer of the Royal Canadian Mounted Police**.**
14. The Foreign recipient **Contractor/Subcontractor** MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system and transfer via an IT link any **CANADA PROTECTED B** information until authorization to do so has been confirmed by the Canadian DSA.
15. The Foreign recipient **Contractor/Subcontractor** must ensure that all the databases including the backup database used by organizations to provide the services described in the proposed Cloud Solutions, containing any **CANADA PROTECTED** Information, related to the Work, are located within Canada.
16. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the Canadian DSA.
17. All Subcontracts awarded to a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.
18. All Subcontracts awarded by a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.
19. Any third party supplier that will require access to CANADA PROTECTED information as part of this contract must adhere to all of the security requirements outlined in this contract.
20. The Foreign recipient **Contractor/Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex _____.
21. Canada has the right to reject any request to electronically access, process, produce, transmit or store **CANADA PROTECTED** information/assets related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

Protection and Security of Data Stored in Databases

1. The foreign recipient **Contractor/Subcontractor** must ensure that all the databases used by organizations to provide the services described in the proposed Cloud Solutions containing any Personal Information, related to the Work, are located in Canada.
2. The foreign recipient **Contractor/Subcontractor** must control access to all databases on which any data relating to the **contract/subcontract** is stored so that only individuals with the appropriate security screening are able to access the database, either by using a password or other form of access control (such as biometric controls).
3. The foreign recipient **Contractor/Subcontractor** must ensure that all databases on which any data relating to the **contract/subcontract** is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases.
4. The foreign recipient **Contractor/Subcontractor** must ensure that all data relating to the **contract/subcontract** is processed only in Canada or in another country approved by the Contracting Authority under subsection 1.
5. The foreign recipient **Contractor/Subcontractor** must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada, unless the Contracting Authority has first consented in writing to an alternate route. The Contracting Authority will only consider requests to route domestic traffic through another country that meets the requirements of subsection 1.
6. Despite any section of the General Conditions relating to subcontracting, the foreign recipient **Contractor/Subcontractor** must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the contract unless the Contracting Authority (in collaboration with the Canadian DSA) first consents in writing.

Personal Information

Interpretation

In the **contract/subcontract**, unless the context otherwise requires,

"General Conditions" means the general conditions that form part of the **contract/subcontract**;

"Personal Information" means information about an individual, including the types of information specifically described in the *Privacy Act*, R.S. 1985, c. P-21;

"Record" means any hard copy document or any data in a machine-readable format containing Personal Information;

Words and expressions defined in the General Conditions and used in these supplemental general conditions have the meanings given to them in the General Conditions.

If there is any inconsistency between the General Conditions and these Personal Information articles, these Personal Information articles prevail.

Ownership of Personal Information and Records

To perform the Work, the foreign recipient **Contractor/Subcontractor** will be provided with and/or will be collecting Personal Information from third parties. The foreign recipient **Contractor/Subcontractor** acknowledges that it has no rights in the Personal Information or the Records and that Canada owns the Records. On request, the foreign recipient **Contractor/Subcontractor** must make all the Personal Information and Records available to Canada immediately in a format acceptable to Canada.

Use of Personal Information

The foreign recipient **Contractor/Subcontractor** agrees to create, collect, receive, manage, access, use, retain and dispose of the Personal Information and the Records only to perform the Work in accordance with the **contract/subcontract**.

Collection of Personal Information

1. If the foreign recipient **Contractor/Subcontractor** must collect Personal Information from a third party to perform the Work, the foreign recipient **Contractor/Subcontractor** must only collect Personal Information that is required to perform the Work. The foreign recipient **Contractor/Subcontractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor/Subcontractor** must inform that individual (at or before the time when it collects the Personal Information) of the following:
   a. that the Personal Information is being collected on behalf of, and will be provided to, Canada;
   b. the ways the Personal Information will be used;
   c. that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement;
   d. the consequences, if any, of refusing to provide the information;
   e. that the individual has a right to access and correct his or her own Personal Information; and
   f. that the Personal Information will form part of a specific personal information bank (within the meaning of the *Privacy Act*), and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the foreign recipient **Contractor/Subcontractor**.
2. The foreign recipient **Contractor/Subcontractor**, and their respective employees must identify themselves to the individuals from whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.
3. If requested by the Contracting Authority, the foreign recipient **Contractor/Subcontractor** must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The foreign recipient **Contractor/Subcontractor** must not begin using the form or script unless the Contracting Authority first approves it in writing. The Contractor must also obtain the Contracting Authority's approval before making any changes to a form or script.
4. At the time it requests Personal Information from any individual, if the foreign recipient **Contractor/Subcontractor** doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the foreign recipient **Contractor/Subcontractor** must ask the Contracting Security Authority for instructions.

