

# KEY DOCUMENTS

## Table of Contents

<b>ANNEX A - STATEMENT OF WORK .....</b>	<b>1</b>
<b>ATTACHMENT 1 - MANDATORY TECHNICAL CRITERIA .....</b>	<b>40</b>
<b>ATTACHMENT 2 - POINT RATED TECHNICAL CRITERIA .....</b>	<b>45</b>
<b>ATTACHMENT 3 - PRICING SCHEDULE .....</b>	<b>52</b>
<b>APPENDIX 1 – ACRONYMS AND GLOSSARY .....</b>	<b>55</b>
<b>APPENDIX 2 – SERVICE LEVEL REQUIREMENTS .....</b>	<b>56</b>
<b>APPENDIX 3 – VOLUMES .....</b>	<b>58</b>
<b>APPENDIX 4 – IT SECURITY CONTROLS .....</b>	<b>60</b>

DRAFT

## ANNEX A - STATEMENT OF WORK

### 1. Title

Hosting and Operations Services and Related Development Tasks for the Multi-jurisdictional Registry Access Service (MRAS)

### 2. Objective

Innovation, Science and Economic Development Canada (ISED) has a requirement for a Contractor to provide the following services:

- Deploy and render functional the current version of MRAS (MRAS System 1.0, supplied as government furnished equipment) in the Contractor's environment utilizing an Approved Government of Canada Cloud Brokering Service;
- Host, operate and maintain MRAS; and
- Continue developing and enhancing MRAS through Related Development Tasks.

### 3. Background

#### 3.1. Strategic objectives

The federal government, in collaboration with the provinces and territories, is working toward digitally connecting all 14 of Canada's business registries (10 provinces, three territories and the federal government) to enable the exchange of business information. Connecting the business registries reduces barriers to internal trade and improves the competitiveness of Canadian businesses. It supports:

- business growth and market access across Canada; and
- those transacting with a business to verify its status.

#### 3.2. High-level description of MRAS System 1.0

MRAS System 1.0 (more particularly described in Section 5 – Technical Environment) is a shared interoperability solution that was developed to achieve these strategic objectives. It currently allows eight business registries (the Participating Business Registries) to exchange business information confidently and efficiently. The other six business registries (the Remaining Business Registries) collaborated in the development of MRAS System 1.0 but are not yet actively interoperating with it. The Participating Business Registries currently are: British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, Nova Scotia and Corporations Canada (federal). The Remaining Business Registries are: New Brunswick, Prince Edward Island, Newfoundland and Labrador, Yukon, Northwest Territories and Nunavut.

MRAS System 1.0 supports three main capabilities:

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

- streamlined extra-provincial/territorial registration – a real-time transaction that allows a business to retrieve its core information from its Home Jurisdiction business registry and use it to complete the registration process in another jurisdiction;
- automated notifications of changes to business information – a related capability that ensures that changes made by a business in its Home Jurisdiction business registry are communicated to any other business registry associated to that business; and
- unified search – a service that allows the public to search for a business across business registries instead of having to search each business registry individually.

These three main capabilities are enabled by an entity correlation capability. The entity correlation capability uses business identifiers to match business records and establish links among the Participating Business Registries that are associated with a particular business. This enables the automated notifications of changes to business information and provides a more accurate representation of a business in unified search.

Additionally, MRAS System 1.0 includes a virtual registry capability. The virtual registry capability is an external component of MRAS System 1.0. It was developed to provide a basic web-based business registry capability to enable one of the Participating Business Registries that did not have online extra-provincial/territorial registration services, to fully interoperate with MRAS System 1.0. In the future, the virtual registry capability could be configured or customized, as required, to enable any of the Remaining Business Registries that do not have online extra-provincial/territorial registration services to be able to interoperate with MRAS.

### **3.3. Current participation in MRAS System 1.0**

Ultimately, the objective is to digitally connect all 14 business registries. However, as mentioned above, the six Remaining Business Registries are not yet actively interoperating with MRAS System 1.0. Additionally, the eight Participating Business Registries are currently at varying stages of development and interoperability with MRAS System 1.0:

- British Columbia, Alberta, Manitoba, Saskatchewan, Ontario, Quebec, Nova Scotia and Corporations Canada currently have the unified search capability operational for two types of Business Entities: business corporations (BCs) and some limited partnerships (LPs).
- British Columbia, Alberta, Saskatchewan and Manitoba have the streamlined extra-provincial/territorial registration and the automated notifications of changes to business information capabilities fully operational for two types of Business Entities - business corporations (BCs) and limited partnerships (LPs) – as of June 2020.
- Quebec and Corporations Canada have the streamlined extra-provincial/territorial registration and the automated notifications of changes to business information capabilities fully operational for business corporations (BCs) as of early 2021.

Current participation in MRAS System 1.0 is summarized as follows:

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

Business Registry	Unified Search	XP Registration	Notifications
AB	Operational for BCs, LPs	Operational for BCs, LPs	Operational for BCs, LPs
BC	Operational for BCs, LPs	Operational for BCs, LPs	Operational for BCs, LPs
CA	Operational for BCs	Operational for BCs	Operational for BCs
MB	Operational for BCs, LPs	Operational for BCs, LPs	Operational for BCs, LPs
NB	To be determined	To be determined	To be determined
NL	To be determined	To be determined	To be determined
NWT	To be determined	To be determined	To be determined
NS	Operational for BCs	To be determined	To be determined
NU	To be determined	To be determined	To be determined
ON	Operational for BCs, LPs	To be determined	To be determined
PEI	To be determined	To be determined	To be determined
QC	Operational for BCs	Operational for BCs	Operational for BCs
SK	Operational for BCs, LPs	Operational for BCs, LPs	Operational for BCs, LPs
YK	To be determined	To be determined	To be determined

### 3.4. Context

Business registries are the authoritative source of information about businesses in a jurisdiction. The private sector relies on business registries for a vast array of commercial transactions critical to the functioning of the economy. Consumers, the legal community, the general public, and other businesses, such as banks, lending institutions, suppliers and creditors, use business registries to verify the active status of a business. Academic and private sector researchers, the media, governments, regulators and law enforcement agencies also regularly rely on business registries.

In Canada, each province and territory, as well as the federal government (Corporations Canada), manages a business registry for their jurisdiction. Each one operates independently with its own rules and business processes.

This means that, in most cases, businesses in Canada are required to register in every province and territory where they want to operate. This process is called “extra-provincial/territorial registration.” Registering in multiple provinces and territories often means that businesses operating across Canada need to provide similar information to many governments, often in different formats and on different dates.

Moreover, once a business is registered in multiple provinces and territories, changes to its business information or status in one jurisdiction (for example, when a business becomes inactive) are not always communicated to the other jurisdictions, resulting in potentially incomplete or incorrect information about the business in those jurisdictions.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

This is a particular problem when one is searching to verify the status of a business. A comprehensive search requires separate searches of multiple business registries, and any inconsistent information needs to be reconciled by the searcher, leaving uncertainty about the business.

**3.5. Federal-provincial-territorial working group**

The burden that extra-provincial/territorial registration puts on businesses operating in Canada has been a recognized issue for more than 20 years. However, harmonizing legal and business requirements across the various jurisdictions has been difficult, and progress has been slow and fragmented. Following the 2014 Council of the Federation Conference of Canadian Premiers, reducing the barriers to extra-provincial/territorial registration across Canada was identified as a priority and undertaken as part of a comprehensive review to strengthen and modernize the Agreement on Internal Trade, now the Canadian Free Trade Agreement.

The Canadian Association of Corporate Law Administrators (CACLA), made up of representatives from all the provinces, territories, and Corporations Canada, a branch within Innovation, Science and Economic Development Canada (ISED), were engaged and invited to form a working group to develop a realistic and achievable action plan to address this issue.

**3.6. Vision and guardrails**

From April 2015 to March 2016, the working group came together through monthly meetings to better understand the problems faced by Canadian businesses and to identify desired outcomes. These collaborative efforts resulted in a shift in focus toward harmonizing the service process rather than continuing to seek alignment on legal and business requirements. This meant looking for a digital solution that would not require changes to business registry data and that would minimize any impact on existing business registry processes and systems. This shift resulted in an unprecedented, unanimous agreement by the working group to “create a scalable and adaptable digital solution that streamlines extra-provincial/territorial registration and reporting” (the Vision).

The working group also developed the following guardrails (the Guardrails) to guide the exploration of the digital solution:

- the source content from each business registry must not be modified;
- the existing business models of each business registry must be respected; and
- the focus of the digital solution must be on harmonizing the service process and improving user-experience without business registries necessarily changing practices.

**3.7. The MRAS journey**

Having established the vision and the guardrails, the working group proceeded with an agile, iterative process to develop the digital solution:

- From April 2016 to August 2016, six jurisdictions co-developed a proof of concept through bi-weekly sprints. This sub-working group explored ideas, concepts, storyboards and user journeys in order to better define the scope of the digital solution. The work was presented to the larger working group, and the result was unanimous agreement that the digital solution would enable three main capabilities:
  - streamlined extra-provincial/territorial registration;
  - automated notifications of changes to business information; and
  - a unified search capability.
- From September 2016 to March 2017, eight jurisdictions co-developed a prototype. This sub-working group explored solution options using sample data in order to determine how to connect the business registry systems and to identify the design, technical and business process risks. The result was again presented to the larger working group and resulted in unanimous agreement that the digital solution to connect Canada's business registries would be through an interoperability broker service that enables information to be shared among the business registries. The working group labelled this broker service the "Multi-jurisdictional Registry Access Service" or "MRAS."
- From October 2017 to April 2018, five jurisdictions participated in the development of a functioning pilot. Using real data, this sub-working group successfully demonstrated interoperable data sharing between the business registries in a test environment. The result was unanimous agreement by the larger working group to continue the development process to bring the digital solution to the beta phase ("MRAS beta").
- In June 2018, the first of the three main capabilities of the MRAS beta was launched - the unified search capability. [Canada's Business Registries beta search service / Registres d'Entreprises au Canada service de recherche bêta](#) provides the public with the ability to search for business information about business corporations and some limited partnerships across six of the Participating Business Registries - British Columbia, Alberta, Manitoba, Ontario, Quebec and Corporations Canada. User feedback is continuously collected on the beta search service in order to inform continuous improvements to the service.
- From September 2018 to March 2019, two more jurisdictions were added to the functioning pilot. In this phase, an additional component of a virtual registry was developed to enable Alberta, one of the Participating Business Registries, which did not have online extra-provincial/territorial registration services, to fully interoperate with the MRAS beta and the other Participating Business Registries.
- Throughout 2019, the MRAS beta was enhanced to the current version of MRAS – MRAS System 1.0 - to support the Participating Business Registries in the development of their streamlined extra-provincial/territorial registration services and automated notifications of changes to business information for business corporations and some limited partnerships.

- As of June 2020, MRAS System 1.0 supports four of the Participating Business Registries – British Columbia, Alberta, Saskatchewan and Manitoba - in their streamlined extra-provincial/territorial registration services and automated notifications of changes to business information for business corporations and some limited partnerships, and Saskatchewan for the unified search capability. It also supports the virtual registry capability and the entity correlation capability. Two additional Participating Business Registries – Quebec and Corporations Canada - are fully supported as of early 2021.
- As of October 2022, MRAS System 1.0 supports Nova Scotia for the unified search capability.

## 4. Scope of Work

### 4.1. Brief overview

This section sets out a brief overview of the scope of services that must be provided by the Contractor.

4.1.1. The scope of work for the Hosting and Operations Services includes:

4.1.1.1. A Transition-In phase of a period of 180 calendar days from Contract award, during which time the Contractor will deploy and render functional the current version of MRAS (MRAS System 1.0 as more particularly described in Section 5 – Technical Environment) in the Contractor's environment utilizing an Approved Government of Canada Cloud Brokering Service. This phase includes testing functionality with the Participating Business Registries that are currently interoperating with MRAS System 1.0. The requirements for the Transition-In phase are more particularly set out in section 4.4.

4.1.1.2. A Hosting and Operations phase which will commence once the Transition-In phase is completed and during which time the Contractor will support the Participating Business Registries and their interoperations with MRAS by:

- hosting and operating MRAS in accordance with specified security, operability and technical requirements;
- supporting the three main MRAS capabilities that are currently operational: streamlined extra-provincial/territorial registration, automated notifications of changes to business information and unified search;
- supporting all MRAS core services, including the entity correlation and the virtual registry capabilities;
- conducting all required maintenance activities, including maintaining MRAS source code and ongoing bug and incident resolution;
- streamlining, automating and enhancing MRAS components as required for efficient operation of MRAS; and
- ongoing reporting.

The requirements for the Hosting and Operations phase are more particularly set out in section 4.5.

- 4.1.1.3. A Transition-out phase which will commence with the establishment of a new contractual or other agreement for the provision of Hosting and Operations services for MRAS after the end of Contract Period. It includes activities that must be undertaken by the Contractor to ensure the transition of MRAS to the new arrangement without interruption for the stakeholders.

4.1.2. The scope of work for the Related Development Tasks (more particularly set out in section 4.7) includes:

- 4.1.2.1. Core enhancements: Tasks that require the skills of various resource categories to continue developing MRAS to support the full participation of all 14 business registries in Canada (10 provinces, three territories and the federal government) in all three of the main MRAS capabilities - streamlined extra-provincial/territorial registration, automated notifications of changes to business information and unified search - for all types of Business Entities.

This will require working directly with the eight Participating Business Registries and the six Remaining Business Registries over the next several years to enable them to interoperate with MRAS in varying degrees as each becomes ready to implement each of the three main capabilities for each of the various types of Business Entities. It will also require that this be done in a way that minimizes as much as possible the impact on the Participating Business Registries that are already interoperating with MRAS and that respects the Vision and the Guardrails (set out in section 3.6). The requirements for the Related Development Tasks for the core enhancements are more particularly set out in section 4.8.

- 4.1.2.2. Other enhancements: Tasks that require the skills of various resource categories to continue developing various other capabilities for MRAS as MRAS continues to evolve in scope and purpose as determined by the Participating Business Registries. The requirements for the Related Development Tasks for the other enhancements are more particularly set out in section 4.9.

- 4.1.2.3. Any applications and related updates, upgrades and maintenance releases developed by the Contractor throughout the Contract Period must be made available to ISED during and at the end of the Contract, as any Intellectual Property that was developed or created by the Contractor in relation to the work performed is deemed developed or created by Canada. At the end of the Contract, the Contractor must transfer all MRAS assets owned by Canada to ISED or to a third party chosen by ISED.

## 4.2. Stipulations

The following underpin the requirements for the work:

4.2.1. The Contractor must carry out the work in furtherance of the MRAS objective of being a single, coordinated access broker through which potentially all 14 business registries in Canada will be able to exchange data.

4.2.2. The Contractor must carry out the work in a manner that respects the Vision and the Guardrails established by the working group as described in section 3.6.

4.2.3. The Contractor must carry out the work in a manner that respects the business requirements of the Participating Business Registries and minimizes as much as possible the impacts on the Participating Business Registries that are currently interoperating with MRAS System 1.0.

4.2.4. The Contractor must carry out the work in a manner that respects the memoranda of understanding or intergovernmental letters of agreement that have been entered into between Canada and each Participating Business Registry for the purpose of participating in MRAS.

## 4.3. Phases of work for the Hosting and Operations Services

The requirements for the Hosting and Operations Services are divided into the following three phases:

- a. Phase 1 – Transition-In
- b. Phase 2 – Hosting and Operations
- c. Phase 3 – Transition Out

## 4.4. Phase 1 – Transition-In [maximum 180 calendar days from commencement of Contract Period]

### 4.4.1. Duration

4.4.1.1. A period of 180 calendar days from Contract award is allotted for the Transition-In phase, during which time the Contractor must complete the requirements set out below in order to render MRAS functional in the Contractor's environment.

4.4.1.2. During the Transition-In Phase, MRAS System 1.0 will continue to operate in its current environment.

4.4.1.3. Once the Contractor has completed all preparations and is ready to release MRAS live, the MRAS System 1.0 environment will be decommissioned.

### 4.4.2. General requirements

4.4.2.1. The Transition-In phase must not require changes by the Participating Business Registries that are currently interoperating with MRAS System 1.0 beyond changes necessary to enable the Participating Business Registries to access MRAS in its new environment.

4.4.2.2. There must not be an interruption in service larger than a normal maintenance window for the Participating Business Registries that have the streamlined extra-provincial/territorial registration and the automated notifications of changes to business information capabilities fully operational.

