ANNEX A- STATEMENT OF WORK

Employment and Social Development Canada (ESDC)
Robotic Process Automation Enterprise Solution
STATEMENT OF WORK (SOW)

1. SCOPE

1.1. Introduction

Robotics Process Automation (RPA) is a Commercial Off-the-Shelf (COTS) software solution that engages virtual workers (robots) that mimic high volume, repetitive, rule-based steps in business processes thereby complimenting the human resources allowing them to focus on more value-added tasks.

Employment and Social Development Canada (ESDC) works to improve the standard of living and quality of life for all Canadians. We do this by offering various benefits programs, such as Employment Insurance (EI), the Canadian Pensions Plan (CPP), the Old Age Security (OAS), Job Bank and many other employment and/or social related programs.

1.2. Objectives of the Requirement

Canadians rely heavily on the efficiency and effectiveness of ESDC's processing processes. The Innovation, Information and Technology Branch (IITB) is the functional authority for technological solution at ESDC. IITB provides IM and IT services throughout ESDC. In order to become more efficient and effective, the IITB ADM/CIO is looking to leverage technology to transform ESDC's services and examine end to end business processes that considers multiple views including the Canadians, the users, the employee, the manager, and the IT specialists.

RPA is one tool envisioned to support programs and practitioners so that they can focus on high-value added services. Deployment of new tools need to comply with overall IM and IT enterprise architecture and security requirements that are approved by Shared Services Canada.

ESDC has approximately 30,000 employees and needs to process millions of benefits related transactions annually. To this, we need to add the half a million yearly transactions related to staffing actions and financial transactions to ensure strong operations. ESDC programs and business processes have shown a significant number of repetitive manual tasks, such as duplicative data entry, that can often be inefficient and time consuming.

1.3. Background and Specific Scope of the Requirement

There are continued increases in workload requiring the quick deployment of programs for the Benefits and Integrated Services Branch (BISB) due to a high volume of Employment Insurance and Pensions (Canada Pension Plan (CPP) & Old Age Security (OAS)) inventories and transactions, as well as human resources challenges such as hiring availability, resource retention, limited space, high attrition, etc.
ESDC must look at altering its business processes and leveraging technology to mitigate issues and delays. Currently, numerous manual interventions are required across the various systems and solution, leading to potential data integrity issues and delays.

Therefore, ESDC is looking to streamline, expedite and reduce the manual data entry process through the RPA capability, while assuring data accuracy, reduction in employee workload, and quality, resulting in timely and accurate pay for our employees and Canadians.

Furthermore, ESDC is looking at reducing the cost and time for these related actions and free up capacity to be allocated to other priorities. Forthcoming/later appendices provide additional details on the technical environment. ESDC has investigated the potential return on investment with automation tools to replicate certain processes' manual tasks and has concluded it is the best way forward.

For the reasons above, ESDC has chosen to procure a technology-based solution that, satisfies the RPA functionality services and that meets Government of Canada security requirements while affording a user-friendly means (i.e. easy to set up and utilize by the technological teams) and ensure the ability to implement automated processes to improve client throughput, and reduce manual workloads.

The business processes identified for possible automation, but not limited to, are as follows:

a) Employment Insurance Processing
b) Pension Processing
c) Pensions and Employment Insurance Call Centres
d) Grants & Contributions Processing
e) HR Processing
f) Financial Transaction Processing
g) Configuration Management Processing
h) Call Centre tasks
i) National Services for Employment Insurance
j) Integrity Services transactions

2. REQUIREMENTS

2.1. Business Requirements - Tasks, Activities, and Deliverables

Employment and Social Development Canada (ESDC) has a requirement to purchase an enterprise Robotic Process Automation (RPA) Solution. The application selected must operate on an ***Enterprise-class infrastructure***[1] that is both ***scalable*** [2] and secure from outside threats and data leaks using either on premises or cloud virtual machines (VMs) and must include the following functionality.