Maintaining the Accuracy, Privacy and Integrity of Personal Information

The foreign recipient **Contractor/Subcontractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The foreign recipient **Contractor/Subcontractor** must protect the

privacy of the Personal Information. To do so, at a minimum, the foreign recipient **Contractor/Subcontractor** must:

a. not use any personal identifiers (e.g. social insurance number) to link multiple databases containing Personal Information;

b. segregate all Records from the foreign recipient **Contractor's/Subcontractor's** own information and records;

c. restrict access to the Personal Information and the Records to people who require access to perform the Work (for example, by using passwords or biometric access controls);

d. provide training to anyone to whom the foreign recipient **Contractor/Subcontractor** will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the Work. The foreign recipient **Contractor/Subcontractor** must provide this training before giving an individual access to any Personal Information and the foreign recipient **Contractor / Subcontractor** must keep a record of the training and make it available to the Contracting Authority if requested;

e. if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the foreign recipient **Contractor/Subcontractor** provides access to the Personal Information to acknowledge in writing (in a form approved by the Contracting Authority) their responsibilities to maintain the privacy of the Personal Information;

f. keep a record of all requests made by an individual to review his or her Personal Information, and any requests to correct errors or omissions in the Personal Information (whether those requests are made directly by an individual or by Canada on behalf of an individual);

g. include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient **Contractor/Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor/Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Subcontractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

h. keep a record of the date and source of the last update to each Record;

i. maintain an audit log that electronically records all instances of and attempts to access Records stored electronically. The audit log must be in a format that can be reviewed by the foreign recipient **Contractor/Subcontractor** and Canada at any time; and

j. secure and control access to any hard copy Records.

Safeguarding Personal Information

The foreign recipient **Contractor/Subcontractor** must safeguard the Personal Information at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality. To do so, at a minimum, the foreign recipient **Contractor/Subcontractor** must:

a. store the Personal Information electronically so that a password (or a similar access control mechanism, such as biometric access) is required to access the system or database in which the Personal Information is stored;

b. ensure that passwords or other access controls are provided only to individuals who require access to the Personal Information to perform the Work;

c. not outsource the electronic storage of Personal Information to a third party (including an affiliate) unless the Canadian DSA has first consented in writing;

d. safeguard any database or computer system on which the Personal Information is stored from external access using methods that are generally used, from time to time, by prudent public and private sector organizations in Canada in order to protect highly secure or sensitive information;

e. maintain a secure back-up copy of all Records, updated at least weekly;

f. implement any reasonable security or protection measures requested by Canada from time to time; and

g. notify the Contracting Authority and the Canadian DSA immediately of any security breaches; for example, any time an unauthorized individual accesses any Personal Information.

Appointment of Privacy Officer

The foreign recipient **Contractor/Subcontractor** must appoint someone to be its privacy officer and to act as its representative for all matters related to the Personal Information and the Records. The foreign recipient **Contractor/Subcontractor** must provide that person's name to the Contracting Authority and the Canadian DSA within ten (10) days of the award of the **contract/subcontract**.

Quarterly Reporting Obligations

Within 30 calendar days of the end of each quarter (January-March; April-June; July-September; October-December), the foreign recipient **Contractor/Subcontractor** must submit the following to the Contracting Authority:

a. a description of any new measures taken by the foreign recipient **Contractor/Subcontractor** to protect the Personal Information (for example, new software or access controls being used by the foreign recipient **Contractor/Subcontractor**);

b. a list of any corrections made to Personal Information at the request of an individual (including the name of the individual, the date of the request, and the correction made);

c. details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the foreign recipient **Contractor/Subcontractor**; and

d. a complete copy (in an electronic format agreed to by the Contracting Authority and the foreign recipient **Contractor/Subcontractor**) of all the Personal Information stored electronically by the foreign recipient C**ontractor/Subcontractor**.