#### 4.4.3. Planning documentation

4.4.3.1. The Contractor must prepare and submit to the Participating Business Registries for approval a series of plans intended to minimize any threat or risk associated with the work being performed under the Contract, including the plans identified below in sections 4.4.3.3 – 4.4.3.8. These documents must address the complete scope of Contractor activities to be completed in performance of the Hosting and Operations Services work performed under the Contract. This means that although the plans are prepared in Phase 1, they must encompass the complete set of required activities throughout Phases 1-3.

4.4.3.2. Section 7.1 summarizes the list of reports, plans and documents that the Contractor must deliver in Phase 1 and their required delivery dates.

#### 4.4.3.3. Risk Management Plan

4.4.3.3.1. Within 45 calendar days of Contract Award, the Contractor must provide a Risk Management Plan to the Participating Business Registries for review and approval. The Risk Management Plan must, at a minimum, identify the overall amount of risk in the work, a description of the tasks to be performed to manage the risks, the list of individuals involved with managing the risks, the method in which risks will be controlled and monitored as well as mitigation and contingency plans to assure the success of the delivery of MRAS.

#### 4.4.3.4. Quality Management Plan

4.4.3.4.1. Within 45 calendar days of Contract Award, the Contractor must submit a Quality Management Plan to the Participating Business Registries for review and approval. The Quality Management Plan must describe how the Contractor will manage the processes involved in delivery of Hosting and Operations Services for MRAS necessary to assure quality and must encompass ongoing processes to assure overall quality and functionality which, at a minimum, must

include problem management, project management, personnel management, testing environment, protocols that respect the Participating Business Registries' existing approaches, and approach to dispute resolution.

#### 4.4.3.5. Security Plan

4.4.3.5.1. Within 45 calendar days of Contract Award, the Contractor must provide a Security Plan to the Participating Business Registries for review and approval. The Security Plan must at a minimum, cover personnel, infrastructure, physical and IT Security.

4.4.3.5.2. The Security Plan must include the following:

- security architecture
- security component design
- security service operations
- hosting solution
- certification for cloud hosting solution
- vulnerability management
- patch management
- strong authentication for elevated privilege accounts
- secure software development processes
- incident response plan
- security test plan

4.4.3.5.3. The Contractor must ensure compliance with and provide evidence of compliance with the security controls listed in Appendix 4 - Annex A 2023 – IT Security Controls. The Contractor must be able to implement any changes to these Security Controls as required by ISED guidelines or standards at their own expense over the course of the Contract.

#### 4.4.3.6. Governance Structure and Methodology

4.4.3.6.1. Within 45 calendar days of Contract Award, the Contractor must provide a Governance Structure to the Participating Business Registries. The Governance Structure must show the Contractor personnel involved in providing Hosting and Operations services for MRAS, an outline of the roles and responsibilities at the Contractor side, and its methodology to be used in managing the relationship with the Project Authority, in governing the relationships between the Contractor's team members, and in governing relationships between the Contractor's team members and Participating Business Registries' personnel. The Contractor must also include a description

of the escalation process within the Contractor's organization to be applied when issues arise.

#### 4.4.3.7. Business Continuity Plan

4.4.3.7.1. At least 30 calendar days prior to transition to Phase 2, the Contractor must provide a Business Continuity Plan to the Participating Business Registries for review and approval. The Business Continuity Plan must ensure the continued availability of MRAS operations and related services in the event of a declared disaster. The Business Continuity Plan's structure must be structured so that it can be updated easily.

4.4.3.7.2. Prior to the transition to Phase 2, the Contractor, in collaboration with the Participating Business Registries, must successfully test the Business Continuity Plan.

4.4.3.7.3. At least 20 calendar days prior to transition to Phase 2, the Contractor must provide a Report of the testing results of the Business Continuity Plan to the Participating Business Registries.

#### 4.4.3.8. Transition-In Plan

4.4.3.8.1. Within 45 calendar days of Contract Award, the Contractor must provide the Participating Business Registries with a Transition-In Plan for review and approval. The Transition-In Plan must outline how MRAS System 1.0 will be installed in the Contractor's environment utilizing an Approved Government of Canada Cloud Brokering Service. As a minimum the plan must include details on:

- assessment of the current MRAS state identifying areas of change, including key policies and business processes;
- the dedicated network environments, including the development environment, the staging/QA environment and the production environment;
- data conversion and migration;
- training on solution capabilities;
- configuration activities;
- integration and testing activities;
- connectivity with Participating Business Registries;
- testing operational solutions;
- delivering functional capability;
- migration of Bulk Data for the Business Entities currently included in MRAS System 1.0;

- developing solution specific guidelines;
- developing operational procedure documentation;
- high-risk transition areas and impact, mitigation strategies and recommended mitigation actions;
- a pre-implementation checklist and post-implementation measurable evaluation criteria; and
- developing a thorough implementation readiness assessment plan, readiness assessment schedule, rollback strategy, assessment scorecards and identified and defined critical readiness criteria that will drive go and no-go decisions related to overall readiness and preparedness for going live.

4.4.3.8.2. The Contractor must develop the Transition-In plan in collaboration with the Participating Business Registries.

#### 4.4.4. Transition integration and system testing

4.4.4.1. The Contractor must develop a Testing Strategy and Plan in collaboration with the Participating Business Registries. The Testing Strategy and Plan must, as a minimum, include details on:

- the proposed integration, test strategy and plan to verify functional, performance and reliability requirements;
- recommended integration and testing requirements; and
- how the Testing Strategy and Plan meets requirements and adheres to defined policies.

4.4.4.2. At least 30 calendar days prior to transition to Phase 2, the Contractor must provide the Participating Business Registries with the Testing Strategy and Plan for review and approval.

4.4.4.3. The Contractor must conduct all system testing in accordance with the approved Testing Strategy and Plan.

4.4.4.4. At least 20 calendar days prior to transition to Phase 2, the Contractor must provide the Participating Business Registries with copies and summaries of the Test Results Report confirming that all such tests have been passed.

#### 4.4.5. User-acceptance testing (UAT)

4.4.5.1. The Contractor must assist the Participating Business Registries in defining UAT scenarios and acceptance criteria.

4.4.5.2. The Contractor must provide the Participating Business Registries with a production-like (test) environment to execute UATs.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

4.4.5.3. The Contractor must facilitate the collection of UAT results.

4.4.5.4. The Contractor must analyze the results of UAT and implement corrective action based on the UAT results and recommendations.

4.4.5.5. The Contractor must assess and communicate the overall impact and potential risk to system components prior to implementing changes.

#### 4.4.6. Transition readiness

4.4.6.1. Following the successful completion of all testing, the Contractor must enable the environment required to assume ongoing Hosting and Operations of MRAS.

4.4.6.2. At least ten calendar days prior to transition to Phase 2, the Contractor must provide a Transition Readiness Report to the Participating Business Registries for review and approval. The Transition Readiness Report must present and detail the steps required to move from system testing, through operations start-up and production roll-out, up to and including the first quarter in which MRAS is available for service delivery.

4.4.6.3. The Contractor must ensure that MRAS is fully functional at the completion of the Transition-In phase and must be fully staffed with trained personnel at that time to commence Hosting and Operations, as described in section 4.5.

#### 4.4.7. Executing the transition

4.4.7.1. Upon approval of the Transition Readiness Report, the Contractor must execute the Transition-In Plan.

4.4.7.2. The Contractor must provide ongoing Progress Reports and maintain a Risk and Issues Log, updated weekly or whenever a new risk/issue is identified.

4.4.7.3. The Contractor must conduct implementation and readiness assessments and report findings and recommendations to the Participating Business Registries on a weekly interval basis prior to cutover and identify any items or situations that would impede successful cutover.

4.4.7.4. The Contractor must perform, and complete remediation actions based on readiness assessments and report status to the Participating Business Registries.

4.4.7.5. The Contractor must verify that all work, testing, evaluation, assessments and corrective remediation activities are performed and successfully completed to

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

ensure 100% implementation readiness for all implementation criteria prior to going live.

4.4.7.6. At least ten calendar days prior to transition to Phase 2, the Contractor must make go/no-go recommendations and prepare an Implementation Decision Document for approval by the Participating Business Registries.

4.4.7.7. The Contractor must complete all post-cutover activities per the Transition-In Plan ensuring 100% completion of post-cutover activities.

#### 4.4.8. Stabilization and post-transition

4.4.8.1. The Contractor must resolve any stabilization/post-cutover issues identified as high priority within five calendar days of each cutover.

4.4.8.2. The Contractor must conduct a post-cutover inspection and submit completed post-cutover checklist within five calendar days following each cutover.

4.4.8.3. The Contractor must resolve any stabilization/post-cutover issues identified as non-high priority within 15 calendar days of each cutover.

4.4.8.4. The Contractor must conduct a stabilization assessment within ten calendar days following each cutover including analysis and recommendation.

4.4.8.5. The Contractor must complete all stabilization activities within 30 calendar days following each cutover.

4.4.8.6. The Contractor must conduct a post-transition review within 60 calendar days of each cutover.

### 4.5. Phase 2 – Hosting and Operations

#### 4.5.1. Duration

4.5.1.1. Hosting and Operations of MRAS will begin upon approval of the Implementation Decision Document (commencing at the end of phase 1) and will continue throughout the Contract Period.

4.5.1.2. Section 7.2 summarizes the list of plans, reports and documents that must be delivered by the Contractor in Phase 2 and their required delivery dates.

#### 4.5.2. General requirements

4.5.2.1. The Contractor must host and operate MRAS in a manner that meets the business requirements of the Participating Business Registries and aligns with the Vision and the guardrails of the working group as set out in section 3.6 as well as the design principles as set out in section 5.3.

#### 4.5.3. Security requirements

4.5.3.1. The Contractor must host and operate MRAS as described in the Security Plan and in accordance with the security requirements.

4.5.3.2. The Contractor must host and operate MRAS in a manner that meets the level of security associated with data management, which is Protected A.

#### 4.5.4. Operability requirements

4.5.4.1. The Contractor's must maintain the high availability and on-going performance of MRAS at or in excess of the Service Level Requirements set out in Appendix 1 – Annex A.

4.5.4.2. The Contractor must ensure that MRAS is able to handle variations in capacity, throughput and response time based on typical service volumes as set out in Appendix 3 – Annex A.

4.5.4.3. The Contractor must ensure that MRAS supports the MRAS System 1.0 data sharing capability that can be rolled out incrementally, according to each Participating Business Registry's readiness.

4.5.4.4. The Contractor must ensure that MRAS supports the MRAS System 1.0 data sharing capability that can be expanded incrementally to address more data about more types of Business Entities.

4.5.4.5. The Contractor must ensure that MRAS supports the MRAS System 1.0 data sharing capability with other differently structured data sets (for example, industry information, financial data, etc.) as may be deemed by the Participating Business Registries as mutually beneficial and of benefit to businesses operating in Canada.

4.5.4.6. The Contractor must undertake continuous streamlining, automation and enhancement of MRAS System 1.0 components as required for the efficient operation of MRAS.

4.5.4.7. The Contractor must undertake future upgrades in order to satisfy increased requirements or to use new technology, as necessary.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

#### 4.5.5. Operating requirements

- 4.5.5.1. The Contractor must ensure that MRAS continues to support the three main MRAS capabilities that are currently operational for the Participating Business Registries: streamlined extra-provincial/territorial registration, automated notifications of changes to business information and unified search, as more particularly described in section 3.2.
- 4.5.5.2. The Contractor must host and operate MRAS (as more particularly described in sections 5.4 to 5.15), including all hardware, network infrastructure, and software, system environments and facilities that are required for the delivery of all MRAS System 1.0 capabilities and services utilizing a cloud service provider that holds a GC Cloud Framework Agreement, 32099-1-1-00X, with Shared Services Canada.
- 4.5.5.3. The Contractor must ensure that [Canada's Business Registries](#) search service (currently in beta), and any subsequent versions, are accessible to all users located in all regions of, as well as outside of, Canada via the internet.
- 4.5.5.4. The Contractor must ensure that Canada's Business Registries search service (currently in beta), and any subsequent versions, are accessible in both official languages (English and French) and uphold Government of Canada accessibility standards.
- 4.5.5.5. The Contractor must ensure that [Canada's Business Registries](#) search service (currently in beta), and any subsequent versions, continue to use neutral branding and are not associated with any single federal, provincial or territorial government or private sector entity.
- 4.5.5.6. The Contractor must ensure that MRAS supports the use of the Business Number as an entity identifier and search key. The Business Number is the unique federal government numbering system that identifies an entity and the accounts it maintains with the Canada Revenue Agency and allows integration with other systems based on it.
- 4.5.5.7. The Contractor must ensure that MRAS facilitates the memoranda of understanding or letters of agreement that have been entered into between Canada and each Participating Business Registry for the purpose of participating in MRAS, as referred to section 4.2.4, including any uses agreed to by the parties to those memoranda or letters of agreement.

#### 4.5.6. Technical requirements

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

4.5.6.1. MRAS must continue to use open standards and ensure that no proprietary software is introduced without the agreement of the Participating Business Registries.

#### 4.5.7.Ongoing activities

4.5.7.1. The Contractor must maintain at least three dedicated network environments: the development environment, the staging/QA environment and the production environment.

4.5.7.2. The Contractor must maintain the MRAS source code to align with Participating Business Registry updates and other enhancements as required.

4.5.7.3. The Contractor must operate and maintain the APIs in alignment with the API specification document.

4.5.7.4. The Contractor must manage and maintain all MRAS components.

4.5.7.5. The Contractor must manage and maintain the search and other core services with the solution infrastructure.

4.5.7.6. The Contractor must maintain and enhance the data mapping configuration and transformation capability as required.

4.5.7.7. The Contractor must develop and manage the execution of test plans related to development activities.

#### 4.5.8.Maintenance requirements

4.5.8.1. MRAS must be maintained and operated at an agreed level of performance as set out in the Service Level Requirements in Appendix 2 – Annex A. All Service Level Requirement changes can only be performed through a contract amendment.

4.5.8.2. MRAS must be continuously maintained and upgraded, as required, including deploying new updates and releases of any third-party components used in MRAS as they become available.

#### 4.5.9.Maintenance activities

4.5.9.1. The Contractor must implement proper monitoring tools that provide information related to MRAS and related services. Any problem needs to be identified, resolved and communicated to the Participating Business Registries through Exception Reports and/or monthly Operations Reports.

- 4.5.9.2. The Contractor may be required to meet with the Project Authority or the Participating Business Registries, as needed.
- 4.5.9.3. The Contractor may be required to attend an annual meeting of the federal, provincial, territorial working group to update the Participating Business Registries and the Remaining Business Registries on MRAS.
- 4.5.9.4. The Contractor must monitor changes and update the Risk Management Plan, the Quality Management Plan, the Business Continuity Plan and the Security Plan when these may be affected. When changes necessitate modifications to these plans, the Contractor must update them and submit them to the Participating Business Registries for review and approval.
- 4.5.9.5. The Contractor must respond to any questions or support issues that might arise in the timeframe set out in the Service Level Requirements outlined in Appendix 2 – Annex A.
- 4.5.9.6. The Contractor must provide an on-line problem/incident reporting (ticketing) system to record and track issues reported by the Participating Business Registries and provide feedback on the resolution of the incident
- 4.5.9.7. The Contractor must manage issues (bugs, triage) within a timeframe agreed to by the Participating Business Registries and maintain a Risk and Issues Log to be provided to the Participating Business Registries monthly or when a new risk or issue is identified.
- 4.5.9.8. The contractor must provide a solution for notification of incidents and outages between MRAS and the Participating Business Registries and between the different Participating Business Registries themselves.
- 4.5.9.9. The Contractor must receive and assess change requests, identify applicable implementation steps and implement changes in a timeframe as agreed to by the Contractor and the Participating Business Registries.
- 4.5.9.10. The Contractor must develop a performance testing strategy and then conduct performance tuning as required, identify and implement performance optimizations.
- 4.5.9.11. The Contractor must ensure that the Business Continuity Plan (see 4.4.3.7) is kept up to date and can be executed in the event of a declared disaster.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

- 4.5.9.12. The Contractor, in collaboration with the Participating Business Registries, must successfully test the Business Continuity Plan every two years.
- 4.5.9.13. The Contractor must ensure processes, procedures and technical documentation are kept up to date to provide the necessary support for MRAS.
- 4.5.9.14. The Contractor must provide support for testing activities when there are releases, modifications or updates to MRAS.
- 4.5.9.15. The Contractor must assess the impact of new releases to MRAS on stakeholders and system operations and ensure that Participating Business Registries have sufficient notice and opportunity to test major updates and material changes prior to their release into production.
- 4.5.9.16. The Contractor must take corrective action to mitigate the impact of any release that negatively impacts the operation of MRAS or related services.