2.1.1 - Mandatory requirements

The RPA solution must:

a) include a bilingual interface (Official languages– English and French).
b) operate on an enterprise-class infrastructure using physical and virtual machines (VMs).
c) include a design suite that will allow ESDC to:
   i) develop and deliver automated processes
   ii) develop and implement both attended and unattended 3 bot licences.
   iii) use a bot administration suite that allow ESDC to manage, schedule, and deploy automated processes (for both attended and unattended automations)
   iv) Have autonomous agents, meaning unattended bots that execute tasks and interact with applications or systems independent of human involvement.
   v) perform Enterprise Optical character recognition (OCR) engine.
   vi) must have the following ***Workflow Management system***[4]: Access controls and permission, Customizable dashboards, Form management, Workflow configuration, Business Process automation, Task Management.
   vii) must have the following ***Data Entry functionality***[5]: Abbreviation Detection, data duplication, data retrieval, mis-keyed variation detection, data capture and transfer, Image capture.
   viii) nominate a series of tasks for an automation, via their frontline agents.
   ix) leverage software capabilities such as process mining and process analysis to allow ESDC to capture and streamline existing processes to evaluate candidate for automation.
   x) execute automated processes over cloud-based services like Microsoft's Azure DevOps.

d) Include a complete list of all components and version numbers included in their solution and must include:
   i) all database components required to support the RPA solution
   ii) all web browsers and versions it supports.
   iii) All cloud base services it supports.

---

[1] ***Enterprise-Class Infrastructure*** - Enterprise IT infrastructure refers to the composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment.

[2] ***Scalable*** - should be scalable infrastructure to accommodate data growth and the key to scalable infrastructure is the cloud. Scalable also refer to capacity to increase or reduce the number of robots available.

[3] ***Attended and unattended*** bot - Attended RPA bots take cues from humans to boost productivity, while unattended RPA bots are designed to automate processes without human interactions.

[4] ***Workflow management system*** - A workflow management system (WfMS or WFMS) provides an infrastructure for the set-up, performance and monitoring of a defined sequence of tasks, arranged as a workflow application.

[5] ***Data Entry Functionality*** – RPA data entry functionality data related scenarios such as data cleansing, data extraction, data enrichment, data de-duplication, and data mining.

e) support
   i) hosting on a virtualized x86-64 architecture and must support hosting on a Windows 64-bit operating systems running Windows Server 2016 and later version. Please refer to Cloud infrastructure requirements section for more information.
   ii) the input and output of data from the following file systems:
      (1) Network File System (NFS)
      (2) SAMBA
   iii) Enterprise browser standards(for example, Edge, Chrome, Firefox) without degradation in functionality.
   iv) the packaging and re-deployment of all required components within a given automation process in order to migrate a process from one RPA infrastructure environment to another such as from a Development environment to Production environment.
   v) authentication credentials:
      (1) the solution must obscure all authentication credentials when entered into the RPA solution.
      (2) the solution must obscure the display of all stored authentication credentials once entered into the RPA solution, including any logs.
   vi) vulnerability assessment scanning tools. The Contractor must provide a list of vulnerability assessment products supported by the proposed RPA solution.
   vii) the manipulation of mouse and keyboard events.
   viii) Representational State Transfer (REST) Application Program Interface (API) and Simple Object Access Protocol (SOAP) API.
   ix) Web Interfaces provided by the solution that are be secured using Communications Security Establishment (CSE) approved protocols (e.g. TLS 1.2) and cryptographic algorithms specified in the August 2016 ITSP 40.111 (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.111-eng.pdf). Web Interfaces provided by the solution must provide mechanisms to protect the authenticity of communication sessions including:
      (1) generating a unique, randomly system generated session identifier for each session;
      (2) session identifier must be at least 128 bits;
      (3) recognizes only session identifiers that are system generated; and
      (4) Invalidates session identifiers upon user logout, session timeout or other session termination.
   x) The ***seamless integration***[6] with third party applications.
   xi) ESDC to operating 3,000 to 6,000 attended robots with a variety of attended automations. The RPA solution must allow ESDC to operate 100 to 300 unattended robots with a variety of unattended automations. The solution must have an interface that allow authorized users to modify robots schedule and change the automated scripts used by a robot or a group of robots.
   xii) the work in a modular structure (libraries and or packages) to facilitate reusability of common functions when developing automated scripts.

