STATEMENT OF WORK

1. TITLE

Immigration, Refugees and Citizenship Canada (IRCC) Stakeholder Information Management System

2. OBJECTIVE

IRCC has a requirement for a web-based service that will include a commercial off-the-shelf (COTS) solution for a Stakeholder Information Management System that will enable IRCC users to continue to effectively and efficiently manage a variety of electronic information related to stakeholders and IRCC's interactions with stakeholders.

3. BACKGROUND

IRCC employs over 5,000 people at locations across Canada and abroad. The Department develops and manages policies and programs related to Canada's immigration, refugees, citizenship, integration and passport program.

IRCC regularly interacts with stakeholders, other government departments, provinces and territories and the Canadian public to communicate with and obtain feedback on existing and planned policies and programs. Additionally, around 40 IRCC missions in foreign countries conduct promotion and recruitment activities on behalf of the department. Currently, this information is stored in a web-based relationship management database.

IRCC seeks to put in place a centrally-managed corporate tool to continue to improve accuracy, consistency and reduce duplication in maintaining stakeholder contact information, as well as following the Department's engagement history and facilitating outreach and communications with stakeholders and public newsletter subscribers. It is expected that this tool would also benefit IRCC through a reduction of time and resources required to obtain stakeholder information and manage stakeholder and subscription lists.

4. SCOPE OF WORK

Herein, the Stakeholder Information Management System, is referred to as "the solution".

The solution is to be delivered as a web-based managed service that can be accessed via a secured internet connection by IRCC employees.

The solution must meet or exceed all the mandatory requirements as indicated in the technical evaluation (attachment 4.1)

5. REQUIREMENTS

5.1. MANAGED SERVICE

The managed service must consist of:

5.1.1. The required hardware platforms and storage to support the solution

5.1.2. Any required network, security & platform software/services (e.g. Operating Systems, Databases, Directories, Firewalls) to support the solution

5.1.3. The required application software to support the solution

The managed service must also include:

5.1.4. The required services to implement and configure the solution, inclusive of importing existing data in the solution

5.1.5. The required services to maintain the solution inclusive of software releases, upgrades and bug fixes, as they become available.

5.1.6. Technical support for the solution as described in section 8.3

5.2. SOFTWARE AVAILABILITY

5.2.1. The latest commercial release of the solution must be available by the bid closing.

5.2.2. The solution must include software releases, upgrades and bug fixes, as they become available.

5.3. TECHNICAL ENVIRONMENT

5.3.1. The solution and all stored data must be hosted on a dedicated secure server within Canada which aligns with the requirements listed in Appendix A.

5.3.2. The solution must provide for real-time security monitoring and notifications to IRCC for security events by e-mail which aligns with the requirements listed in Appendix A.

5.3.3. The solution must permit selected user and administrative actions to be audited/tracked. The auditing function should provide details on who performed changes on specific fields in a record, when a record was last updated and by whom.

5.3.4. The solution must use data information to and from (interoperate) with Microsoft Outlook 2013 service pack 1 and compatible with future versions of Microsoft Outlook.

5.3.5. The solution must use data information to and from (interoperate) with Microsoft Outlook 2007 (12.0.6680.5000) service pack 3 and must be compatible with future versions of Microsoft Outlook.

5.3.6. The solution must be compliant with the version of Windows Internet Explorer 11 in use at IRCC - Support only TLS version 1.2 – 256-AES cipher as well as future versions of Internet Explorer and other internet browsers (e.g. Firefox, Chrome).

5.3.7. The solution must allow use of files with the following formats: jpg, jpg2000, tiff, bmp, xls, xlsx, xlsm, ppt, rtf, mso, txt, pdf, pptx, doc, docx, and docm.

5.3.8. The solution must accommodate at minimum 500 users and has the capability to scale to increase users.

5.4. SYSTEM ADMINISTRATION

5.4.1. The solution must permit IRCC Account Administrators to assign access rights to an individual staff member or a group of multiple staff members.

5.4.2. The solution must not allow operations to be performed on database objects unless the user is authorized for the operation concerned.