#### **4.6. Phase 3 - Transition Out [minimum 180 calendar days before the end of Contract Period]**

- 4.6.1. The Transition Out phase is the period that commences with the establishment by ISED of a new contractual or other agreement for the provision of Hosting and Operations services for MRAS after the Contract Period. It includes activities that must be undertaken by the Contractor to ensure the smooth, efficient and complete transition without interruption of access by the stakeholders to MRAS.
- 4.6.2. The Transition Out phase will begin as and when ISED requests and at a minimum 180 calendar days before the end of the Contract Period.
- 4.6.3. At the request of ISED, the Contractor must submit, within 30 calendar days of the commencement of Phase 3, a comprehensive Transition Out Plan to the Participating Business Registries to ensure the efficient, complete and secure transitioning of MRAS, including all MRAS assets owned by Canada, to ISED or to a third party chosen by ISED.
- 4.6.4. Following acceptance of the Transition Out Plan by the Participating Business Registries, the Contractor must undertake all obligations contained within the plan in accordance with the schedule approved by the Participating Business Registries and included in the Transition Out Plan, in addition to the following:
- 4.6.4.1. The Contractor must provide transfer of knowledge to ISED or ISED's delegated third party, in accordance with the schedule and the method to be used as outlined in the Transition Out Plan.

- 4.6.4.2. The Contractor must respond to queries regarding the Transition Out activities and any in-progress work to ensure a smooth transition to ISED or ISED's delegated third party and to ensure uninterrupted service.
- 4.6.4.3. During the Transition Out phase, the Contractor is responsible for complete and continued Hosting and Operations of MRAS as per the Contract, and the completion of any in-progress work, in accordance with the Transition Out Plan.
- 4.6.5. Prior to the fulfillment of the Contract or prior to the termination of the Contract, as applicable, the Contractor must deliver, enable and support the necessary activities (as determined by ISED) related to transition MRAS to the new service provider.
- 4.6.6. Prior to the fulfillment of the Contract or prior to the termination of the Contract, as applicable, the Contractor must make available to ISED any applications, and related updates, upgrades and maintenance releases developed by the Contractor and transfer all MRAS assets owned by the Participating Business Registries to ISED or a third party chosen by ISED.

#### **4.7. Related Development Tasks**

The Related Development Tasks will be required on an "as-and-when requested basis" and are divided into the following two categories:

- a. Core enhancements (more particularly set out in section 4.8); and
- b. Other enhancements (more particularly set out in section 4.9).

4.7.1. The Related Development Tasks for the work to be performed by the Contractor as set out in sections 4.8 and 4.9 will be requested by ISED using the Task Authorization process.

4.7.2. The Contractor will be required under a Task Authorization to provide the resource categories set out below:

1. Project Administrator
2. Business System Analyst
3. Business Transformation Architect
4. Web Designer
5. Database Administrator
6. Data Conversion Specialist
7. Programmer/Software Developer
8. Tester

The description of the above Task-Based Informatics Professional Services can be found at the following link: [Task-Based Informatics Professional Service: Requirements for services - TBIPS -](#)

[Centralized Professional Services ePortal - Professional Services - Buying and Selling - PSPC \(tpsgc-pwgsc.gc.ca\)](https://tpsgc-pwgsc.gc.ca)

#### 4.8. Core enhancements

4.8.1. In order to ensure that the vision of the working group is achieved, various resources will be required to provide services to continue developing MRAS to support the full participation of all 14 business registries in Canada (10 provinces, three territories and the federal government) in all three of the main MRAS capabilities - streamlined extra-provincial/territorial registration, automated notifications of changes to business information and unified search - for all types of Business Entities.

4.8.2. Core enhancements must be implemented with minimal impact on the Participating Business Registries that are already interoperating with MRAS and may include any of the services set out below.

4.8.2.1. Working with any Participating Business Registry that does not have already all three of the main MRAS capabilities operational in MRAS System 1.0 to enable it to interoperate with MRAS in order to implement any remaining capabilities as the Participating Business Registry becomes ready to do so.

4.8.2.2. Working with the Remaining Business Registries to implement each of the three main MRAS capabilities in order to enable them to interoperate with MRAS and become Participating Business Registries as each of them becomes ready to do so. This may require different timing for different capabilities, according to each Remaining Business Registry's readiness.

4.8.2.3. Configuring the virtual registry capability to enable businesses to register extra-provincially/territorially through an online process for any of the Participating or Remaining Business Registries that do not have a public-facing web presence that allows businesses to extra-provincially/territorially register.

4.8.2.4. Enabling all Participating Business Registries to include all types of Business Entities in all three of the main MRAS capabilities (for example, non-profits, cooperatives, etc.).

4.8.2.5. Enabling entity correlation for all types of Business Entities in MRAS, including entity correlations from Bulk Data.

4.8.2.6. Adapting MRAS to receive and implement additional APIs and data feeds as Participating and Remaining Business Registries are integrated for each of the three main MRAS capabilities.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

4.8.2.7. Enhancing the MRAS source code, the data mapping configuration and the transformation capability as Participating and Remaining Business Registries are integrated for each of the three main MRAS capabilities for each type of Business Entity.

4.8.2.8. Adapting MRAS to meet additional security requirements as identified and required by the Participating Business Registries as the core enhancements are developed.

4.8.2.9. Ensuring that MRAS allows future upgrades required to satisfy increased processing requirements as each of the Participating and Remaining Business Registries are integrated for each of the three main MRAS capabilities for each type of Business Entity.

#### **4.9. Other enhancements**

4.9.1. MRAS must be adaptable to evolve in scope and purpose as determined by the Participating Business Registries. Various resources will be required to provide services to continuously develop various other capabilities for MRAS as requested by the Participating Business Registries. These enhancements may include any of the services set out below.

4.9.1.1. Scaling and adapting MRAS both quantitatively and qualitatively to allow future upgrades in order to use new technologies, as required.

4.9.1.2. Scaling and adapting MRAS to accommodate change impact analyses, transformation and change management activities that may be undertaken by any of the Participating Business Registries.

4.9.1.3. Scaling and adapting MRAS to support the sharing of beneficial ownership data in order to facilitate pan-Canadian access to collected beneficial ownership information.

4.9.1.4. Scaling and adapting MRAS to correlate Business Entities to other sources of authoritative government information (for example, to information from the Canadian Securities Administrators, Statistics Canada and the Canadian Intellectual Property Office).

4.9.1.5. Scaling and adapting MRAS to support data sharing capability with other differently structured data sets (for example, industry information, financial data, etc.).

4.9.1.6. Ensuring that MRAS can receive, send and implement additional APIs and data feeds as other sources of authoritative government information and differently structured data sets are integrated with MRAS.

4.9.1.7. Enhancing the reporting and analytics capacity set out in section 5.12 to include dynamic and near real-time integration with other differently structured data sets to support economic analysis and research to better inform policy, strategic direction and program operations for all levels of government programs and services related to business activity in Canada.

## 5. Technical Environment

MRAS System 1.0, as described in this section, including source content, information architecture and design and the current business requirements of the Participating Business Registries, will be provided to the Contractor as Government Furnished Equipment.

### 5.1. Architecture overview

MRAS System 1.0 is a single, coordinated access broker through which potentially all 14 business registries in Canada will be able to exchange data. This data exchange is enabled by a single, common data model: Participating Business Registries map their individual data representations for the purposes of exchanging data with MRAS System 1.0 and, through MRAS System 1.0, to the other Participating Business Registries.

This approach avoids the problems associated with trying to map each of the business registries to the other business registries, an approach that was previously demonstrated to be unsustainable. It also enables the Participating Business Registries to enjoy the benefits of data sharing without having to change their systems or operating procedures beyond what is necessary to enable the data exchange and to leverage the data being exchanged, thereby respecting the working group's Vision and the Guardrails.

MRAS System 1.0 leverages existing international standards and proven technologies, including open-source components, in order to realize a data sharing capability that can be:

- rolled out incrementally, according to each business registry's readiness;
- expanded incrementally to address more data about more types of Business Entities; and
- adapted to facilitate other data collaborations as may be deemed mutually beneficial and of benefit to businesses operating in Canada.

### 5.2. Main capabilities

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

MRAS System 1.0 currently supports the three main capabilities identified by the working group for the Participating Business Registries (although the Participating Business Registries are currently at varying stages of development and interoperability with MRAS System 1.0, as described in section 3.3): streamlined extra-provincial/territorial registration, automated notifications of changes to business information and unified search.

5.2.1. The first capability is support for streamlined extra-provincial/territorial registration. When a business, established in a Home Jurisdiction, extra-provincially/territorially registers to operate in another jurisdiction, MRAS System 1.0 supports a tell-us-once registration process. That is, the business' core information is retrieved from its Home Jurisdiction business registry and the business only needs to add any additional data that is required to complete the registration in the Extra-provincial/territorial Jurisdiction.

5.2.2. Automated notifications of changes to business information are a related capability. Once a business completes an extra-provincial/territorial registration, a relationship is created in MRAS System 1.0 that links the participating business registries that are associated with that business (for example, a link is created between a business' record in its Home Jurisdiction business registry and all the records for that business that exist in the participating Extra-provincial/territorial Jurisdiction business registries in which that business is registered to operate). These relationships form the basis of a notification subscription that allow the participating business registries to be notified of changes that occur in another jurisdiction that affect a business in their jurisdiction.

5.2.3. The third capability is a unified search service that is publicly available in English as "[Canada's Business Registries](#)" and in French, as "[Registres d'Entreprises au Canada](#)". This no-fee service allows the public to identify any business that is registered in any of the Participating Business Registries through one coordinated search instead of having to go to each business registry individually. By design, the search service displays a limited amount of information on a business and provides a link to the business' Home Jurisdiction business registry so the searcher can get more information from the "source of truth." Any extra-provincial/territorial registration information that can be associated with that business by MRAS System 1.0 is also shown and includes a link to the Extra-provincial/territorial Jurisdiction business registry as the "source of truth" for that extra-provincial/territorial registration information.

### 5.3. Design principles

5.3.1. MRAS System 1.0 respects the Vision and the Guardrails established by the working group (as set out in section 3.6) and minimizes as much as possible the impact on the business registries:

- the source content from each business registry must not be modified;
- the existing business models of each business registry must be respected; and

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

- the focus of MRAS must be on harmonizing the service process and improving user experience without business registries necessarily changing practices.

5.3.2. MRAS System 1.0 is also based on the following design principles:

- the business registries are the source of truth;
- MRAS is not the source of truth;
- MRAS responds to the source of truth;
- MRAS retains only as much data as it needs to support its services;
- MRAS is event-driven;
- MRAS only reacts to specific instructions provided by the business registries; and
- MRAS does not enforce the business registries' business rules.

#### 5.4. Core services

MRAS System 1.0 consists of the following core services:

- entity correlation service, more particularly described in section 5.8;
- notification subscription and delivery service, more particularly described in section 5.9;
- data model and XML transformation service, more particularly described in section 5.10; and
- administrative services, more particularly described in section 5.12.

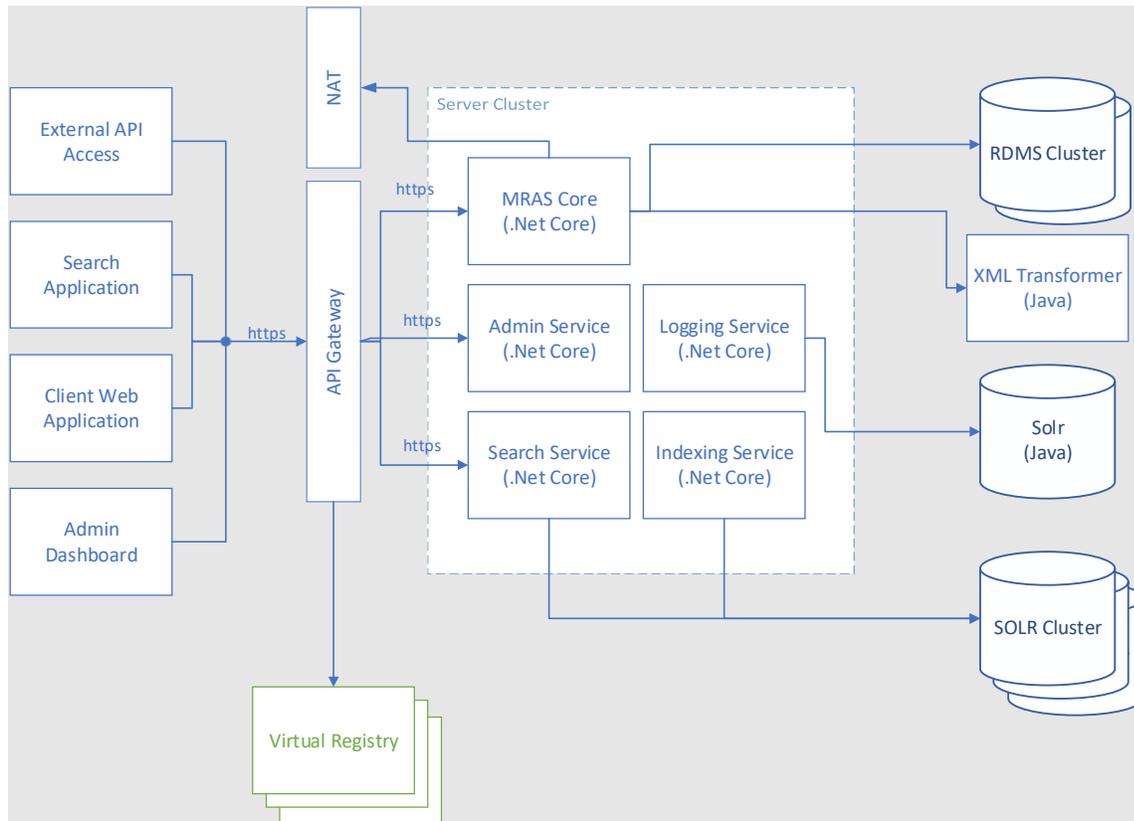
#### 5.5. Related services

In addition, two related services exist outside of the core services:

- search service, more particularly described in section 5.13; and
- virtual registry, more particularly described in section 5.14.

#### 5.6. Functional components

The following diagram illustrates the MRAS System 1.0 functional components.



## 5.7. General technical requirements

5.7.1. MRAS System 1.0 is comprised of web services that communicate with each other via RESTful APIs. The solution is currently hosted on Windows 2019 servers, on Amazon AWS infrastructure.

5.7.2. MRAS System 1.0 is a high availability solution. It ensures that, at a minimum, the core services are deployed with scalability, failover and redundancy in mind.

5.7.3. Both access to the API services, and the storage and transfer of data are secured. API access is protected by, at a minimum, an API key and IP restricted access. Keys must only be distributed to authorized parties and must only be stored as non-reversible hash in MRAS System 1.0. Data is transferred via HTTPS. Stored data is encrypted, and access to servers hosting services and data is controlled and secured.

## 5.8. Entity correlation service

The entity correlation service manages the correlations for each business between the Participating Business Registries. Correlations are typically between a business' Home Jurisdiction business registry and all of the business registries in which the business is extra-provincially/territorially registered to

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

operate. These correlations are set, modified and cancelled via messages sent by the Extra-provincial/territorial Jurisdiction business registries. In some specific cases (for example, when a business legally moves from one jurisdiction to another), correlations are between a business' former Home Jurisdiction and its new Home Jurisdiction. In these cases, the correlations are set by messages sent by the Home Jurisdiction business registries. Correlations are stored in a PostgreSQL database.

The technical requirements currently include:

- PostgreSQL
- SQL
- .Net Core 2.x
- Parsing large volumes of data in various formats including XML, CSV

### 5.9. Notification subscription and delivery service

The correlations described above create a subscription that enables notifications to be sent and received by the business registries. A notification for a business is sent by one business registry to MRAS System 1.0 and then by MRAS System 1.0 to all of the business registries that are actively subscribed to that business' correlations. For example, when the status of a business changes in its Home Jurisdiction business registry, all business registries where that business is extra-provincially/territorially registered to operate and that are actively subscribed to that business' correlations in MRAS System 1.0 are notified.

MRAS System 1.0 supports two notification types: extra-provincial/territorial registration notifications and change notifications.

#### 5.9.1.Extra-provincial/territorial registration notifications

Extra-provincial/territorial registration notifications are created when a business successfully completes an extra-provincial/territorial registration in a jurisdiction outside of its Home Jurisdiction. The extra-provincial/territorial registration notification is sent by the Extra-provincial/territorial Jurisdiction business registry and is forwarded by MRAS System 1.0 to the business' Home Jurisdiction business registry. This is the primary means of creating an entity correlation and the resulting subscription.