[6] ***Seamless Integration*** - third party integration is a separate tool designed to connect seamlessly with another product application in order to extend the core functionality of that application system. The software product acts as the central hub where information is collected and shared between each 3rd party system connected to the software product.

f) integrate with
   i) directory services using Lightweight Directory Access Protocol (LDAP) in order to:
      (1) Enforce role-based access control (RBAC) policies defined by ESDC for both bots and authorized users;
      (2) Enforce authentication and authorization for any logical access to information and solution resources; and
      (3) Enforce authentication and authorization before performing any action that creates, views, updates, transmits or deletes data.
   ii) the GOC approved list of applications and interfaces. As an example but not limited to:
      (1) Microsoft Office suite 2016 (Word and Excel)
      (2) Windows-based applications with a Graphical User Interface (GUI)
      (3) Outlook
      (4) Shared folders
      (5) Web applications (ex: Java/.Net)
      (6) Unisys and IBM Mainframe applications (ex : Cobol)
      (7) Desktop applications
      (8) SAP The solution must also support Representational State Transfer (REST) Application Program Interface (API) and Simple Object Access Protocol (SOAP) API.
g) adhere to remote secure login through ESDC network and remote desktop protocols.
h) not require the use of Adobe Flash or Shockwave for any functionality.
i) define, collect and store audit records and events associated with all user or bot operations listed below:
   i) successful and unsuccessful attempts to create, access, modify, or delete security objects including audit data, system configuration files and file or users' formal access permissions;
   ii) successful and unsuccessful logon attempts;
   iii) privileged activities;
   iv) type of activity that occurred;
   v) date and time the activity occurred;
   vi) where the activity occurred;
   vii) the source of activity;
   viii) success or failure outcome of activity; and
   ix) identity associated with activity.
j) employ ***cryptographic mechanisms*** [7] for end-to-end protection of data, from desktop to datacenter, both when in motion or at rest that have been approved by Communication Security Establishment (CSE) and validated by the Cryptographic Algorithm Validation Program (CAVP), and are specified in the August 2016 ITSP.40.111 (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.111-eng.pdf).
k) not interfere with the operation of any Anti-Virus, Anti-Malware, and Host Intrusion Detection systems on a host computer.
l) be compatible with, interacting with, and supporting the manipulation of data within:
   i) Microsoft Office Suite
   ii) Windows-based applications with a Graphical User Interface (GUI)
   iii) Citrix applications displayed in a Windows environment
   iv) Mainframe or terminal screens
   v) SAP
   vi) emulate end user input on:
   vii) Mainframe screens
   viii) Web interfaces
   ix) Microsoft Native thick-client screens
   x) Java Swing thick-client screens

---

[7] ***Employing cryptographic mechanisms*** - The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of Assignment: organization-defined information on Assignment: **organization-defined information system components**.

m) provide a GUI adapter layer between the native GUI and the RPA such that the native GUI and RPA Logic can vary independently. The solution must NOT reference or be dependent on pixel location for bot functionality.
n) store information gathered through the target system for no longer than the duration of the bot interaction.
o) Offer continuous compliance with IT security standards of the ESDC organization.
p) provide Real time:
    i) execution of automation processes and/or requests.
    ii) reporting on application processes speed, performance, and all exceptions and all issues.
    iii) analytics capabilities to run analysis (counting bot executions, automation failures) on a single data source or that combine multiple different data sources.
    iv) operational monitoring to gage efficiency and effectiveness of the digital workforce (ex: number of successful automations executed, failed, etc…).
q) allow ESDC agents to use one or many automated processes as requested
r) allow ESDC to build automated processes that use multiple ESDC systems and platforms.