5.4.3. The solution must provide the ability to control various types of user access rights capability including:

5.4.3.1. read-only,
5.4.3.2. view or not to view,
5.4.3.3. right to delete or not delete,
5.4.3.4. right to modify or not modify,
5.4.3.5. right to create/add records,
5.4.3.6. right to generate reports
5.4.3.7. right to perform system administrator tasks.

5.4.4. The solution must permit IRCC Account Administrators to create, manage and maintain information contained in the user accounts of all IRCC staff members.

5.4.5. The solution must allow or be configured to allow IRCC Account Administrators to manage the structured keywords or tags that users may associate with records for easy identification, permitting Account Administrators to create, delete/archive, and rename keywords or tags.

5.4.6. The solution must provide, or can be configured to provide a list of the operations and authorizations that an individual user or group or class of users is able to perform within the solution at either the application level or the database level.

5.4.7. The solution must provide an auditing facility which records the information for the database updates, insertions, deletions and selects by individual users on any selected individual object.

5.4.8. The database must accommodate at minimum 50 concurrent users.

5.4.9. The solution must allow administrators to segregate or hide certain data (e.g. specific subscription lists) so that only select groups can view and edit it.

5.5.BUSINESS FUNCTIONALITY

5.5.1. The solution must include or must be configured to include, standard database fields for contact information, including, but not limited to:

5.5.1.1. Contact name and surname
5.5.1.2. Organization
5.5.1.3. Job Title
5.5.1.4. Address
5.5.1.5. E-mail and alternate e-mail address

5.5.1.6. Telephone and alternate telephone numbers (work, cell, fax)
5.5.1.7. Postal Code
5.5.1.8. Country
5.5.1.9. Preferred language of correspondence

5.5.2. The solution must allow for the ability to set mandatory fields.

5.5.3. The solution must allow users to edit, create and associate at least 50 keywords or tags to each record.

5.5.4. The solution must allow for users to associate tags or keywords to records for the purpose of grouping/linking records together and facilitate searching.

5.5.5. The solution must include a notes function that users can post against a record.

5.5.6. The solution must not limit the number of notes that users can post against a record.

5.5.7. The solution must include a calendar/event planning function which allows information to be categorized by date and group.

5.5.8. The solution must not limit, or can be configured to not limit the number of calendar items that users can post against a record.

5.5.9. The solution must have a calendar/event management function that allows internal users to send invitations to external stakeholders through e-mail. Stakeholders should be able to accept, decline and or nominate a delegate through the e-mail invitation (through buttons or integration with MS Outlook).

5.5.10. The solution must have a calendar/event management function that allows internal users to add event records (short entries to mark upcoming events) and manage RSVPs to particular events within the solution or through integration with MS Outlook.

5.5.11. The solution must not limit, or can be configured to not limit the number of calendar items that users can post against a record.

5.5.12. The solution must display, or can be configured to display the name and date of information inputted by users in records, notes or calendar functions.

5.5.13. The solution must allow users to associate an unlimited number of electronic documents, including e-mails to records and calendar items. It must allow the use of files with the following formats: jpg, jpg2000, tiff, bmp, xls, xlsx, xlsm, ppt, rtf, mso, txt, pdf, pptx, doc, docx, and docm.

5.5.14. The solution must allow the launch of an attachment in its native application. It must allow the use of files with the following formats: jpg, jpg2000, tiff, bmp, xls, xlsx, xlsm, ppt, rtf, mso, txt, pdf, pptx, doc, docx, and docm.

5.5.15. The solution must include a listserv function (customizable subscription forms, ability for individuals to subscribe/unsubscribe from e-mails, and automation of e-mail distribution to a list of subscribers).

5.5.16. The solution must have a listserv form that can connect to the IRCC website either through HTML coding or another means

5.5.17. The solution must allow, or can be configured to allow users to create distribution lists based on user-identified criteria, including, but not limited to:

5.5.17.1. stakeholders by name
5.5.17.2. stakeholders by organization
5.5.17.3. stakeholders by activity
5.5.17.4. stakeholders by keyword or tag
5.5.17.5. stakeholders by region (country, province, city)
5.5.17.6. stakeholders by industry or sector
5.5.17.7. The solution must allow users to send individual and bulk e-mails.

5.5.18. The solution must allow users to send individual and bulk e-mail jobs. Bulk jobs must be able to accommodate up to 500,000 or more target e-mail addresses.