#### 5.9.2.Change notifications

Change notifications are created when an update is made to an existing business' information. Change notifications can be sent by either a Home Jurisdiction business registry or an Extra-provincial/territorial Jurisdiction business registry. Change notifications are forwarded through MRAS System 1.0 to any business registry that is actively subscribed to that business' correlations.

The sending and receiving of notifications is managed by several components: the notification API, the transformer service and the notification queue.

- a. The notification API allows business registries to send and receive notifications. It is a RESTful API that sends and receives notifications in XML format, in the schema specific to each business registry and a common MRAS System 1.0 notification schema.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

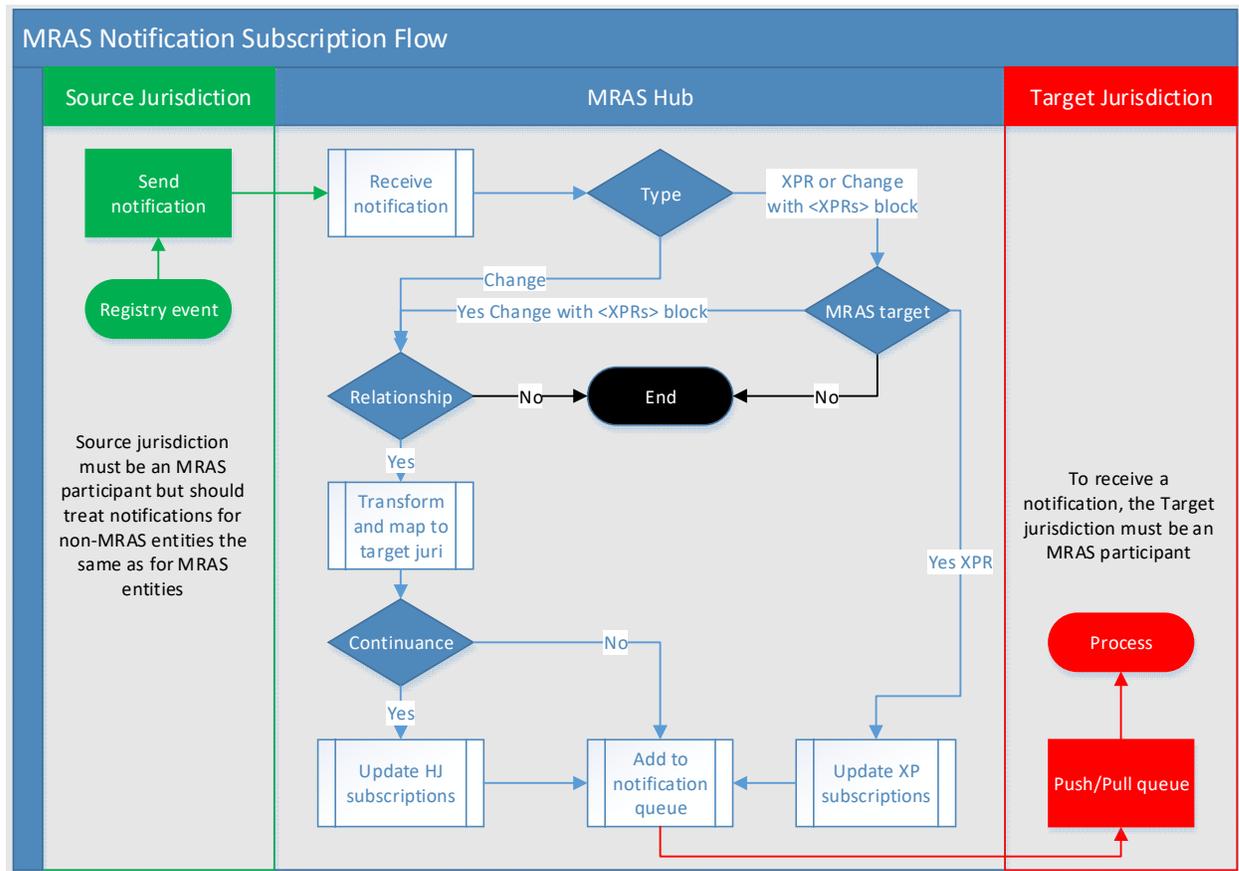
- b. The transformer service transforms notifications from the schema of the sending business registry to the schemas of the receiving business registries.
- c. Once notifications are transformed to the receiving business registries' schema, they are placed in a queue or storage mechanism that stores and delivers notifications in the order in which they are received. The queue is hosted in the PostgreSQL database.

Business registries either pull notifications from MRAS System 1.0 via the notification API, or they have notifications pushed to them by a MRAS System 1.0 service if they have configured an API endpoint at their location.

The technical requirements currently include:

- .Net Core 2.x web services
- XML
- PostgreSQL
- SQL
- Parallel processing
- RESTful API services
- Distributed services

The following diagram illustrates the notification process:



### 5.10. Data model and XML transformation service

The MRAS data model is the common data model to which all business registries' data is mapped for the purposes of exchanging data through MRAS System 1.0 to the other business registries. The MRAS data model covers all data elements needed to support the three main capabilities: streamlined extra-provincial/territorial registration, automated notifications of changes to business information, and unified search as well as the supporting capability of entity correlation.

The XML transformation service transforms the business registries' data to and from the MRAS data model. This ensures that each participating business registry can provide and receive data in the form that they specify, and that is directly compatible with their own business registry systems. This service is central to the operation of MRAS System 1.0. It facilitates the data exchange between fundamentally different systems in a way that minimizes the complexity of the necessary interoperability.

The transformation service is a Java-based web service that accepts XML documents in the sending business registry's XML schema, transforms the XML into the central MRAS System 1.0 XML schema, and then transforms to and returns XML documents in the receiving business registry's XML schema.

The technical requirements currently include:

- Extensible Stylesheet Language Transformations (XSLT)

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

- XML Schema Definition (XSD)
- Java web services
- RESTful APIs

### 5.11. Extra-provincial/territorial registration and notification processes

This section describes the processes whereby the business registries and MRAS System 1.0 interact to enable streamlined extra-provincial/territorial registration and automated notifications.

#### 5.11.1. Extra-provincial/territorial registration

- Initiate: The extra-provincial/territorial registration is initiated by a business from within the business' Home Jurisdiction business registry. (Alternatively, the process can be initiated from within the Extra-provincial/territorial Jurisdiction business registry in which the business wants to operate (the target business registry), in which case the next step is skipped).
- Business registry lookup: Based on the provision of a business identifier, MRAS System 1.0 returns a list of business registries in which extra-provincial/territorial registration is available for the business (e.g., jurisdictions in which the business is not already registered to operate). The returned list includes the URL of relevant business registries' sites. When the business selects a business registry (the target business registry), the business is transferred to that location.
- Request data: Once the business arrives at the target business registry site, it completes any account setup required by that business registry. When completed, the business enters its Home Jurisdiction and business identifier for its Home Jurisdiction business registry. This triggers a request to MRAS System 1.0 which passes the request to the business' Home Jurisdiction business registry. The Home Jurisdiction business registry responds with a data packet that includes the full profile of the business.
- Transform and map data: MRAS System 1.0 receives the profile and the transformation mapping service transforms and maps it to the required target business registry format, first transforming and mapping it to the MRAS System 1.0 data model, and then to the target business registry's format. MRAS System 1.0 then passes this transformed profile to the target business registry.
- Receive data: The target business registry populates its extra-provincial/territorial registration interface fields with the information from the profile. The business then adds any additional data that is required by the target business registry to complete the extra-provincial/territorial registration in accordance with the business rules that apply in that jurisdiction.

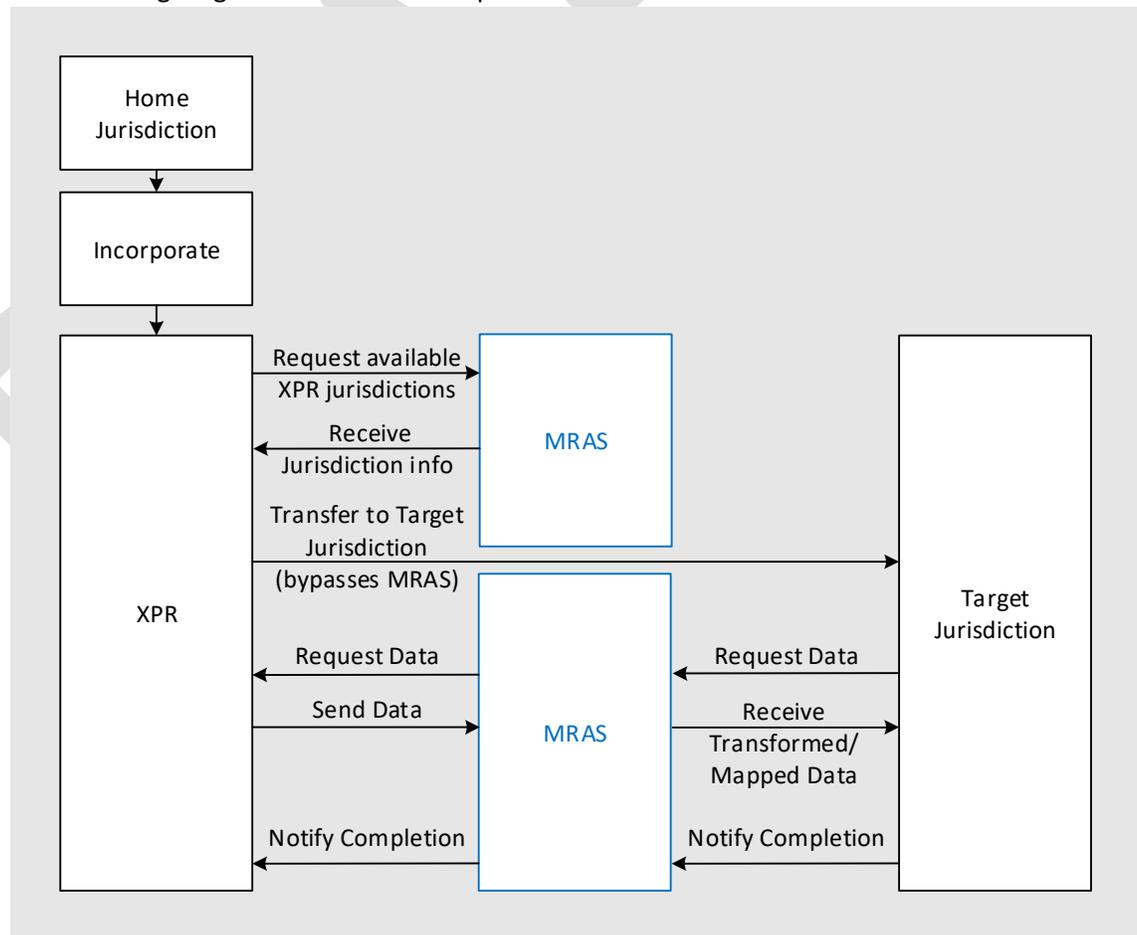
#### 5.11.2. Extra-provincial/territorial registration notifications

- a. For each new extra-provincial/territorial registration completed, the target business registry sends details of the completion to MRAS System 1.0, which in turn updates the entity correlation service with the relationship between the business' Home Jurisdiction business registry and the business registry in which the business is now extra-provincially/territorially registered to operate. A notification is also sent to the business' Home Jurisdiction business registry that the extra-provincial/territorial registration has been completed.

### 5.11.3. Change notifications

- a. Going forward, important data updates about the business will trigger additional notifications to all business registries that are actively subscribed to that business' correlations. For example, notifying the target business registry that the business that is registered to operate in that jurisdiction has undergone a significant status change within its Home Jurisdiction business registry.

The following diagram illustrates these processes:



### 5.12. Administrative services

MRAS System 1.0 contains a number of administration or utility services and scripts that provide a number of maintenance and reporting capabilities. These are available to both the internal administration team and the Participating Business Registries' teams.

The administrative components are written as .Net Core 2.x web services or console apps that run on a scheduled basis. Reporting tools are provided as .Net Core API services that provide raw data and functionality.

Any required UIs are implemented by each business registry.

The following Reporting Tools are available to Participating Business Registries (XML reports):

- List of Extra-provincial/territorial Jurisdiction profiles for one or more Home Jurisdiction profile IDs
- List of Home Jurisdiction profiles for one or more Extra-provincial/territorial Jurisdiction profile IDs
- List of previously read notifications in queue
- List of completed Extra-provincial/territorial registration transactions
- List of orphaned Extra-provincial/territorial Jurisdiction profiles for active Home Jurisdiction profiles
- List of log entries
- List of jurisdiction configurations (URLs, etc.)
- Other database-related query generated reports

The following Internal Administrative Reports are also available:

- Admin view of search results
- Manually generated reports via SQL
- Performance metrics
- Dashboard

The technical requirements currently include:

- .Net Core 2.x web services
- PostgreSQL, SQL

### 5.13. Search service

The search service makes core data provided by the business registries available for a public search application. The search service consists of:

- a. a web interface (UI)
- b. an API service that is accessed by the search UI
- c. a Solr full text index, which contains searchable profiles

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

- d. a database, which contains the extra-provincial/territorial registration entity correlations
- e. a process and a set of tools for deriving entity correlations from Bulk Data for various types of Business Entities and
- f. search notification handler, which processes incoming notifications.

When a user initiates a search, profiles are searched and returned from the Solr index and the extra-provincial/territorial registration entity correlations to determine the Home Jurisdiction and Extra-provincial/territorial Jurisdiction profiles for a particular business. Any required profiles that are not in the initial result set are retrieved from Solr. The final result set is ordered so that, for each business, the Home Jurisdiction profile is shown first. The result set is returned to the UI in paged fashion.

By design, the public search application displays a limited amount of information about a business, as agreed to by the working group, and provides a link to the Home Jurisdiction business registry so the user can get more information from the “source of truth.” Extra-provincial/territorial registration information can be associated with that business by MRAS System 1.0 is also shown. This also includes a link to the extra-provincial/territorial business registry providing that information as the “source of truth” for that information only.

The search service depends on the persistence and indexing of data received from the business registries. While it is not the objective of MRAS System 1.0 to maintain full copies of the business registries’ data holdings (in fact, MRAS System 1.0 is explicitly barred from doing so), data is held in a structured store that supports the operation of MRAS System 1.0’s core services and that is updated as continuously as possible to reflect the master data representations maintained by the business registries.

The technical requirements currently include:

- .Net Core 2.x web services
- Apache Solr 9.x
- XML
- Relational Databases (PostgreSQL), SQL
- Enterprise search experience dealing with large volumes of data
- Angular 7
- Web Experience Toolkit (WET)

#### **5.14. Virtual registry**

The virtual registry is an external component of MRAS System 1.0. It was developed to provide a basic web-based business registry capability to enable Participating Business Registries that do not have online extra-provincial/territorial registration services to fully participate in all three of the main MRAS System 1.0 capabilities. It requires customization for each business registry that uses it to meet their requirements.

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

The virtual registry provides a basic web-based business registry capability, including data capture and display facilities. It is a near end-to-end solution that allows businesses to complete an extra-provincial/territorial registration online. When the virtual registry is connected to the complete MRAS System 1.0 environment, the result is a business registry capability that the business registry can use to participate in and enjoy the benefits of MRAS System 1.0.

The virtual registry interacts with MRAS System 1.0 in the same way as the other business registries. It consists of a UI that contains the forms relevant to extra-provincial/territorial registration, an API service that acts as a bridge between the UI and the business registry-specific internal systems, and a customizable user authentication service that can be configured to work with most modern authentication models.

The virtual registry is designed to be generic enough to allow straight-forward use by most business registries requiring an online solution, with minimal customization. The virtual registry is built on mainstream open-source software components so that business registries are unrestricted in how they reuse and modify those components as part of either a virtual registry or a custom solution of their own design.

The business registries that choose to use the virtual registry capability are responsible for integrating the virtual registry capability with their own environments and their own business processes. Once integrated, the business registry assumes the responsibility for the resulting capability and for the associated ongoing maintenance.

The technical requirements currently include:

- .Net Core 2.x web services
- Identity Server
- Angular 7
- Web Experience Toolkit (WET)

### **5.15. System environments**

MRAS System 1.0 includes the following dedicated network environments.