2.2. Specifications and Security Standards

2.2.1 Technical requirements

The product must:

a) Be a Commercial-off-the-Shelf product;
b) Be web-hosed and accessible via a URL;
c) Provide real-time, sustained, reporting;
d) Be accessible via the following web browsers: Internet Explorer 8 and higher, Chrome, Firefox, Safari;
e) Be stable and restartable: the system does not experience unexpected session log-offs, unresponsiveness/latency or other system failures that are not due to external causes (loss of power; loss of internet connection, inadequate internet connection);

2.2.2 Ease of use

The solution must:

a) offer a login process for developers and administrators (for more details, see 2.6 d));
b) offer a user interface experience evident by not requiring additional training to use the system;

2.2.3 Privacy / security requirements:

The RPA solution must :

a) Be proven compliant with departmental security standards;
b) Allow for ESDC to establish a ***non-identifying client profile***[8] enabling clients to log in via a non-identifying code (password) provided to the client by ESDC; - Guest accounts.
Keep data provided for support services within Canada and must not be used or accessed from outside Canada, in accordance with Treasury Board Secretariat (TBS) Direction for Electronic Data Residency ITPIN (2017-11-07). If support is provided from outside of Canada, the Contractor must allow ESDC to provide sanitized data at its discretion.

[8] ***non-identifying client profile*** - authentication to electronically connected resources is made via credentials, keys, or certificates. RPA toolsets should not have excessive rights, and should not store unencrypted credentials in order to establish connections for automation.

c) Have the ability for clients to provide a non Government of Canada email address or cell phone number to receive a text message enabling a password reset should the ESDC issued password be lost;
d) Have Password-attempt lockout;
e) Have IP restriction for login;
f) Enable each user to establish a unique username and password;
g) Utilize SSL-encrypted SQL authentication;
h) Have the ability for ESDC to define logoff procedures from the central web application and make available automatic log-off of users to further protect session information;
i) Have role-based access for users as designated by ESDC. Roles that must, at a minimum, be supported by the system include:
    i. Administrators (access to all features and capabilities);
    ii. Developers to create and publish RPA procesess.
j) Have SSL encrypted login information;
k) Make available to Adminstrators, for audit purposes, as of the date of service launch, all session data including host name, non-identifying login information, session commands, first connection and last connection time stamps; and
l) Provide to Administrators information relating to the encryption parameters established for each individual engagement, to be logged and available for audit and review purposes as of the date of service launch.
m) Have the ability to assign different roles to different users.
n) Define, collect, and store audit records and events associated with automations (attended and unattended) into the target business applications used by the automations. The RPA solution must provide monitoring functionality on the productivity of the deployed robots. The solution must provide functionality to extra statistics on automations (current, per day, per week and per month). These statistics must be stored and saved and must be extractable for other data manipulations by the RPA administrators (ESDC).
o) Have a Security Assessment (SA&A) be completed prior to the 'signing' a contract and any SA&A security failure will reject the solution. The contract must include clauses to ensure that the contractor must support the ESDC SA&A process through the security deliverables such as security architecture, operational security procedures, build and implementation technical details, security testing plan and results. This will involve at minimum the aforementioned artefacts.

2.3. Technical, Operational and Organizational Environment

The RPA solution must:

a) support cloud and/or on premise hosting on a x86-64 architecture (virtualized for the Cloud) and a Windows 64-bit operating systems running Windows Server 2016 and later versions and/or a Red Hat Linux Operating system for managing large volumes of user sessions

b) Allow installation and use of the Robotic Process Automation (RPA) Enterprise Solution in a protected B cloud environment or on premise environment.

c) Follow Government of Canada security standards, guidelines and best practices

d) Require limited(1 connection) or no linkages to networks outside of the Government of Canada for installations and daily operations operation.

e) Interact with developed application solutions or RPA tools or Artificial Intelligence solutions that are either in the cloud environment or on the on premise environment.

f) The RPA solution must support GoC standard web browsers – MS Edge, Internet Explorer, Google Chrome, Mozilla Fire Fox.

Required for a cloud hosted environment only:

a) being able to work with the various cloud offerings and services (MS AZUR/AMAZON / Oracle/ VULTR/ Google ...)
b) Ability to offer Software as a Service (SaaS) as a potential solution

2.4. Reporting Requirements

The selected tool must have reporting capabilities in both official languages. Audit reporting and Perfomance metrics must be included on an adhoc and scheduled basis.