Threat and Risk Assessment

Within ninety (90) calendar days of the award of the **contract/subcontract** and, if the **contract/subcontract** lasts longer than one year, within thirty (30) calendar days of each anniversary date of the **contract/subcontract**, the foreign recipient **Contractor/Subcontractor** must submit to the Contracting Authority and the Canadian DSA a threat and risk assessment, which must include:

a. a copy of the current version of any request for consent form or script being used by the foreign recipient **Contractor/Subcontractor** to collect Personal Information;

b. a list of the types of Personal Information used by the foreign recipient **Contractor/Subcontractor** in connection with the Work;

c. a list of all locations where hard copies of Personal Information are stored;

d. a list of all locations where Personal Information in machine-readable format is stored (for example, the location where any server housing a database including any Personal Information is located), including back-ups;

e. a list of every person to whom the foreign recipient **Contractor/Subcontractor** has granted access to the Personal Information or the Records;

f. a list of all measures being taken by the foreign recipient **Contractor/Subcontractor** to protect the Personal Information and the Records;

g. a detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and

h. an explanation of any new measures the foreign recipient **Contractor/Subcontractor** intends to implement to safeguard the Personal Information and the Records.

Audit

Canada may audit the foreign recipient **Contractor's/Subcontractor's** compliance with these supplemental general conditions at any time. If requested by the Contracting Authority, the foreign recipient **Contractor/Subcontractor** must provide Canada (or Canada's authorized representative) with access to its premises and to the Personal Information and Records at all reasonable times. If Canada identifies any deficiencies during an audit, the foreign recipient **Contractor/Subcontractor** must immediately correct the deficiencies at its own expense.

Statutory Obligations

1. The foreign recipient **Contractor/Subcontractor** acknowledges that Canada is required to handle the Personal Information and the Records in accordance with the provisions of Canada's *Privacy Act, Access to Information Act,* R.S. 1985, c. A-1, and *Library and Archives of Canada Act,* S.C. 2004, c. 11. The foreign recipient **Contractor/Subcontractor** agrees to comply with any requirement established by the Contracting Authority that is reasonably required to ensure that Canada meets its obligations under these acts and any other legislation in effect from time to time.

2. The foreign recipient **Contractor/Subcontractor** acknowledges that its obligations under the **contract/subcontract** are in addition to any obligations it has under the *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5, or similar legislation in effect from time to time in any province or territory of Canada. If the foreign recipient **Contractor/Subcontractor** believes that any obligations in the **contract/subcontract** prevent it from meeting its obligations under any of these laws, the foreign recipient **Contractor/Subcontractor** must immediately notify the Contracting Authority of the specific provision of the **contract/subcontract** and the specific obligation under the law with which the foreign recipient **Contractor/Subcontractor** believes it conflicts.

Disposing of Records and Returning Records to Canada

The foreign recipient **Contractor/Subcontractor** must not dispose of any Record, except as instructed by the Contracting Authority. On request by the Contracting Authority, or once the Work involving the Personal Information is complete, the **contract/subcontract** is complete, or the **contract/subcontract** is terminated, whichever of these comes first, the foreign recipient **Contractor/Subcontractor** must return all Records (including all copies) to the Contracting Authority.

Legal Requirement to Disclose Personal Information

Before disclosing any of the Personal Information pursuant to any applicable legislation, regulation, or an order of any court, tribunal or administrative body with jurisdiction, the foreign recipient **Contractor/Subcontractor** must immediately notify the Contracting Authority, in order to provide the Contracting Authority with an opportunity to participate in any relevant proceedings.

Complaints

Canada and the foreign recipient **Contractor/Subcontractor** each agree to notify the other immediately if a complaint is received under the *Access to Information Act* or the *Privacy Act* or other relevant legislation regarding the Personal Information. Each Party agrees to provide any necessary information to the other to assist in responding to the complaint and to inform the other immediately of the outcome of that complaint.