The following are the environments that are accessible by the Participating Business Registries:

#### Development Environment

- Used for testing and debugging of components and services before deployment to the staging environment
- Limited test data used
- Environment and data frequently reset

#### Staging/QA Environment

- Used for validation of component updates before deployment to the production environment

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

- Closely replicates production environment including network and server configuration, logging and monitoring
- Ideally tested with production or production like data and volumes

#### Production Environment

- Environment configured to handle production data

## 6. Business Environment

### 6.1. Stakeholders

6.1.1. The following list describes MRAS stakeholders.

Businesses	Any business operating in Canada, in any province or territory. Includes all types of Business Entities. Also includes foreign businesses registered to operate in one or more Canadian jurisdiction.
General Public	Any member of the public seeking to verify a business. May be acting on behalf of an organization (e.g., a bank checking the status of a company for a loan, media researching a company, lawyers and other service providers assisting businesses to comply with registration requirements etc.).
Innovation Science and Economic Development Canada (ISED)	Different sectors of ISED use Canadian business data for research, service delivery initiatives, etc.
Federal Government Departments and Agencies	Other departments use business data, among them Statistics Canada and the Canada Revenue Agency, and also for financial management purposes.
Provincial/Territorial Government Departments/Agencies	Like the above, other departments and agencies at the provincial and territorial level are consumers of the business data.

### 6.2. Information providers

6.2.1. The federal government and each of the provincial and territorial governments provides or will provide information to MRAS, in accordance with a memorandum of understanding that has been entered into between Canada and each Participating Business Registry for the purpose of participating in MRAS. The following describes the information providers.

Provincial and Territorial Business Registries	Each province and territory operate a registry (or registries) of businesses (that is, Business Entities) in that jurisdiction, and is the authoritative source of business information in that jurisdiction.
Corporations Canada	Corporations Canada is the federal incorporating authority in Canada and maintains its own database of federal corporations.

### 6.3. MRAS governance structure

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

6.3.1. As a true multi-jurisdictional initiative, MRAS relies heavily on active participation from the federal, provincial and territorial governments.

6.3.2. The Participating Business Registries and the Remaining Business Registries have collaboratively developed a governance structure related to decision-making and the on-going operation of MRAS. This governance structure is intended to ensure fair representation and a whole-of-government approach to MRAS.

6.3.3. The MRAS Secretariat is the coordinating body housed at ISED and is responsible for overseeing the central operations of MRAS on behalf of the Participating Business Registries.

#### 6.4. Estimated volumes and activity

6.4.1. Participating Business Registries access MRAS System 1.0 for the streamlined extra-provincial/territorial registration and automated notifications of changes to business information capabilities. Information on the volume of automated notifications of changes to business information and estimated distribution of the number of active extra-provincial/territorial registrations for business corporations in each of the Participating Business Registries as well as the Remaining Business Registries is set out in Appendix 3 – Annex A - Volumes. Typically, these numbers increase by approximately 10% per year.

6.4.2. Multiple concurrent public users access MRAS System 1.0 for the unified search capability. The activity on the [Canada's Business Registries beta search service](#) currently averages approximately 6,500 sessions (approximately averaged 22,000 page views) per day.

6.4.3. MRAS System 1.0 currently holds approximately 9,4 million records in the CBR.

## 7. Reporting Requirements

### 7.1. Phase 1 Transition-In

Report Deliverables – Phase 1 Transition-In	Contractor must deliver on or before
Ongoing Progress Reports	Weekly throughout Phase 1
Risk Management Plan	45 calendar days of Contract Award
Security Plan	45 calendar days of Contract Award
Governance Structure	45 calendar days of Contract Award
Transition-In Plan	45 calendar days of Contract Award
Quality Management Plan	45 calendar days of Contract Award
Business Continuity Plan	30 calendar days prior to transition to Phase 2

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
Client Ref. No. – N° de réf. De client	File No. – N° du dossier	CCC No./ N° CCC – FMS No/ N° VME

Testing Strategy and Plan	30 calendar days prior to transition to Phase 2
Test Results Report – System	20 calendar days prior to transition to Phase 2
Test Results Report - Business Continuity Plan	20 calendar days prior to transition to Phase 2
Transition Readiness Report	10 calendar days prior to transition to Phase 2
Risk and Issues Log	Weekly or when new risk or issue is identified
Implementation Decision Document	10 calendar days prior to transition to Phase 2
Lessons Learned (Phase 1)	On completion of Phase 1

## 7.2. Phase 2 – Hosting and Operations

<b>Deliverables – Phase 2 Hosting and Operations</b>	<b>Contractor must deliver on or before</b>
Operations Reports	Within 10 business days of the end of the month
Exception Reports	Within 3 business days of occurrence
Risk and Issues Log	Monthly – On the first of every Month or when new risk or issue is identified
Updated Risk Management Plan, Quality Management Plan, Security Plan, Governance Structure and Business Continuity Plan	Only as changes occur
Lessons Learned (Phase 2)	On completion of Phase 2

## 7.3. Phase 3 – Transition Out

<b>Deliverables – Phase 3 Transition Out</b>	<b>Contractor must deliver on or before</b>
Transition Out Plan and Schedule	Within 30 calendar days of the commencement of Phase 3
Lessons Learned (Phase 3)	On completion of Phase 3

## 7.4. Related Development Tasks – core and other enhancements

7.4.1. Contractor reporting requirements will be identified by the Participating Business Registries, as required, within each Task Authorization and may include, but not necessarily be limited to, any of the following:

- Status reports, describing the state of ongoing project work and covering specific issues as requested by the Participating Business Registries. Status updates must be delivered as required, with weekly status updates at a minimum;
- Milestone Reports, describing the completion of a significant piece of work or as described in a Task Authorization, delivered as required; and
- Other reports, as required.

## 8. Contractor Obligations

- 8.1. The Contractor must provide the services of a team of resources for the provision of all activities necessary to efficiently achieve and proceed through each phase of the Contract for the Hosting and Operations services and for the Related Development Tasks, as required.
- 8.2. The Contractor must immediately notify the Project Authority of any issues, problems, or areas of concern that could adversely affect the ability of the Contractor to complete the work specified under any phase of the Contract for the Hosting and Operations services or for the Related Development Tasks under a Task Authorization.

## 9. Terminology

- 9.1. A list of definitions, abbreviations and acronyms relevant to and that form part of this Statement of Work is included with Appendix 1 - Annex A.

## 10. Location of Work

- 10.1. Most of the work to be completed under the Contract must be conducted at the Contractor's premises which must be located in Canada, in compliance with the requirements for secure information management.
- 10.2. Meetings with the Project Authority and the Participating Business Registries may take place by teleconference, virtually or at the Project Authority's premises, located in the National Capital Region (NCR).
- 10.3. There will also be an annual meeting of the federal, provincial, territorial working group, which Contractor personnel may be requested to attend. The annual meetings are typically held in a different province or territory each year.

## 11. Travel

- 11.1. There may be a requirement for Contractor personnel to travel to the annual meetings of the federal, provincial, territorial working group in the province or territory in which the meetings are being held. Dates and locations will be provided in advance of the meetings.

## **12. Language of Work**

- 12.1. The work will be conducted in English.

- 12.2. All deliverables will be in English

## **13. Management of the Project**

- 13.1. All deliverables and services rendered under this Contract are subject to inspection by the Project Authority. The Project Authority shall have the right to reject any deliverables or services that are not considered satisfactory, or require their correction, before payment will be authorized.

## **14. Project Management Control Procedures**

The Project Authority will monitor and control the work by scheduling weekly progress meetings with the Contractor personnel, as needed, in order to ensure the Contract will be brought in on time, on budget and of an acceptable quality. The Contractor is to provide progress reports in addition to those set out in Section 7 – Reporting requirements, as and when requested by the Project Authority and additional systems testing will be performed as required.

## ATTACHMENT 1- MANDATORY TECHNICAL CRITERIA

ID	Requirement	Substantiation
M1	Bidder's Experience – Project Management	<p>The Bidder must provide two reference contracts demonstrating its experience, the first within the last five years and the second within the last ten years (as of bid closing), in providing project management services for IT projects involving two or more stakeholders, performing all of the following tasks:</p> <ol style="list-style-type: none"> <li>1. Scope management;</li> <li>2. Cost management;</li> <li>3. Schedule management;</li> <li>4. Risk management;</li> <li>5. Change management activities;</li> <li>6. Communications and stakeholder management;</li> <li>7. Quality control management; and</li> <li>8. Financial and budget management.</li> </ol> <p>The following contract parameters must apply to each of the reference contracts:</p> <ol style="list-style-type: none"> <li>i. The contract cited must have a minimum contract value of \$500,000.00, including any amendments, and applicable taxes, excluding option years that have yet to be exercised;</li> <li>ii. The contract cited must have been for an on-going duration or have a completed duration greater than one year (Note: duration does not include option periods that have not been exercised); and</li> <li>iii. The contract cited must have a minimum total invoiced amount of 50% (including applicable taxes) of the total value of the contract.</li> </ol> <p>For each of the reference contracts cited, the following information must be identified:</p> <ol style="list-style-type: none"> <li>i. The name of the client organization (to whom the services were provided);</li> <li>ii. The contract number or the contract name;</li> <li>iii. The contract dates and duration (indicating the years/months of engagement and the start and end dates);</li> <li>iv. A summary of the contract scope as well as objectives, deliverables and tasks performed;</li> <li>v. A description of the project management services provided;</li> </ol>

		<p>vi. Client reference information (The name, title, telephone number and e-mail address of the Project Authority) that can validate the stated experience.</p> <p>The referenced contracts must have been contracted with the Bidder submitting a bid for this requirement. "Bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both.</p>
M2	Bidder's Experience – Cloud Hosting	<p>The Bidder must provide two reference contracts demonstrating its experience within the last five years (as of bid closing) of providing cloud hosting services for government clients using a GC-approved cloud brokering service (<a href="http://GC Cloud FA (canada.ca)">GC Cloud FA (canada.ca)</a> )</p> <p>The following contract parameters must apply to each of the reference contracts:</p> <ul style="list-style-type: none"> <li>i. The contract cited must have a minimum contract value of \$250,000.00, including any amendments, and applicable taxes, excluding option years that have yet to be exercised;</li> <li>ii. The contract cited must have been for an on-going duration or have a completed duration greater than one year (Note: duration does not include option periods that have not been exercised); and</li> <li>iii. The contract cited must have a minimum total invoiced amount of 50% (including applicable taxes) of the total value of the contract.</li> </ul> <p>For each reference contract cited, the following information must be identified:</p> <ul style="list-style-type: none"> <li>i. The name of the client organization (to whom the services were provided);</li> <li>ii. The contract number;</li> <li>iii. The contract dates and duration (indicating the years/months of engagement and the start and end dates);</li> <li>iv. A summary of the contract scope as well as objectives, deliverables and tasks performed; and</li> <li>v. Client reference information (The name, title, telephone number and e-mail address of the Project Authority) that can validate the stated experience.</li> </ul> <p>The referenced contracts must have been contracted with the Bidder submitting a bid for this requirement. "Bidder" means the person or entity (or, in the case of a</p>

		joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both.
M3	Bidder's Experience – Transition of Existing Operational IT Solutions	<p>The Bidder must provide two reference contracts demonstrating its experience, within the last five years (as of bid closing) of assuming responsibility for (taking over) an existing operational IT solution involving two or more stakeholders and performing each of the following tasks:</p> <ol style="list-style-type: none"> <li>1. Preparing planning documentation;</li> <li>2. Transition integration and system testing;</li> <li>3. User acceptance testing;</li> <li>4. Transition readiness;</li> <li>5. Executing the transition; and</li> <li>6. Stabilization and post-transition services.</li> </ol> <p>The following contract parameters must apply to each of the reference contracts:</p> <ol style="list-style-type: none"> <li>i. The contract cited must have a minimum contract value of \$500,000.00, including any amendments, and applicable taxes, excluding option years that have yet to be exercised;</li> <li>ii. The contract cited must have been for an on-going duration or have a completed duration greater than one year (Note: duration does not include option periods that have not been exercised); and</li> <li>iii. The contract cited must have a minimum total invoiced amount of 50% (including applicable taxes) of the total value of the contract.</li> </ol> <p>For each reference contract cited, the following information must be identified:</p> <ol style="list-style-type: none"> <li>i. The name of the client organization (to whom the services provided);</li> <li>ii. The contract number;</li> <li>iii. The contract dates and duration (indicating the years/months of engagement and the start and end dates);</li> <li>iv. A summary of the contract scope as well as objectives, deliverables and tasks performed; and</li> <li>v. Client reference information (The name, title, telephone number and e-mail address of the Project Authority) that can validate the stated experience.</li> </ol> <p>The referenced contracts must have been contracted with the Bidder submitting a bid for this requirement. "Bidder" means the person or entity (or, in the case of a</p>

		joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both.
M4	Bidder's Experience – Support	<p>The Bidder must provide two reference contracts demonstrating its experience within the last five years (as of bid closing) of production and stakeholder support for an IT solution that:</p> <ul style="list-style-type: none"> <li>• includes a significant public facing component</li> <li>• Facilitates at least 50k transactions per year</li> <li>• Consists primarily of server-side software</li> </ul> <p>The following contract parameters must apply to each of the reference contracts:</p> <ol style="list-style-type: none"> <li>i. The contract cited must have a minimum contract value of \$500,000.00, including any amendments, and applicable taxes, excluding option years that have yet to be exercised;</li> <li>ii. The contract cited must have been for an on-going duration or have a completed duration greater than one year (Note: duration does not include option periods that have not been exercised); and</li> <li>iii. The contract cited must have a minimum total invoiced amount of 50% (including applicable taxes) of the total value of the contract.</li> </ol> <p>For each reference contract cited, the following information must be identified:</p> <ol style="list-style-type: none"> <li>i. The name of the client organization (to whom the services were provided);</li> <li>ii. The contract number;</li> <li>iii. The contract dates and duration (indicating the years/months of engagement and the start and end dates);</li> <li>iv. A summary of the contract scope as well as objectives, deliverables and tasks performed; and</li> <li>v. Client reference information (The name, title, telephone number and e-mail address of the Project Authority) that can validate the stated experience.</li> </ol> <p>The referenced contracts must have been contracted with the Bidder submitting a bid for this requirement. "Bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both.</p>

M5	Bidder's Experience - Professional Services	<p>Using reference contract(s), the Bidder must demonstrate its experience within the last ten years (as of bid closing), providing resources required to provide professional services for each of the following resource categories:</p> <ol style="list-style-type: none"> <li>1. Project Administrator</li> <li>2. Business System Analyst</li> <li>3. Business Transformation Architect</li> <li>4. Web Designer</li> <li>5. Database Administrator</li> <li>6. Data Conversion Specialist</li> <li>7. Programmer/Software Developer</li> <li>8. Tester</li> </ol> <p>The resource must have been invoiced for a minimum of 50 hours within a one-year period.</p> <p>For each of the reference contracts cited, the following information must be identified:</p> <ol style="list-style-type: none"> <li>i. The name of the client organization (to whom the services were provided);</li> <li>ii. The contract number and or the contract name;</li> <li>iii. The contract dates and duration (indicating the years/months of engagement and the start and end dates);</li> <li>iv. A description of the tasks performed;</li> <li>v. Copies of Invoices for each resource category and</li> <li>vi. Client reference information (The name, title, telephone number and e-mail address of the Project Authority) that can validate the stated experience.</li> </ol> <p>The referenced contracts must have been contracted with the Bidder submitting a bid for this requirement. "Bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both. It does not include the parent, subsidiaries or other affiliates of the Bidder, or its subcontractors.</p>
----	---	--

## ATTACHMENT 2- POINT RATED TECHNICAL CRITERIA

ID	Rated criteria	Substantiation	Rating scale	Scoring	Bid Reference paragraph and page no.
P1	Project Plan	<p>The Bidder should describe its proposed implementation approach and provide a high level Project Plan to demonstrate how it plans to deliver all of the work described under Annex A – Statement of Work of this bid solicitation, with specific details about how the Bidder will respect the vision and the guardrails established by the working group described in Section 3.6 – Vision and guardrails under Annex A – Statement of Work of this bid solicitation.</p> <p>The Project plan must include a description of the following key elements:</p> <ul style="list-style-type: none"> <li>i. The overall approach and project schedule;</li> <li>ii. The major activities;</li> <li>iii. The key deliverables;</li> <li>iv. The three most significant risks inherent in implementation and how each risk would be mitigated; and</li> <li>v. The resource team structure, including the main point of accountability, the roles of each member and the specific activities in which each member will be involved.</li> </ul>	<p>Maximum of 10 points</p> <p><i>2 points per description of each key element.</i></p>		
P2	Service Management Framework	<p>The Bidder should describe the service management framework that it proposes to use to manage the delivery of all work described under Annex A – Statement of Work of this bid solicitation.</p> <p>The Service Management Framework must include specific details about how the Bidder will meet the needs of the Participating Business Registries, specifically with regard to:</p> <ul style="list-style-type: none"> <li>i. the scope and nature of support services;</li> <li>ii. the accessibility of support services, including hours of service and response times;</li> <li>iii. incident management and problem management;</li> </ul>	<p>Maximum of 10 points</p> <p><i>2 points per description of each service management framework element.</i></p>		