2.5. ESDCs Obligations

Project engagement

a) ESDC will respond to the Contractor's weekly briefings and any ad-hoc questions that arise durign the selection process in a 2 working days basis;
b) ESDC will provide the video-conferencing account to faciliate knowledge transfer and meetings

2.6. Contractor's responsibilities /obligations for the Proof of Concept (see Appendix B)

a) The Contractor must develop and implement an RPA solution including:
    i. design and configuration of RPA solution based on business process evaluation;
    ii. testing of the design including development of User Acceptance (UA) test cases; and
    iii. create problem and resolution log(s).
b) The Contractor must provide ESDC a written RPA strategic enterprise implementation plan which includes recommendations on the following:
    i. ESDC infrastructure requirements;
    ii. best practices for business and IT RPA centres of expertise (CoE);
    iii. business process evaluation and creation of inventories of potential RPA candidates;
    iv. development, testing, implementation, and maintenance of the RPA solution ;
    v. training;
    vi. change management
        a. • updates to RPA solution, ESDC applications, and business processes
        b. • deployment between environments
        c. • testing strategy
    vii. bot credential management;
    viii. bot governance;
    ix. business continuity;
    x. contingency planning; and
    xi. Strategy to ramp up from initial RPA pilot to organizational level implementation.

c) Unless otherwise specified, the Contractor must use its own equipment and software for the performance of the work;
d) A dedicated member of the Contractor's IT team must be provided by the Contractor to adminsister and oversee the project; and have the ability to engage via video conference, should the Contractor be located outside of the NCR.
Meetings will be conducted via teleconference or video-enabled conferencing. No onsite meetings at an ESDC workplace or office will be required. Further consultations or clarifications will be done as required.

Training:

e) Deliver online/video training to IT employees (developers, administrators) covering the various features and components of the software solution. Additionally IT employees will need training on how to develop and maintain the bot configurations, how to administer the bots on a daily basis, and how to monitor the bots' performance. The Contractor will also supply the ESDC with user guides and with technical specifications.
f) The Contractor must provide training of the RPA solution to ESDC employees for the following:
    i. **Developer Role**
        1. Provide technical instruction for all features and components of the software solution including:
        2. Bot development
        3. Bot deployment
        4. Bot maintenance
    ii. **Administrator Role**
        1. Provide technical instruction for various administrative tasks that are included in the software solution including:
        2. Administration Functions
        3. Credential Management
        4. Monitoring
    iii. The training must be provided in English.

2.7. Constraints

All information provided by ESDC to the contractor shall be used solely in support of this requirement. The contractor shall be required to secure information from unauthorized use and shall not release it to any third party, person or agency external to ESDC without the express written permission of the project authority. Such material(s) must be returned to the project authority upon completion of each task or when requested by the project authority.

The solution will need to integrate:

a) Government of Canada (GoC) standards;
b) Government of Canada accessibility standards; and
c) Official language standards.

The systems will be housed within ESDC and GoC data centers. The RPA software solution will need to connect into all the above systems for the first RPA implementation.

2.8. Location of Work, Work site and Delivery Point

The work will be conducted at the Contractors regular location of work.

2.9. Language of Work

Apart from the requirements outlined the language of work for this requirement will be English.

3. APPLICABLE DOCUMENTS AND GLOSSARY

3.1. Applicable Documents

Annex C – Mandatory and Rated Criteria
Annex E – Proof of Concept

3.2. Relevant Terms, Acronyms and Glossaries

a) RPA: Robotic Process Automation
b) ADM: Assistant Deputy Minister
c) IITB: Innovation Information and Technology Branch
d) CIO: Chief Information Officer
e) COTS : Commercial off the Shelf
f) BISB: Benefits and Integrated Services Branch
g) OAS: Old Age Security
h) CPP: Canadian Pension Plan
i) CSE: Communication Security Establishment
j) PIPEDA: Personal Information Protection and Electronic Documents Act
k) SSL: Secure Socket Layer
l) SQL: Structured Query Language