Exception

The obligations set out in these supplemental general conditions do not apply to any Personal Information that is already in the public domain, as long as it did not become part of the public domain as a result of any act or omission of the Contractor or any of its subcontractors, agents, or representatives, or any of their employees.

SECURITY REQUIREMENT FOR ADMINISTRATIVE / PRIVILEGED ACCESS

SECRET

The contractor and/or any and all subcontractors must be from a country with which Canada has an international bilateral industrial security instrument or will have such an instrument with Canada by the end of the bidding period. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.

1. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of the **Contract / Standing Offer / Subcontract**, hold a valid Facility Security Clearance (FSC), issued by the National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country**, at the equivalent level of **SECRET**, and hold an approved Document Safeguarding Capability Clearance **and Production Capabilities** at the level of **SECRET**
2. All **CANADA PROTECTED / CLASSIFIED** information/assets provided or generated under this **Contract / Standing Offer / Subcontract** will continue to be safeguarded in the event of withdrawal by the recipient party or upon termination of the **Contract / Standing Offer / Subcontract**, in accordance with the National legislation, regulations and policies of **the supplier's country.**
3. The Foreign recipient **Contractor / Offeror / Subcontractor** shall provide the **CANADA PROTECTED / CLASSIFIED** information/assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Security legislation, regulations, policies and as prescribed by the National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country.**
4. All **CANADA PROTECTED / CLASSIFIED** information/assets provided to the Foreign recipient **Contractor / Offeror / Subcontractor** pursuant to this **Contract / Standing Offer / Subcontract** by the Government of Canada, shall be marked by the Foreign recipient **Contractor / Offeror / Subcontractor** with the equivalent

security classification utilized by **the supplier's country** and in accordance with the National legislation, regulations and policies of **the supplier's country**.

5. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of this **Contract / Standing Offer / Subcontract**, ensure the transfer of **CANADA PROTECTED / CLASSIFIED** information/assets be facilitated in accordance with the National legislation, regulations and policies of **the supplier's country,** and in compliance with the provisions of the Bilateral Industrial Security Instrument between **the supplier's country** and Canada.
6. Upon completion of the work, the Foreign recipient **Contractor / Offeror / Subcontractor** shall return to the Government of Canada, via government-to-government channels, all **CANADA PROTECTED / CLASSIFIED** information/assets furnished or produced pursuant to this **Contract / Standing Offer / Subcontract**, including all **CANADA PROTECTED / CLASSIFIED i**nformation/assets released to and/or produced by its subcontractors, unless otherwise authorised in writing by the Canadian DSA.
7. Subcontracts which contain security requirements are **NOT** to be awarded without the prior written permission of **their respective National Security Authority (NSA) or Designated Security Authority (DSA), in accordance with the National legislation, regulations and policies of the supplier's country / the Canadian DSA.**
8. The Foreign recipient **Contractor / Offeror / Subcontractor** MUST NOT utilize its Information Technology systems to electronically process, produce, or store on a computer system **and transfer via an IT link** any **CANADA PROTECTED / CLASSIFIED** information/assets until the National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country** has granted approval to do so. After approval has been granted in writing to the Foreign recipient **Contractor / Offeror / Subcontractor**, these tasks may be performed up to the level of **SECRET.**
9. The Foreign recipient **Contractor / Offeror / Subcontractor** shall not use the **CANADA PROTECTED / CLASSIFIED** information/assets for any purpose other than for the performance of the **Contract / Standing Offer / Subcontract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.
10. The Foreign recipient **Contractor / Offeror / Subcontractor** visiting Canadian Government or industrial facilities, under this contract, will submit for approval a Request for Visit form to Canada's Designated Security Authority (DSA) through their respective National Security Authority (NSA) or Designated Security Authority (DSA).
11. The Foreign recipient **Contractor / Offeror / Subcontractor** shall immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED / CLASSIFIED** information/assets pursuant to this **Contract / Standing Offer / Subcontract** has been compromised.
12. The Foreign recipient **Contractor / Offeror / Subcontractor** shall not disclose **CANADA PROTECTED / CLASSIFIED** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent shall be sought through the {recipient's National Security Authority/ Designated Security Authority (NSA/DSA) / Canadian DSA}.
13. The Foreign recipient **Contractor / Offeror / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex _____.