5.5.19. The solution must be able to send bulk e-mails at a minimum rate of 50,000 per hour.

5.5.20. The solution must not limit the number of individual or bulk e-mail jobs users can send.

5.5.21. The solution must allow the administrator to merge duplicate records (e.g. stakeholders or tags).

5.5.22. The solution must be able to accommodate at minimum 5 million records and must be scalable to increase volumes.

5.6. SEARCH

5.6.1. The solution must allow users to perform searches using a variety of terms or methods, including, but not limited to:

5.6.1.1. Date or date range
5.6.1.2. Keyword or tag
5.6.1.3. Organization name
5.6.1.4. Contact name
5.6.1.5. E-mail
5.6.1.6. Postal address
5.6.1.7. Web site
5.6.1.8. Telephone number
5.6.1.9. Country, province or city

5.6.2. The search function must allow users to search using full or truncated keywords or terms.

5.6.3. The solution must be able to perform, or be configured to perform, searches for entries listed in records or notes functions.

5.6.4. The solution must keep, or be configured to keep a record history of certain fields (e.g., keep the names and history of previous contact persons).

5.7.USER INTERFACE

5.7.1. The solution must provide a web-based user interface.

5.7.2. The solution must permit the use of the complete Canadian English and Canadian French language character sets based on Unicode UTF-8 v4.1 at a minimum.

5.7.3. The solution must allow, or can be configured to allow users to work in the official language of their choice: Canadian English, and Canadian French.

5.7.4. The solution must provide the users the ability to view all screens, prompts, and on-line help in Canadian English or Canadian French.

5.7.5. The solution must permit the security classification [Protected A] of the database to be marked on all database screens and reports.

5.8.REPORTS

5.8.1. The solution must provide, or can be configured to provide a set of common reports that the user can run within the system, including reports of:

5.8.1.1. stakeholder records by keyword or tag
5.8.1.2. stakeholder records by region (city, province, country)
5.8.1.3. stakeholder notes/interactions by keyword or tag
5.8.1.4. stakeholder events by date or date range
5.8.1.5. stakeholder events by keyword or tag
5.8.1.6. number of e-mail campaigns/jobs sent by date range
5.8.1.7. number of active user accounts

5.8.2. The solution must provide, or can be configured to provide analytic reports on sent e-mails, which include:

5.8.2.1. Read-rate or open-rate
5.8.2.2. Click-rate (the rate at which a URL within an e-mail was clicked on)
5.8.2.3. Opt-outs or unsubscribe
5.8.2.4. Bounces or undeliverable e-mails

5.8.3. The solution must be able to save and print standardized and ad hoc reports.

5.8.4. The solution must allow, or can be configured to allow users to export reports in xlsx or csv and pdf.

Documentation, training, Professional services:

6. DOCUMENTATION

6.1. The Contractor must provide the following documentation in the form of User Guides:

6.1.1. Installation Manual
6.1.2. Administrator Manual
6.1.3. User Manual
6.1.4. Training Manual
6.1.5. The documentation must be up to date with the version of the software being proposed.

6.2. The Contractor must provide IRCC the right to copy or print documentation for the solution. The documentation must be available in electronic form (Microsoft Word).

6.3. The Contractor must provide all documentation in Canadian English and Canadian French.

7. TRAINING

7.1. The Contractor must provide 20 hours of training for System Administrators, End Users and Technical Support resources. This training should include tutorials of the system and its features and question and answer periods. Training can be provided on-site at 70 Crémazie Street, Gatineau, Quebec or remotely via internet meeting.

7.2. The Contractor must supply all applicable training documentation in Canadian English and Canadian French and in electronic (Microsoft Word) format

8. PROFESSIONAL SERVICES

8.1. The Contractor must provide technical services to complete the following tasks within the time specified. Note: times refer to the cumulative level of effort required to complete the task rather than consecutive.

8.2. The Contractor must complete the activities below within three months following the contract award. The IRCC project lead must provide electronic sign-off to mark satisfactory completion of each phase.

8.2.1. Design – the Contractor must complete the development and documentation of the design of IRCC’s solution within 15 business days.

8.2.2. Installation – the Contractor must complete the installation of the solution in IRCC’s development environment within 5 business days.