		<p>iv.change management; and</p> <p>v.communicating with the Participating Business Registries, both individually and collectively, particularly with regard to operational and system needs.</p>			
P3	Complex Search Solutions	<p>The Bidder should demonstrate, using up to two (2) reference contract(s), experience within the last five years (as of bid closing) of implementing, configuring and administering complex search solutions. The following contract parameters must apply to each of the reference contracts:</p> <ul style="list-style-type: none"> <li>i.The contract cited must have a minimum contract value of \$500,000.00, including any amendments, and applicable taxes, excluding option years that have yet to be exercised;</li> <li>ii.The contract cited must have been for an on-going duration or have a completed duration greater than one year (Note: duration does not include option periods that have not been exercised); and</li> <li>iii.The contract cited must have a minimum total invoiced amount of 50% (including applicable taxes) of the total value of the contract.</li> </ul> <p>For each of the reference contracts cited, the following information must be identified:</p> <ul style="list-style-type: none"> <li>i.The name of the client organization (to whom the services were provided);</li> <li>ii.The contract number or the contract name;</li> <li>iii.The contract dates and duration (indicating the years/months of engagement and the start and end dates);</li> <li>iv.A summary of the contract scope as well as objectives, deliverables and tasks performed;</li> <li>v.A description of the complex search solutions and how they are similar to the search solutions for MRAS System 1.0 described in Section 5.13 – Search service under Annex A – Statement of Work of this bid solicitation; and</li> <li>vi.Client reference information (The name, title, telephone number and e- mail address of the Project Authority) that can validate the stated experience.</li> </ul>	<p>Maximum of 10 points</p> <p><i>5 points per reference describing the experience, meeting all the parameters and including all required information.</i></p>		

		<p>ISED will evaluate the risk and degree to which the Bidder provides supportive evidence of or demonstrates that the experience and expertise of the Bidder described under each contract is relevant in relation to the work described under Annex A – Statement of Work of this bid solicitation.</p> <p><i>The referenced contracts must have been contracted with the Bidder submitting a bid for this requirement. "Bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both.</i></p>			
P4	Transformation Services	<p>The Bidder should demonstrate, using up to two (2) reference contract(s), experience within the last five years (as of bid closing) of implementing and administering a transformation service similar to the transformation service for MRAS System 1.0 described in Section 5.10 – Data model and XML transformation service under Annex A – Statement of Work of this bid solicitation.</p> <p>The following contract parameters must apply to each of the reference contracts:</p> <ul style="list-style-type: none"> <li>i. The contract cited must have a minimum contract value of \$500,000.00, including any amendments, and applicable taxes, excluding option years that have yet to be exercised;</li> <li>ii. The contract cited must have been for an on-going duration or have a completed duration greater than one year (Note: duration does not include option periods that have not been exercised); and</li> <li>iii. The contract cited must have a minimum total invoiced amount of 50% (including applicable taxes) of the total value of the contract.</li> </ul> <p>For each of the reference contracts cited, the following information must be identified:</p> <ul style="list-style-type: none"> <li>i. The name of the client organization (to whom the services were provided);</li> <li>ii. The contract number or the contract name;</li> <li>iii. The contract dates and duration (indicating the years/months of engagement and the start and end dates);</li> <li>iv. A summary of the contract scope as well as objectives, deliverables and tasks performed;</li> </ul>	<p>Maximum of 10 points</p> <p><i>5 points per reference describing the experience, meeting all the parameters and including all required information.</i></p>		

		<p>v.A description of the transformation service and how it is similar to the transformation service for MRAS System 1.0 described in Section 5.10 – Data model and XML transformation service under Annex A – Statement of Work of this bid solicitation; and</p> <p>vi.Client reference information (The name, title, telephone number and e- mail address of the Project Authority) that can validate the stated experience.</p> <p>ISED will evaluate the risk and degree to which the Bidder provides supportive evidence of or demonstrates that the experience and expertise of the Bidder described under each contract is relevant in relation to the work described under Annex A – Statement of Work of this bid solicitation.</p> <p><i>The referenced contracts must have been contracted with the Bidder submitting a bid for this requirement. "Bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both.</i></p>			
P5	Data Management	<p>The Bidder should demonstrate, using up to two (2) reference contract(s); experience within the last five years (as of bid closing) in delivering data management services that included each of the following tasks:</p> <ol style="list-style-type: none"> <li>1. analyzing different data formats from various content sources;</li> <li>2. validating and operationalizing an IT solution that aggregated data from various sources and was delivered as web-ready information resources;</li> <li>3. implementing quality control processes during data rendering of content sources; and</li> <li>4. refining and enhancing the content transformation processes associated with different content sources.</li> </ol> <p>The following contract parameters must apply to each of the reference contracts:</p> <ol style="list-style-type: none"> <li>i.The contract cited must have a minimum contract value of \$500,000.00, including any amendments, and applicable taxes, excluding option years that have yet to be exercised;</li> </ol>	<p>Maximum of 10 points</p> <p><i>5 points per reference describing the experience, including each required tasks, meeting all the parameters and including all required information.</i></p>		

		<p>ii. The contract cited must have been for an on-going duration or have a completed duration greater than one year (Note: duration does not include option periods that have not been exercised); and</p> <p>iii. The contract cited must have a minimum total invoiced amount of 50% (including applicable taxes) of the total value of the contract.</p> <p>For each reference contract cited, the following information must be identified:</p> <p>i. The name of the client organization (to whom the services were provided);</p> <p>ii. The contract number;</p> <p>iii. The contract dates and duration (indicating the years/months of engagement and the start and end dates);</p> <p>iv. A summary of the contract scope as well as objectives, deliverables and tasks performed; and</p> <p>v. Client Reference Information (The name, title, telephone number and e- mail address of the Project Authority) that can validate the stated experience.</p> <p>ISED will evaluate the risk and degree to which the Bidder provides supportive evidence of or demonstrates the experience and expertise of the Bidder described under each contract is relevant in relation to the work described under Annex A – Statement of Work of this bid solicitation.</p> <p><i>The referenced contracts must have been contracted with the Bidder submitting a bid for this requirement. "Bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both.</i></p>			
P6	Extensibility and Scalability	<p>The Bidder should demonstrate, using up to two (2) reference contract(s), experience within the last five years (as of bid closing) developing web services that were extensible and scalable and able to accommodate enhancements similar to those set out in Sections 4.8 – Core enhancements and 4.9 – Other enhancements under Annex A – Statement of Work of this bid solicitation, including:</p> <p>1. supporting data sharing capabilities that can be rolled out incrementally to multiple stakeholders over time as each stakeholder becomes ready and able;</p>	<p>Maximum of 10 points</p> <p><i>5 points per reference describing the experience, including each required tasks, meeting all the parameters and including all required information.</i></p>		

		<p>2. expanding data sharing capabilities to include more types of data and other data sets; and</p> <p>3. absorbing increased volumes of data.</p> <p>The following contract parameters must apply to each of the reference contracts:</p> <ul style="list-style-type: none"> <li>i. The contract cited must have a minimum contract value of \$500,000.00, including any amendments, and applicable taxes, excluding option years that have yet to be exercised;</li> <li>ii. The contract cited must have been for an on-going duration or have a completed duration greater than one year (Note: duration does not include option periods that have not been exercised); and</li> <li>iii. The contract cited must have a minimum total invoiced amount of 50% (including applicable taxes) of the total value of the contract.</li> </ul> <p>For each reference contract cited, the following information must be identified:</p> <ul style="list-style-type: none"> <li>i. The name of the client organization (to whom the services were provided);</li> <li>ii. The contract number;</li> <li>iii. The contract dates and duration (indicating the years/months of engagement and the start and end dates);</li> <li>iv. A summary of the contract scope as well as objectives, deliverables and tasks performed; and</li> <li>v. Client reference information (The name, title, telephone number and e- mail address of the Project Authority) that can validate the stated experience.</li> </ul> <p>ISED will evaluate the risk and degree to which the Bidder provides supportive evidence of or demonstrates that the experience and expertise of the Bidder described under each contract is relevant in relation to the work described under Annex A – Statement of Work of this bid solicitation.</p> <p><i>The referenced contracts must have been contracted with the Bidder submitting a bid for this requirement. "Bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both.</i></p>			
--	--	---	--	--	--

<b>Requirement Number</b>	<b>Maximum Points Available</b>	<b>Contractor Score</b>
<b>P-1</b>	<b>10</b>	
<b>P-2</b>	<b>10</b>	
<b>P-3</b>	<b>10</b>	
<b>P-4</b>	<b>10</b>	
<b>P-5</b>	<b>10</b>	
<b>P-6</b>	<b>10</b>	
<b>Total Technical Score (TTS) out of 60:</b>		
<b>The minimum passing score is 42 points.</b>		

Solicitation No. – N° de l'invitation  
U6265-218741

Amd. No – N° de la modif.

Buyer ID – Id de l'acheteur  
638zm

Client Ref. No. – N° de réf. De client  
U6265-218741

File No. – N° du dossier

CCC No./ N° CCC – FMS No/ N° VME

### ATTACHMENT 3 - PRICING SCHEDULE

#### 1. INITIAL CONTRACT PERIOD:

Transition In – as described in section 4.4 of the Statement of Work in Annex A:

Transition In - 6 month period	Firm Monthly Rate (A)
Month # 1	\$ _____
Month # 2	\$ _____
Month # 3	\$ _____
Month # 4	\$ _____
Month # 5	\$ _____
Month # 6	\$ _____
<b>(B) Total Transition-In Estimated Value [SUM: A]</b>	\$ _____

Note: Reference throughout this Annex B to “Hosting and Operations (for the 8 Participating Business Registries)” means as they are currently inter-operating with MRAS System 1.0 at the time of Contract Award

Hosting and Operations (as described in sections 4.5 and 4.6 of the Statement of Work in Annex A):

INITIAL CONTRACT PERIOD (3 YEARS)	Firm Monthly Rate		
Hosting and Operations	Months (C)	Firm Monthly Rate (D)	Cost (E) [C x D]
<b>Remainder of Year 1</b> Hosting and Operations (for the 8 Participating Business Registries)	6	\$ _____	\$ _____
<b>Remainder of Year 1 (Per Additional Business Registry)</b> Hosting and Operations	6	\$ _____	\$ _____
<b>Year 2</b> Hosting and Operations (for the 8 Participating Business Registries)	12	\$ _____	\$ _____
<b>Year 2 (Per Additional Business Registry)</b> Hosting and Operations	12	\$ _____	\$ _____
<b>Year 3</b> Hosting and Operations (for the 8 Participating Business Registries)	12	\$ _____	\$ _____
<b>Year 3 (Per Additional Business Registry)</b> Hosting and Operations	12	\$ _____	\$ _____
<b>(F) Total Cost</b> Hosting and Operations [SUM: E]			\$ _____

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

**Related Development Tasks - as described in section 4.7 of the Statement of Work in Annex A) - As and when required:**

<b>INITIAL CONTRACT PERIOD (3 YEARS)</b>	<b>Firm Per Diem Rate</b>			
<b>Resource categories</b>	<b>Year 1 (G)</b>	<b>Year 2 (H)</b>	<b>Year 3 (I)</b>	<b>Cost (J) [G + H + I]</b>
Project Administrator	\$ _____	\$ _____	\$ _____	\$ _____
Business systems analyst	\$ _____	\$ _____	\$ _____	\$ _____
Business transformation architect)	\$ _____	\$ _____	\$ _____	\$ _____
Web designer	\$ _____	\$ _____	\$ _____	\$ _____
Database administrator	\$ _____	\$ _____	\$ _____	\$ _____
Data Conversion Specialist	\$ _____	\$ _____	\$ _____	\$ _____
Programmer/Software Developer	\$ _____	\$ _____	\$ _____	\$ _____
Tester	\$ _____	\$ _____	\$ _____	\$ _____
<b>(K) Total Cost of Related Development Tasks [SUM: J]</b>				<b>\$ _____</b>

## 2. OPTION PERIODS:

**Hosting and Operations – (as described in section 4.5 and 4.6 of the Statement of Work in Annex):**

<b>OPTION PERIOD (3 YEARS)</b>	<b>Firm Monthly Rate</b>		
<b>Hosting and Operations</b>	<b>Months (L)</b>	<b>Firm Monthly Rate (M)</b>	<b>Cost (N) [L x M]</b>
<b>Year 4</b> <b>Hosting and Operations</b> (for the 8 Participating Business Registries)	12	\$ _____	\$ _____
<b>Year 4 (Per Additional Business Registry)</b> <b>Hosting and Operations</b>	12	\$ _____	\$ _____
<b>Year 5</b> <b>Hosting and Operations</b> (for the 8 Participating Business Registries)	12	\$ _____	\$ _____
<b>Year 5 (Per Additional Business Registry)</b> <b>Hosting and Operations</b>	12	\$ _____	\$ _____
<b>Year 6</b> <b>Hosting and Operations</b> (for the 8 Participating Business Registries)	12	\$ _____	\$ _____
<b>Year 6 (Per Additional Business Registry)</b> <b>Hosting and Operations</b>	12	\$ _____	\$ _____
<b>(O) Total Cost Hosting and Operations [SUM: N]</b>			<b>\$ _____</b>

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

**Related Development Tasks - (as described in section 4.7 of the Statement of Work in Annex A) - As and when required:**

<b>OPTION PERIOD (3 YEARS)</b>	<b>Firm Per Diem Rate</b>			
<b>Resource categories</b>	<b>Year 4 (P)</b>	<b>Year 5 (Q)</b>	<b>Year 6 (R)</b>	<b>Cost (S) [P + Q + R]</b>
Project Administrator	\$ _____	\$ _____	\$ _____	\$ _____
Business systems analyst	\$ _____	\$ _____	\$ _____	\$ _____
Business transformation architect	\$ _____	\$ _____	\$ _____	\$ _____
Web designer	\$ _____	\$ _____	\$ _____	\$ _____
Database administrator	\$ _____	\$ _____	\$ _____	\$ _____
Data Conversion Specialist	\$ _____	\$ _____	\$ _____	\$ _____
Software Developer	\$ _____	\$ _____	\$ _____	\$ _____
Tester	\$ _____	\$ _____	\$ _____	\$ _____
<b>(T) Total Cost of Related Development Tasks [SUM: S]</b>				<b>\$ _____</b>

**3. TRANSITION – OUT:**

<b>Transition - Out</b>	<b>Firm Rate (U)</b>
<b>Total Cost of Transition-Out [SUM: U]</b>	<b>\$ _____</b>

<b>Total Bid Price</b>	<b>Cost</b>	<b>Points</b>
<b>Transition In [B]</b>	\$ _____	<b>18 points</b>
<b>Hosting and Operations [F + O + U]</b>	\$ _____	<b>70 points</b>
<b>Related Development Tasks [K+ T]</b>	\$ _____	<b>12 points</b>
<b>Total:</b>	\$ _____	<b>100 points</b>

<b>Solicitation No. – N° de l’invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l’acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

## APPENDIX 1 – ACRONYMS AND GLOSSARY

**Approved Government of Canada Cloud Brokering Service** means the GC Cloud Providers that have been approved by Canada and that are listed on the following web page: [https://cloud-broker.canada.ca/s/central-provider-page-v2?language=en\\_CA](https://cloud-broker.canada.ca/s/central-provider-page-v2?language=en_CA).

**Bulk Data** means the collection of data provided by the Participating Business Registries and is a compilation of information about Business Entities received or collected by each of the Participating Business Registries and owned by each of the Participating Business Registries respectively.

**Business Entities** or **Business Entity** means any organization included in any Participating Business Registry and may include, but is not limited to, business corporations, not-for-profit corporations, foreign corporations, limited partnerships, limited liability partnerships, co-operatives, trusts and sole proprietorships.

**Extra-provincial/territorial Registration Jurisdiction** means the province or territory in which a Business Entity is registered, other than in its Home Jurisdiction, in order to carry on business in that province or territory.

**Home Jurisdiction** means the jurisdiction under whose laws a Business Entity was formed, incorporated or amalgamated or, if so, the jurisdiction into which such Business Entity was continued or was transferred by a process similar to continuation.

**MRAS** means the Multi-jurisdictional Registry Access Service. It is a shared interoperability solution that allows the Participating Business Registries to exchange business information confidently and efficiently. It includes all software, hardware, data, domain names, processes and procedures, documentation and website employed in the operation of MRAS, both individually and collectively.