8.2.3. Configuration – the Contractor must complete the configuration of the solution in IRCC’s development environment within 20 business days.

8.2.4. Data Migration – the Contractor must complete migration of data from .xls to the solution in an IRCC development environment within 5 business days.

8.2.5. Reports Generation – the Contractor must complete the configuration and implementation of Reports in an IRCC development environment within 20 business days.

8.2.6. System Verification – the Contractor must complete system verification of the solution in an IRCC environment within 10 business days.

Project authority will provide sign-off within 3 business days. The vendor will have 3 business days to correct issues if necessary. Should additional time (up to 3 business days as noted above) be required to correct these issues, subsequent phases/milestones would be adjusted accordingly.

8.3. The Contractor must provide technical services for customer support for the duration of the contract period, which includes:

8.3.1. Web-based customer support

8.3.2. Online tracking of customer support requests which identifies the problem, date created and response

8.3.3. Ability to view status of customer support requests

9. DELIVERABLES

The Contractor must provide the following:

Activity / Deliverable	Associated Schedule	Format
9.1. Launch Meeting	Within one week following contract award.	In person at 365 Laurier Avenue West, Ottawa, ON or by teleconference/web conference
9.2. Project Management Documentation 9.2.1. Project Management Plan 9.2.2. Project Schedule 9.2.3. Data Migration Plan 9.2.4. Configuration guides and specifications 9.2.5. Test plan 9.2.6. Implementation strategy and plan	Within three weeks following contract award and when major changes (change requests) are made.	Microsoft Word
9.3. Access to a web-based managed service for a minimum of 50 concurrent users.	Within one month following contract award.	
9.4. User Guides: 9.4.1. Installation Manual 9.4.2. Administrator Manual 9.4.3. User Manual 9.4.4. Training Manual	Within two months following contract award.	Microsoft Word
9.5. Status Reports	Weekly until solution has been fully implemented at IRCC.	Microsoft Word
9.6. Final Report	Within three months following contract award.	Microsoft Word

10.MEETINGS

The Contractor will be required to attend meetings in person at 365 Laurier Avenue West, Ottawa, ON or by teleconference/web conference with the project team as required.

11.TRAVEL

Canada will not pay for travel or living expenses associated with performing the Work. Travel expenses, if any, will be the sole responsibility of the Contractor.

12.CONSTRAINTS

The Contractor will not be able to begin the technical implementation of the solution until the IT Privacy Impact Assessment and Security Assessment and Authorization (SA&A) are completed by Canada.

13. CLIENT SUPPORT

IRCC will provide the following as required for the completion of the work under the Contract:

13.1. Provision of relevant documentation and reference materials via e-mail in Microsoft Word, Excel or PDF format;

13.2. Review of reports/submissions, as required, and the provision of comments/suggested revisions, in a timely manner;

13.3. Coordination of activities and responses from the areas within IRCC to enable the Contractor to provide Services, as these relate to issues identified by the Contractor;

13.4. Provision of all necessary data to support transition to the Stakeholder Information Management System;

13.5. Provision of guidance to the Contractor, where possible and upon request, with respect to the Contractor's obligations in relation to the privacy legislation, regulations, and policies of Canada; and,

13.6. Other assistance and support as appropriate.

APPENDIX A - PRIVACY AND SECURITY REQUIREMENTS

This Appendix describes the privacy and security requirements that the Contractor must meet to ensure that the privacy and security measures specified in this document are implemented and maintained throughout the provision of the Stakeholder Information Management System.

1) Operational Security

a) Data must be stored, accessed and transmitted in accordance with the Government of Canada's "Protected A" security control profile as outlined in ITSG-33 (Communications Security Establishment Canada publication, https://www.cse-cst.gc.ca/en/node/265/html/22839).

b) The Contractor must ensure that all activities carried out in relation to the Privacy and Security Requirements section provide comparable levels of protection to those identified in Government of Canada policies as well as meets or exceeds industry standard or best practice, whichever is greater.

c) The Contractor must prevent its personnel from having access to personal e-mail or instant messaging applications on the computing resources used to conduct the Work.