**MRAS System 1.0** means the current implementation of the technical system developed by Canada for the purpose of digitally connecting Canada’s 14 business registries to enable the exchange of business information. It includes all software, hardware, data, domain names, processes and procedures, documentation and website employed in the operation of MRAS System 1.0, both individually and collectively.

**Participating Business Registries** means the seven business registries in Canada that are currently interoperating with MRAS System 1.0 – namely, the official business registries in British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec as well as Corporations Canada (federal) - and includes any of the Remaining Business Registries as soon as they interoperate with MRAS.

**Project Authority** means the manager of the MRAS Program Office within ISED.

**Remaining Business Registries** means the seven business registries in Canada that are not currently interoperating with MRAS System 1.0 – namely, the official business registries in New Brunswick, Nova Scotia, Prince Edward Island, Newfoundland and Labrador, Yukon, North West Territories and Nunavut, any one of whom becomes a Participating Business Registries as soon as it interoperates with MRAS.

**Service Level Requirements** or **Service Levels** is a defined level of service, such as but not limited to: accessibility, availability, response time, etc. for MRAS that the Contractor must meet or exceed in order to fulfill its obligations under the Contract, as more particularly set out in Appendix 2 – Annex A.

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

## APPENDIX 2 – SERVICE LEVEL REQUIREMENTS

Item	Requirement
<b>Core business hours</b>	8:00 to 19:00 Eastern Time, Monday to Friday
<b>Non-core business hours</b>	19:00 to 8:00 Eastern Time, Monday to Friday, weekends, and holidays
<b>MRAS online system availability</b>	99.0%
<b>Search and legacy XPR data updates (monthly bulk data updates for new search onboarding participants)</b>	Within 2 business days of receipt. New data will only be loaded when XPR matching has been performed.
<b>System Outage Response and Resolution</b>	As per incident management table (below)
<b>Application deployments – scheduled releases</b>	Deployed within 4 hours of scheduled deploy time
<b>Application deployments – response to incidents</b>	Deployment included within resolution time as per incident management table
<b>System environment changes</b>	As mutually agreed with the Participating Business Registries
<b>Disaster Recovery</b>	Resumption of full service of elements within Contractor's control within 48 hours of the declaration of a disaster.
<b>Scheduled downtime communication – Inform Participating Business Registries of approved downtimes for system maintenance.</b>	<ol style="list-style-type: none"> <li>1) At least seven (7) calendar days in advance for planned outages or updates causing outages, plus a reminder twenty-four (24) hours in advance</li> <li>2) Twenty-four (24) hours for updates not causing outages or impacting Participating Business Registries</li> </ol>
<b>Change Window – Vendor will endeavour to schedule any downtime and/or updates within this window</b>	19:00 Eastern Time Friday to 8:00 Eastern Time Monday
<b>MRAS online system API access time</b>	99.5% of accesses within 10 seconds
<b>Reports of incidents received by email during a month will be satisfactorily resolved within 24 hours of receipt</b>	95.0%
<b>Outage reporting communicated to Participating Business Registries</b>	As per response time in incident management table
<b>Exception reports, submitted to Participating Business Registries</b>	Within 3 business days of occurrence
<b>Ad hoc reports, submitted to Participating Business Registries</b>	To be mutually agreed when report requested

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

Item	Requirement
<b>Monthly operations report submitted to Participating Business Registries</b>	Within 10 business days of the end of the month

## Incident Management Table

The following table defines the criticality of MRAS faults and the expected response and resolution times.

Level	Definition	Response Time	Resolution Time
<b>1 - Critical</b>	<ul style="list-style-type: none"> <li>Ongoing incident affecting more than one Participating Business Registry that prevents performance of normal business</li> <li>Data loss or corruption is occurring</li> <li>Security Breach</li> </ul>	30 minutes	4 Hours
<b>2 – High</b>	<ul style="list-style-type: none"> <li>Ongoing incident affecting a single Participating Business Registry that prevents performance of normal business</li> <li>Incident affecting more than one Participating Business Registry that allows normal business to continue with a workaround</li> <li>Significant performance degradation</li> </ul>	1 hour	8 Hours
<b>3 – Medium</b>	<ul style="list-style-type: none"> <li>Incident affecting one Participating Business Registry that that allows normal business to continue with a workaround</li> <li>Usable performance degradation</li> </ul>	4 Business Hours	2 Business Days
<b>4 - Low</b>	<ul style="list-style-type: none"> <li>Issue that has low impact on business performance</li> <li>Minor inconvenience to users</li> <li>Minor performance degradation</li> </ul>	8 Business Hours	5 Business Days

Response Time: time from the initial report of incident to acknowledgment of issue by the vendor to the participating Business Registries

Resolution Time: target maximum time from report of issue to deployment of fix to production

<b>Solicitation No. – N° de l’invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l’acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

### APPENDIX 3 – VOLUMES

Information on the Yearly Volume of Automated Notifications & Estimated Distribution of Active Extra- provincial/territorial Registrations for Business Corporations

	Information on the Yearly Volume of Automated Notifications*							
	AB	BC	CA	MB	QC	SK	CBR	Total
<b>New XPRs</b>	85,460	101,335	N/A	27,974	70,777	5,602	N/A	291,148
<b>Notifications Sent</b>	668,337	119,253	421,976	20,269	51,672	57,370	N/A	1,338,877
<b>Notifications Received</b>	17,365	33,628	0	10,281	6,633	17,814	1,621,870	1,707,591
<b>Total</b>	771,162	254,216	421,976	58,524	129,082	80,786	1,621,870	3,337,616

\* Notes for this table:

- Numbers are projected for a yearly period from the 60 day retention period currently allowed in the system
- Numbers used to generate the table are as of February 15, 2023
- “Search” represents the Canada Business Registries and is considered a client to MRAS just like any of the participating jurisdictions. Unlike the jurisdictions who only receive their notifications, “Search” receives all notifications.

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

Home Jurisdiction	Estimated Number of Active Extra-provincial/territorial Registrations in Each Home Jurisdiction**															Total
	AB	BC	CA	MB	NB	NL	NWT	NS	NU	ON	PE	QC	SK	YK	Other	
AB	x	9540	10990	850	400	80	120	940	10	4670	30	390	2830	50	1900	32800
BC	9760	x	12380	590	290	30	40	830	10	4250	20	370	830	130	2620	32150
CA	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0	0
MB	1730	1490	4500	x	150	20	20	520	10	2660	10	160	640	20	670	12600
NB	440	630	2520	60	x	60	10	120	0	1540	80	370	40	10	320	6200
NL	590	720	3090	60	320	x	10	780	10	1640	30	270	30	20	580	8150
NWT	660	380	1010	40	40	10	x	190	10	500	0	40	30	30	120	3060
NS	560	790	3670	70	80	160	10	x	0	1940	120	230	40	10	540	8220
NU	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	x	N/A	N/A	N/A	N/A	N/A	0	0
ON	7730	11790	293050	2140	2100	340	60	4130	20	x	110	5400	710	340	8470	336390
PE	250	350	1300	50	300	30	10	500	0	1000	x	150	30	10	250	4230
QC	920	1860	111670	130	410	40	10	660	10	6500	10	x	120	10	4900	127250
SK	7020	2340	3460	900	150	10	10	460	0	1880	10	150	x	20	710	17120
YK	430	690	810	40	40	10	30	170	0	500	0	40	30	x	110	2900
<b>Total</b>																591070

\*\* Notes for this table:

- Numbers are estimated
- Information is as of May 2020. Typically, these numbers increase by approximately 10% per year.
- NB and NS have an agreement whereby corporations from those jurisdictions do not have to register in the other, although some do so voluntarily
- Information on the Home Jurisdiction of business corporations registered in NU is not currently available
- 'Other' refers to jurisdictions outside of Canada.

## APPENDIX 4 – IT SECURITY CONTROLS

<b>ID:</b>	<b>ASC-1 - Architecture, design and threat modelling</b>
<b>Description:</b>	<p>Document the system design and architecture by identifying all application components including components that are not part of the application but that the application relies on to operate. The production of a data flow diagram (DFD) is an effective way to document the system design and architecture.</p> <p>A DFD is required to gain a comprehensive understanding of the mechanics of the application. When the important characteristics of the application and actors are documented, it is easier to identify relevant threats. The DFD will give a graphical representation of the data flow through an information system. It provides with a common understanding of the application. It also creates the opportunity to identify where sensitive data is coming from and how it is processed and stored.</p>
<b>Evidence Required:</b>	<p>1. Provide a data flow diagram (DFD).</p> <p>The Diagram must illustrate the following:</p> <ul style="list-style-type: none"><li>* Core System components, (e.g., servers, databases, etc.) and network zones in which they reside (e.g., DMZ, Operational Zone, Restricted Zone, etc.).</li><li>* Interconnectivity with existing systems (integrations with components already in place (e.g., Active Directory, IDM, Cognos BI, etc.).</li><li>* Traffic flow patterns (e.g., ports, protocols in use (e.g., http, https, LDAP, RDP, SSH, etc.)</li><li>* Protected B data (where it resides and transits)</li></ul>

<b>ID:</b>	<b>ASC-2 - Access control</b>
<b>Description:</b>	<p>Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment.</p> <p>Access Control Best Practices</p> <ol style="list-style-type: none"><li>1. Operation with least privilege<ul style="list-style-type: none"><li>** Design the application to work with fewest possible rights and permissions while still allowing it to accomplish what it needs to do.</li><li>** The bare minimum rights are granted to each user or account.</li></ul></li><li>2. Separating duties<ul style="list-style-type: none"><li>** Use dedicated role-based accounts to carefully segregate and limit the number of people who can access administrative functionality.</li></ul></li></ol>

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

	<p>** Separation of duties (SoD), as it relates to security, has two primary objectives. The first is the prevention of conflict of interest (real or apparent), wrongful acts, fraud, abuse and errors. The second is the detection of control failures that include security breaches, information theft and circumvention of security controls. Correct SoD is designed to ensure that individuals don't have conflicting responsibilities or are not responsible for reporting on themselves or their superior.</p> <p>3. Allow account to be disabled</p> <p>** Disabling an account can be useful when a user or employee goes on an extended leave of absence and you want to reduce the potential attack surface without having to delete the account. It also allows locking down a specific account that's been compromised without disrupting availability for other users.</p> <p>Sources / References:</p> <ol style="list-style-type: none"> <li>1. Web Application Security, A Beginner's Guide by Bryan Sullivan and Vincent Liu</li> <li>2. Securing Web Application Technologies [SWAT] Checklist <a href="https://software-security.sans.org/resources/swat">https://software-security.sans.org/resources/swat</a></li> </ol>
<b>Evidence Required:</b>	<ol style="list-style-type: none"> <li>1. Provide access control procedure documentation. The documentation must identify: <ul style="list-style-type: none"> <li>* How access requests are submitted</li> <li>* Who is responsible for authorizing (approving) requests</li> <li>* Who creates and configures the accounts</li> <li>* Who is responsible to review account and privilege assignments (i.e., clean-up)</li> <li>* How are the principles of least privilege and separation of duties implemented</li> </ul> </li> <li>2. Provide an access control matrix. The matrix must identify the roles used within the application and their associated privileges</li> </ol>

<b>ID:</b>	<b>ASC-3 - Authentication and identification</b>
<b>Description:</b>	<p>Authentication is the act of establishing or confirming, something (or someone) as authentic. Proper authentication ensures that a verified application verifies the digital identity of the sender of a communication and ensures that only those authorised can authenticate and that credentials are transported in a secure manner.</p> <p>Secure Authentication Best Practices</p> <ol style="list-style-type: none"> <li>1. Usernames/user ids must be case insensitive. <ul style="list-style-type: none"> <li>** User 'smith' and user 'Smith' should be the same user. User names should also be unique.</li> <li>** For more sensitive applications, usernames could be assigned and secret instead of user-defined public data.</li> </ul> </li> <li>2. Require re-authentication if invoking an important function. <ul style="list-style-type: none"> <li>** In order to mitigate Cross-Site Request Forgery (CSRF) and session hijacking, it's important to require the current credentials for an account before updating sensitive account information such</li> </ul> </li> </ol>

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

as the user's password, user's email, or before sensitive transactions, such as shipping a purchase to a new address. Without this countermeasure, an attacker may be able to execute sensitive transactions through a CSRF or Cross Site Scripting (XSS) attacks without needing to know the user's current credentials. Additionally, an attacker may get temporary physical access to a user's browser or steal their session ID to take over the user's session.

3. Deploy Two-factor / Multi-factor Authentication when the application processes Protected B information and is accessible over the Internet.

\*\* Also, multi-factor authentication is a very powerful deterrent when trying to prevent brute force attacks since the credentials are a moving target. When multi-factor is implemented and active, account lockout may no longer be necessary.

4. Allow account lockout.

\*\* This defensive technique is designed to counter brute-force attacks.

\*\* This defense can be abused to create a denial-of-service condition. Do not allow an administrative account to be locked out.

\*\* When locking an account is not feasible, use alternative measures like:

\*\*\* Throttling. Use increasing timeout values between subsequent failed authentication attempts.

\*\*\* CAPTCHAs. Make sure that the "**Completely Automated Public Turing test to tell Computers and Humans Apart** (CAPTCHA) used is authorized as it could violate disability/accessibility policies.

Account Lockout Guidance

	# of Attempts	Window of measurement	Lockout Period
	MEDIUM CIA Rating*	10 60 minutes	30 minutes
	HIGH CIA Rating*	5 30 minutes	Indefinite

\*CIA rating: Confidentiality, Integrity and Availability ratings can be found in the application's Statement of Sensitivity (SoS)

5. Do not hard-code credentials.

\*\* The recommended approach is to use some form of key or credential management system, or use a properly secured configuration file.

6. Avoid the "Remember Me" feature.

7. Keep accounts unique

\*\* Don't encourage use cases where users have to share accounts.

Password Best Practices

Because the use of passwords is pervasive as authentication factor in applications, they are also a very popular target for attackers. The attacks can be performed online against live applications, or they can be performed offline against hashed password values that an attacker has acquired.

Also, we must keep in mind that improperly designed password reset systems can lead to compromise of user accounts, and in some cases, to dangerous account lockout conditions.

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

	<p>Take into account the following password policy best practices when designing the application password policy:</p> <ol style="list-style-type: none"> <li>1. Require a minimum password/passphrase length of at least 20 characters</li> <li>2. Passwords must be case insensitive</li> <li>3. Do not rotate passwords periodically</li> </ol> <p>** Note that if a system cannot meet the password length requirement, a password rotation schedule and password complexity requirements will be necessary.</p> <p>** Ideally, users would only need to change their passwords on indication or suspicion of compromise.</p> <p>4. Systems should help users when selecting passwords by blocking passwords that are common or obvious. (E.g., previous passwords, passwords that are equal to (or contains) the username, etc.)</p> <p>For more guidance on password policy best practices: Government of Canada Password Guidance v.0.9  <a href="https://docs.google.com/document/d/1Vhg_B6nIIYMtEhO6SaMGatRHwabapz2HLAHMT9V4Ev0/edit?usp=sharing">https://docs.google.com/document/d/1Vhg_B6nIIYMtEhO6SaMGatRHwabapz2HLAHMT9V4Ev0/edit?usp=sharing</a>) and OWASP Authentication Cheat Sheet  <a href="https://www.owasp.org/index.php/Authentication_Cheat_Sheet">https://www.owasp.org/index.php/Authentication_Cheat_Sheet</a>)</p> <p>Sources / References:</p> <ol style="list-style-type: none"> <li>1. Web Application Security, A Beginner's Guide by Bryan Sullivan and Vincent Liu</li> <li>2. User Authentication Guidance for IT systems (<a href="https://www.cse-cst.gc.ca/en/node/2454/html/28582">https://www.cse-cst.gc.ca/en/node/2454/html/28582</a>) by the Communications Security Establishment (CSE)</li> <li>3. Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (<a href="https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111">https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111</a>)</li> <li>4. Digital Identity Guidelines (<a href="https://pages.nist.gov/800-63-3/sp800-63-3.html">https://pages.nist.gov/800-63-3/sp800-63-3.html</a>) NIST 800-63-3</li> <li>5. Government of Canada Password Guidance v.0.9  <a href="https://docs.google.com/document/d/1Vhg_B6nIIYMtEhO6SaMGatRHwabapz2HLAHMT9V4Ev0/edit?usp=sharing">https://docs.google.com/document/d/1Vhg_B6nIIYMtEhO6SaMGatRHwabapz2HLAHMT9V4Ev0/edit?usp=sharing</a>]</li> <li>6. OWASP Authentication Cheat Sheet  <a href="https://www.owasp.org/index.php/Authentication_Cheat_Sheet">https://www.owasp.org/index.php/Authentication_Cheat_Sheet</a>]</li> </ol>
<p><b>Evidence Required:</b></p>	<p>Which existing identification and authentication framework are you using? (E.g., IDM (i.e., GCKEY/Secure Key), MyKey, ISED Active Directory via LDAPS, Active Directory via Kerberos, etc.)</p> <p>If the application is a custom authentication system, please provide:</p> <ol style="list-style-type: none"> <li>1. Documentation explaining the identification and authentication process</li> </ol> <p>The documentation must identify:</p> <ul style="list-style-type: none"> <li>- How the application assigns usernames and if those usernames are case-sensitive</li> <li>- The use cases when sharing credentials are essential for the application to work</li> </ul>

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

- If the application uses hard-coded credentials
  - If the application processes Protected B data and is accessible over the Internet
  - \*\* If so, does the application leverages 2 factor or multi factor authentication (2FA/MFA)
  - How does the application prevent misuse of the account recovery/ password change functionality
  - If users are notified (out-of-band) if changes to their accounts are made
  - How failed authentication attempts are handled
  - The authentication error messages used by the application
2. Documentation explaining the password policy
- The documentation must explain how the password policy follows the password policy best practices.
3. A list of all the service accounts used by the application and their purpose
- a. Does the application use service accounts?
  - b. User accounts are used by real users, service accounts are used by system services such as web servers, mail transport agents, databases etc.
4. Documentation explaining the account lockout policy
- The documentation must identify:
- How many failed attempts triggered the lockout?
  - Within what timeframe are you counting failed attempts?
  - How long do you lockout the account until it automatically resets?
  - Does that application leverages throttling and/or CAPTCHAs?
5. Documentation explaining how database credentials are handled and where they are stored.