2) Physical Security

a) The Contractor must implement physical security safeguards to protect Canada's material and information from loss, damage or theft. The Contractor must at a minimum provide the following safeguards:

i) Control personnel access to the facility;
ii) Fire prevention and suppression equipment;
iii) Provide intrusion detection against forced entry;
iv) Monitor the facility;
v) Provide the ability to remove disorderly, disruptive or threatening people from the facility;
vi) Restrict public traffic to one area - Reception Zone;
vii) Provide a secure physical area to host the IT backend systems such as file and database servers containing information related to the Work that meets the standards outlined in RCMP's guideline entitled: G1-031 Physical Protection of Computer Servers; and
viii) Use approved secure containers which provide a comparable national level of protection as Canadian standards (from the RCMP Security Equipment Guide provided by the Project Authority upon request) for the storage of any data related to the Work, including any laptops or tablets.

b) Maintaining authorized access to protected and classified assets and valuables is paramount when being transported.

c) When transporting protected and classified assets from one person or place to another, safeguards must include controlling access to the information by need-to-know. This also applies to the servicing of containers.

d) When transmitting protected and classified assets from one person or place to another, safeguards must depend on proper packaging, an appropriate and reliable postal or courier service and the anonymity of the information while in transit.

3) Information Technology Security

a) The Contractor must safeguard any database or computer system on which the data related to the Work under this Contract is stored from unauthorized access using safeguards. Such safeguards must include:

i) Authentication and authorization controls;
ii) Perimeter defence – firewall;
iii) Intrusion detection;
iv) Network isolation; and
v) Disabling all removable media access to desktop computer, such as: USB ports, Wi-Fi, Disk Drives, DVD/CDROM drive, Bluetooth.

4) Event Logs, Audits

a) The Contractor must maintain audit logs that electronically record all instances of any attempts to access stakeholder information records stored electronically. The audit log must be in a format that can be reviewed by the Contractor and Project Authority at any time. The audit logs must contain at a minimum the following data elements:

i) Originating entity (e.g. user id);
ii) Date and time of event;
iii) Type of event;
iv) Object: unique identifier of the records/data set that was manipulated;
v) Result status (if applicable);
vi) Machine: unique identifier of the machine; and
vii) Location: unique identifier of the location.

b) The Contractor must retain securely the audit logs for at least six (6) months and make the logs available to the Project Authority upon request.

5) Authentication and Authorization

a) The Contractor must store stakeholder information electronically so that a password (or a similar access control mechanism) is required to access the system or database in which the stakeholder information is stored.

b) The Contractor must ensure that passwords or other access controls are provided only to personnel who require access to the stakeholder information to perform the work.

c) The Contractor must implement strong passwords that adhere to the following characteristics:

i) Force a lock-out period after a configurable number of unsuccessful attempts.

ii) Consist of at least eight (8) characters, and include, at a minimum, all of the following requirements:
   i. at least one (1) uppercase letter (i.e., A – Z);
   ii. at least one (1) lowercase letter (i.e., a – z);
   iii. at least one (1) non-alphanumeric character (i.e. %+@!); and
   iv. at least two (2) numerical characters (i.e., 0 – 9).

iii) The Contractor must prompt users to change their password every 84 days.

d) The Contractor must ensure user accounts are promptly removed upon termination of personnel.

7) Malware Prevention

a) The Contractor must install anti-malware software using safeguards onto all IT systems involved in the performance of the Work under this Contract.

b) The Contractor must ensure that anti-virus verification is performed daily and that the virus definitions are updated daily.

8) Network Security

a) The Contractor must encrypt all information that is gathered, stored, transferred and transmitted in system and must use the CSEC approved algorithms specified in ITSP.40.111 *Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information* https://www.cse-cst.gc.ca/en/node/1831/html/26515

9) Other IT Security

a) The Contractor must immediately apply the security patches as recommended by the publisher of the operating system and application vendors on all computing platforms used in the performance of the Work under the Contract.

b) The Contractor must maintain detailed records of any changes performed on information systems processing/storing of stakeholder information. The Contractor must make change and configuration management records available to the Project Authority upon request.

10) Information Management

a) The Contractor must develop and provide the Project Authority with a Security Plan for review and approval. The Security Plan must address, at a minimum, a description of:
   i. The Contractor's security roles and responsibilities;
   ii. The Contractor Security screening process and related personnel security safeguards;
   iii. The physical security safeguards;
   iv. The Contractor security awareness program;
   v. The Contractor configuration management program;
   vi. The Contractor's IT security safeguards (e.g. firewall, authentication and authorization systems, auditing and logging);
   vii. The Contractor contingency planning (business continuity, disaster recovery);

viii. The Contractor’s privacy and security incident response processes;
ix. The Contractor’s audit and accountability program;
x. The Contractor’s internal verification and risk mitigation processes;
xi. The Contractor’s security hardening process;
xii. The Contractor’s operating system and applications patching process;
xiii. The Contractor’s hardening practices and standards; and
xiv. The Contractor’s safeguards around secure containers and the management of their keys and combinations.

b) The Contractor must make available to the Project Authority upon request, all reasonable, pertinent information to allow Canada to conduct a Threat and Risk Assessment, should Canada decide to conduct its own threat and risk assessment of site operations. This information may include, but is not limited to:
i. Policies and procedures;
ii. Security Plan;
iii. Emergency Response Plan;
iv. System logs related to IT system processing/storing stakeholder information;
v. Vulnerability assessment reports;
vi. Penetration test reports; and
vii. User and authorization definition reports.

c) The Contractor must periodically monitor its security posture and provide to the Project Authority at a minimum, the following:
i. Re-assess local security threats at least once a year, or when a significant change demands it;
ii. Conduct security review after a significant security incident;
iii. Conduct vulnerability assessments of system hosts, at least once a year;
iv. Conduct perimeter defence safeguard penetration testing at least once a year;
v. Conduct internal or authorized third party audit of security processes and procedures, at least once a year; and
vi. Conduct information systems and manual logs review, at least once weekly.

d) The Contractor must ensure that all information and systems are segregated for this service from all other information, data, documents or records of the Contractor and not shared with or accessible by the Contractor’s other business lines.

11) Detection, Response and Recovery

a) The Contractor must notify the Project Authority immediately of any security breaches or security incidents related to the performance of the Work under the Contract. Such incidents may include:
i. Unauthorized access, use or disclosure of stakeholder information;
ii. Incidents that may jeopardize the security or integrity of stakeholder information;
iii. Malfeasance (stakeholder information theft, allegations of bribery or blackmail);
iv. Bomb threats;
v. Fire emergencies;
vi. Physical assaults;
vii. Threats (oral/written/telephone);
viii. Break and enter;
ix. Demonstrations/illegal occupations;

x. Vandalism;
xi. Theft (inventoried assets/items);
xii. Damage/loss (material assets);
xiii. Computer malware (e.g. virus);
xiv. IT system security breach; and
xv. Tampering of security containers.

b) The Contractor must develop and document Incident Handling Procedures for privacy breaches and security incidents, including escalation procedures depending on the severity of the breach or incident. Such procedures must include:

i. Taking immediate action to stop the breach and to secure the affected records, systems or websites;
ii. Taking all reasonable steps to resolve the problem and prevent its re-occurrence;
iii. Documenting the privacy breach or security incident;
iv. Notifying the Project Authority immediately of situations where stakeholder information is at risk of being compromised;
v. Notifying the individuals whose information has been disclosed;
vi. Implementing measures requested by the Project Authority;
vii. Documenting the corrective actions taken.

12) Security Reporting

a) Within thirty (30) calendar days after the end of the calendar year, the Contractor must submit to the Project Authority the Annual Security Report containing at a minimum the following:
i. The list of all locations where stakeholder information in electronic format is stored (e.g., the location where any server housing a database including any stakeholder information is located), including back-ups;
ii. The list of every person to whom the Contractor has granted access to the stakeholder information;
iii. The list of all safeguards being taken by the Contractor to protect the stakeholder information;
iv. The list and detailed explanation of any potential or actual threats to the stakeholder information together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and
v. The list and detailed explanation of any new safeguards the Contractor intends to implement to protect the stakeholder information in the next year.

13) Disposing of Records

a) The Contractor must dispose of records and electronic data as prescribed in the Communications Security Establishment publication “ITSP.40.006 v2 IT Media Sanitization” found at https://www.cse-cst.gc.ca/en/node/2206/html/27963.