<b>ID:</b>	<b>ASC-4 - Session management</b>
<b>Description:</b>	<p>A session, in its broad theoretical sense, is simply a means for tracking single user's interactions with the application.</p> <p>If the application has no need to track user behavior prior to authentication, it is safer to defer generating and issuing session IDs until a user has successfully completed the authentication procedure.</p> <p>One of the core components of any application is the mechanism by which it controls and maintains the state for a user interacting with it. This is referred to as Session Management and is defined as the set of all controls governing state-full interaction between a user and the application. This control ensures that a verified application (1)</p>

creates sessions that are unique to each individual and cannot be guessed or shared and (2) invalidates sessions when they are no longer required and timed out during periods of inactivity.

Session management go hand in hand with authorization.

#### Session Management Best Practices

##### 1. Enforcing absolute session timeouts

\*\* If you're storing session state at the server, you can alleviate the inconvenience of forcing users to start from scratch with their tasks by restoring their session state when they re-authenticate and receive a new session ID.

\*\* Destroy the expired session ID, but keep the session state around for later use.

\*\* Protected B applications should limit session IDs to two hours, while for Protected A (or lower) applications, a four hour limit is sufficient. Adjust these values based on the level of risk you're willing to accept.

\*\* While you should specify an expiration timestamp on the session ID cookie itself, you must also enforce session timeouts on the server.

##### 2. Enforcing idle session timeouts

\*\* Best practice for Protected B applications is an idle timeout of no more than 15 minutes, and a 30-minute timeout for Protected A (or lower) application.

##### 3. Limiting session concurrency

\*\* The reasonable limit for your application will depend on the nature of the application.

##### 4. Mandating secure cookies

\*\* One of the attributes you can set on the cookie that holds your application's encrypted session ID is the "Secure" flag, which mandate that the web client uses encrypted communications (SSL and HTTPS) when sending cookie back to the server along with each request.

##### 5. Using the HttpOnly flag

\*\* The HttpOnly flag on a cookie instructs the client that the cookie is only to be used in communications over HTTP protocol. This effectively denies access to the cookie to any client-side code such as JavaScript.

##### 6. Using cryptographically random session IDs

\*\* Session ID should be of at least 128 bits in length and generated using secure pseudorandom number generator.

\*\* Use a cryptographically secure random number generator (CSPRNG). Random number sequences can be predictable, and not all random number generators are equal.

##### 7. Destroying invalidated session IDs

\*\* Invalidate the session ID on the server.

\*\* Immediately destroy any related client-side cookie value. Do this by including a Set-Cookie directives in the response with an expiration time set in the past.

\*\* Delete cookies when the browser closes.

##### 8. Using encrypted cookies

\*\* Encrypt any data you store in cookies on the web client.

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

	<p>** Encrypt any data that is sent with a key that is not accessible to the client, so the client cannot decrypt it.</p> <p>** If session state information ever does have to leave the server-side, encrypt it.</p> <p>** Use a Hash-based Message Authentication Code (HMAC) to verify the integrity of state information received from the client.</p> <p>9. Logging out</p> <p>** Provide an explicit logout facility in your application's UI</p> <p>10. Regenerating session IDs on authentication / privilege level change</p> <p>** When a user authenticates to a higher level (or even switches roles to access a different area), then the application should grant a new session ID with different rights or update the rights associated with the existing session ID. Updating the rights associated with a session ID is fraught with complexity and potential for introducing vulnerabilities into the application. Generally, it is safer to invalidate an older session ID and issue a new one any time a user changes authentication levels – upward or downward.</p> <p>11. Keep all session state information on the server-side</p> <p>** Keep as much as you can on the server. Ideally, keep all session state information at the server end.</p> <p>** Transmit as little as possible to the client. Ideally, don't transmit anything other than opaque session ID.</p> <p>** Encrypt anything that is sent to the web client for storage and that needs to come back unmodified, using an encryption key that is not available to the client, because the client should never be able to decrypt the encrypted data.</p> <p>** Rely on non-malleable cryptographic algorithms as a means to detect tampering; let decryption failures trigger immediate invalidation of the session.</p> <p>12. Make sure that your web application contains code that validates the session ID every time that protected data or functionality is being requested.</p> <p>Sources / References:</p> <p>1. Web Application Security, A Beginner's Guide by Bryan Sullivan and Vincent Liu</p>
<p><b>Evidence Required:</b></p>	<p>If the application uses an existing session management framework, (e.g., IDM), please name the framework and do not provide evidence item #1.</p> <p>Please provide:</p> <p>1. Documentation explaining the session management policy</p> <p>The documentation must identify:</p> <ul style="list-style-type: none"> <li>- If the application enforces absolute session timeouts</li> <li>** After how long does the timeout occur?</li> <li>** Is the session timeout enforced on the server?</li> <li>** Is the session state kept on the server side?</li> <li>- If the application enforces idle session timeouts</li> </ul>

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

	<ul style="list-style-type: none"> <li>** After how long does the timeout occur?</li> <li>- If the application allow concurrent sessions</li> <li>** How many concurrent sessions are allowed</li> <li>- The security flags set on the cookie</li> <li>** Secure flag</li> <li>** HttpOnly flag</li> <li>** Domain flag</li> <li>** Path flag</li> <li>- How are cryptographically session IDs generated</li> <li>** Which cryptographically secure pseudo-random number generator (CSPRNG) is used?</li> <li>** How long are the session IDs?</li> <li>- How are session IDs invalidated</li> <li>** Are session IDs invalidated on the server?</li> <li>** Are Set-Cookie directives included in the response with an expiration time set in the past?</li> <li>** Are cookies deleted when the browser closes?</li> <li>- If encrypted cookies are used</li> <li>** Is the encryption key accessible to the client side?</li> <li>** Is a Hash-based Message Authentication Code (HMAC) used to verify the integrity of state information received from the client?</li> <li>- If the application proved an explicit logout facility in the application`s UI</li> <li>- If the application regenerates session IDs on authentication / privilege change</li> <li>- If all session state information kept on the server side</li> <li>- If the application validates the session ID every time protected data or a protected functionality is being requested</li> <li>- Where the sessions IDs are stored</li> </ul> <p>2. Quality Assurance (QA) test results related to session management (e.g., absolute and idle session timeouts, session concurrency, cookie attributes, session ID randomness, session ID destruction, etc)</p>
--	--

<b>ID:</b>	<b>ASC-5 - Authorization</b>
<b>Description:</b>	<p>Authorization is the concept of allowing access to only those resources permitted to use them. A verified application ensures that (1) persons accessing resources hold valid credentials to do so, (2) users are associated with a well-defined set of roles and privileges and that (3) role and permission metadata is protected from replay or tampering.</p> <p>You can put the authorization logic, the code that enforces those permission policy decisions, into the application itself or into the database layer, or even both.</p>

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

	<p>Authorization Best Practices</p> <ol style="list-style-type: none"> <li>1. Failing closed <ul style="list-style-type: none"> <li>** If anything fails, the application will fail into a secure state</li> <li>** Consider configuring the top most exception-handling mechanisms in your application framework to take a known-safe action when encountering an unexpected, unhandled error. (E.g., immediately invalidating the user's session ID and redirecting the user's browser back to the application's root.)</li> </ul> </li> <li>2. Authorizing on every request <ul style="list-style-type: none"> <li>** Authorization is not a one-time event. It should happen at many points and many times within an application.</li> </ul> </li> <li>3. Centralizing the authorization mechanism <ul style="list-style-type: none"> <li>** Design a clean authorization architecture that can be easily shared across the entire application.</li> <li>** Factor your authorization code into a library that can be easily called when needed.</li> </ul> </li> <li>4. Minimizing custom authorization code <ul style="list-style-type: none"> <li>** Writing custom authorization code is difficult, expensive, and prone to give you worse results than if you used a reliable, well-tested, off-the-shelf authorization module.</li> </ul> </li> <li>5. Avoiding insecure client-side authorization tokens <ul style="list-style-type: none"> <li>** Cryptographically secure client-side tokens are acceptable- ones that are made opaque through strong encryption and where the decryption keys are not available to the client.</li> </ul> </li> <li>6. Using server-side authorization <ul style="list-style-type: none"> <li>** Authorization checks should happen on the server and never solely on the client.</li> </ul> </li> <li>7. Use trusted data source <ul style="list-style-type: none"> <li>** Servers should rely on only trusted data sources such as LDAP or a back-end database, to provide a subject's access rights at run time.</li> <li>** Do not use hidden form field, URL parameters.</li> <li>** Access rights should always be stored and maintained on the server.</li> </ul> </li> </ol> <p>Sources / References:</p> <ol style="list-style-type: none"> <li>1. Web Application Security, A Beginner's Guide by Bryan Sullivan and Vincent Liu</li> <li>2. Securing Web Application Technologies [SWAT] Checklist <a href="https://software-security.sans.org/resources/swat">https://software-security.sans.org/resources/swat</a></li> </ol>
<b>Evidence Required:</b>	<p>Please provide:</p> <ol style="list-style-type: none"> <li>1. Quality Assurance (QA) test case demonstration that user roles are limited to the privileges identified within the Access Control Matrix <ol style="list-style-type: none"> <li>a. The test case must cover each role identified within the access control matrix</li> </ol> </li> <li>2. Pentest <ol style="list-style-type: none"> <li>a. Purpose of the Pentest is to attempt to defeat authorization mechanism or trick the application into escalating ones privileges</li> </ol> </li> </ol>

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

<b>ID:</b>	<b>ASC-6 - Malicious input handling (parametrized queries, input validation, encoding data)</b>
<b>Description:</b>	<p>The most common application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all the major vulnerabilities in applications, such as cross site scripting, SQL injection, interpreter injection, locale/unicode attacks, file system attacks, and buffer overflows. A verified application ensures that (1) all input is validated to be correct and fit for the intended purpose and that (2) data from an external entity or client should never be trusted and should be handled accordingly.</p> <p>From a pure security perspective, input validation must be performed on the server. Any protections built using client-side techniques can be bypassed by using a simple web proxy. While client-side validation may not be trusted by the server, it tends to be more focused on immediate feedback to the user. Not only does this save a round trip, or many round trips, to the server, it cuts down on the processing the server needs to handle.</p> <p>Input and Output Handling Best Practices</p> <ol style="list-style-type: none"> <li>1. Conduct Contextual Output Encoding <ul style="list-style-type: none"> <li>** All output functions must contextually encode data before sending it to the user. Depending on where the output will end up in the HTML page, the output must be encoded differently. For example, data placed in the URL context must be encoded differently than data placed in JavaScript context within the HTML page.</li> </ul> </li> <li>2. Prefer Whitelists over Blacklists <ul style="list-style-type: none"> <li>** For each user input field, there should be validation on the input content. Whitelisting input is the preferred approach. Only accept data that meets a certain criteria.</li> <li>** For input that needs more flexibility, blacklisting can also be applied where known bad input patterns or characters are blocked.</li> </ul> </li> <li>3. Use Parameterized SQL Queries <ul style="list-style-type: none"> <li>** SQL queries should be crafted with user content passed into a bind variable. Queries written this way are safe against SQL injection attacks.</li> <li>** SQL queries should not be created dynamically using string concatenation.</li> <li>** SQL query string used in a bound or parameterized query should never be dynamically built from user input.</li> </ul> </li> <li>4. Set the Encoding for Your Application <ul style="list-style-type: none"> <li>** For every page in your application set the encoding using HTTP headers or meta tags within HTML. This ensures that the encoding of the page is always defined and that browser will not have to determine the encoding on its own. Setting a consistent encoding, like UTF-8, for your application reduces the overall risk of issues like Cross-Site Scripting.</li> </ul> </li> <li>5. Validate Uploaded Files <ul style="list-style-type: none"> <li>** When accepting file uploads from the user make sure to validate the size of the file,</li> </ul> </li> </ol>

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

	<p>the file type, and the file contents as well as ensuring that it is not possible to override the destination path for the file.</p> <p>** Scanning is required to catch malicious files.</p> <p>6. Validate the Source of Input</p> <p>** The source of the input must be validated. For example, if input is expected from a POST request do not accept the input variable from a GET request.</p> <p>Sources / References:</p> <p>1. Securing Web Application Technologies [SWAT] Checklist <a href="https://software-security.sans.org/resources/swat">https://software-security.sans.org/resources/swat</a></p>
<b>Evidence Required:</b>	<p>Please provide:</p> <p>1. Documentation explaining the management of malicious input</p> <p>The documentation must identify:</p> <ul style="list-style-type: none"> <li>- Which framework is used for output encoding and input validation</li> <li>** If a framework is not used, how are output encoding and input validation handled?</li> <li>- How the application is protected from user input when building SQL queries</li> <li>- How uploaded files are validated and scanned for viruses</li> </ul> <p>2. SonarQube report</p> <p>3. Pentest report</p>

<b>ID:</b>	<b>ASC-7 - Error and exception handling</b>
<b>Description:</b>	<p>The primary objective of error handling and logging is to provide a useful reaction by the user, administrators, and incident response teams. The objective is not to create massive amounts of logs, but high-quality logs, with more signal than discarded noise.</p> <p>High quality logs will often contain sensitive data, and must be protected as per local data privacy laws or directives.</p> <p>A verified application should (1) not collect or log sensitive information if not specifically required, (2) should ensure all logged information is handled securely and protected as per its data classification, (3) and should ensure that logs are not forever, but have an absolute lifetime that is as short as possible. If logs contain sensitive data, the logs become some of the most sensitive information held by the application and thus very attractive to attackers.</p> <p>Error Handling Best Practices</p> <p>1. Display Generic Error Messages</p>

<b>Solicitation No. – N° de l'invitation</b> U6265-218741	<b>Amd. No – N° de la modif.</b>	<b>Buyer ID – Id de l'acheteur</b> 638zm
<b>Client Ref. No. – N° de réf. De client</b> U6265-218741	<b>File No. – N° du dossier</b>	<b>CCC No./ N° CCC – FMS No/ N° VME</b>

	<p>a. Error messages should not reveal details about the internal state of the application. For example, file system path and stack information should not be exposed to the user through error messages.</p> <p>2. No Unhandled Exceptions</p> <p>a. Given the languages and frameworks in use for web application development, never allow an unhandled exception to occur. Error handlers should be configured to handle unexpected errors and gracefully return controlled output to the user.</p> <p>3. Suppress Framework Generated Errors</p> <p>a. Your development framework or platform may generate default error messages. These should be suppressed or replaced with customized error messages as framework generated messages may reveal sensitive information to the user.</p> <p>4. Logs Errors and Exceptions</p> <p>a. Content must not be exposed but error and exceptions must be logged</p> <p>Sources / References:</p> <p>1. Securing Web Application Technologies [SWAT] Checklist <a href="https://software-security.sans.org/resources/swat">https://software-security.sans.org/resources/swat</a></p>
<b>Evidence Required:</b>	<p>Please provide a:</p> <ol style="list-style-type: none"> <li>1. List of error messages displayed when error/exception occurs.</li> <li>2. Log sample containing errors / exception</li> </ol>

DRAFT