**RFB for Artificial Intelligence Solutions – Tender 20123**

**ATTACHMENT 2 – DEFINITIONS**

The defined terms contained in Attachment 1-1 Schedule A (Definitions) shall apply to the RFB. In addition, the following terms shall have the following meanings.

“**24/7/365**” means twenty-four (24) hours per day, seven (7) days per week, three-hundred and sixty-five (365) days per year.

**“Accessible”** means that which can be easily reached or obtained; a facility that can be easily entered; information that can be easily accessed; posing no obstacles to persons with disabilities.

**“Accessibility”** means a general term which is used to describe the degree of ease that something (e.g., device, service, and environment) can be used and enjoyed by persons with a disability. The term implies conscious planning, design and/or effort to ensure it is barrier-free to persons with a disability, and by extension, usable and practical for the general population as well.

“**Adware**” means Software that can display advertising banners while a program is running or via some other triggering mechanism.

“**Agent**” means Software that performs information gathering or processing tasks, usually transmitting data to a centralized location.

“**Agreement**” means the agreement to be entered into with the Preferred Bidder(s) as set forth in Attachment #1 – Form of Agreement.

“**AI**” is the acronym for Artificial Intelligence.

“**Annual Refresh**” means the process described in the Description of Deliverables which may result in the qualification of new vendors on an annual basis.

**“Application Programming Interface (API)”** means a set of protocols, routines, and tools that allow different software applications to communicate with each other.

“**Application and Network Security Testing**” is a testing process, utilizing tools and software for penetration testing and/or Red Team engagements. Depending upon the context, the testing process may also refer to penetration testing and/or Red Team exercises performed by security consultants.

“**Assessment/Advisement**” means the capability to conduct feasibility studies, fit-gap analyses, providing solution options & recommendations, and design, implementation and adherence to best practices.

“**Attachments**” are the documents listed in the Qualification Envelope of the RFB and located in the “RFB Attachments” folder, which can be accessed from the ‘RFx’ page, “RFx Details” tab, “Buyer Attachments” section of the OTP eTendering System.

“**Attestation**”means a vendor’s confirmation that any revised or new Solution that is proposed during the Semi-Annual Refresh meets all the Requirements of the RFB for the Category into which the Solution is being placed and for which the Vendor is already qualified.

“**Attestation Form**” means the Attestation document, provided by SO, to be completed by Vendors participating in a Catalogue Refresh, similar to the template provided in Attachment 5 to the RFB, as may be amended by Supply Ontario from time to time.

“**Auditing**” means, in the context of information security, an independent examination of data processing system records to, among other things, validate system controls, ensure object integrity, and to detect potential breaches.

“**Authentication” or “Authenticated**” means the process or condition of identifying an individual or entity. In security systems, Authentication is distinct from authorization, which is the process of giving individuals access to resources based on their identity.

**“Availability”** means ensuring timely and reliable access to and use of information.

“**Bid**” has the meaning set out in Attachment 1 (Form of Agreement).

“**Bidder**” means the legal entity that submits a Bid in response to this RFB.

“**Bid Form**” is the part of a Category Bid in which the Bidder submits their proposed Solution for that Category.

“**Business Hours**” means the hours from 9AM to 5PM on any Business Day

“**Catalogue**” means the collection of information and data relating to qualified Solutions provided by a Vendor in Catalogue submission(s).

“**Catalogue Refresh**” means the process described in the Description of Deliverables which may result in a semi-annual revision to the Catalogue.

“**Category**” means any of the Solution categories described in Attachment #1-2 (Description of Deliverables) of the RFB, to which specific criteria and Requirements apply.

“**Category Bid**” refers to a Bidder’s response to the Requirements and Bid Form within an individual Category RFx. A Category Bid will only be considered if it is part of a Bid that has passed the Qualification envelope in the evaluation process.

“**CD**” means a compact disc which is a type of optical media used for storing digital data.

“**Ceiling Price**” is the maximum amount, specific to a Solution, that may be charged by a Vendor for the Solution as determined by applying the Minimum Discount to the Price.

**“CIFS”** is the acronym for Common Internet File System.

“**Client**” means, for the purpose of Part 3 of the RFB, an OPS Entity who is allowed to procure Solutions under the VOR arrangement arising from this RFB or a Non-OPS Entity who has entered into a separate agreement with a Vendor in accordance with the VOR arrangement and is allowed to procure Solutions under that separate agreement.

“**Common Vulnerabilities and Exposures**” is a list of entries each containing an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities.

“**Common Vulnerability Scoring System”** or **“CVSS**” is an industry standard for assessing the severity of computer system security vulnerabilities. The current version of CVSS (CVSSv3.1) was released in June 2019.

**“Company Level Check”** has the meaning set out in the Attachment 1 (Form of Agreement).

**“Company Security Officer”** has the meaning set out in the Attachment 1 (Form of Agreement).

“**Configuration**” means the computers, processes and devices that compose the Solution and its boundary. More generally, the Solution configuration is the specific definition of the elements that define and/or prescribe what a Solution is composed of. By extension, Solution configuration also refers to the specific settings that have been set by default, automatically or manually by a given program, administrator, or user.

**“Console”** means a logical device used for communication between the user  and  the system.

“**Contractor Security Screening**” means a security screening check that individuals performing work for the OPS on behalf of a Vendor will be required to participate in, as described in the RFB and Attachment 1 (Form of Agreement).

“**COTS**” is the abbreviation for Commercial Off-the -Shelf.

**“Credit Check”** has the meaning set out in the Attachment 1 (Form of Agreement).

**“Criminal Record and Judicial Matters Check (CRJMC)”** has the meaning set out in the Attachment 1 (Form of Agreement).

**“CSA STAR”** means the Cloud Security Alliance’s Security, Trust & Assurance Registry. It is a security certification.

**“CSP”** refers to a Cloud Service Provider.

“**CSS**” has the same meaning as "Contractor Security Screening".

“**CSV**” is the acronym for “comma-separated values”.

“**CVE**” has the same meaning as “Common Vulnerabilities and Exposures”.

“**Cyber Security**” means the business unit within MPBSD.

“**Data Mining**” means the process of autonomously extracting useful information or knowledge from large amounts of data to produce data content relationships.

**“Deliverable(s)”** has the meaning set out in Attachment 1 (Form of Agreement).

“**Discount**” means the percentage by which a Vendor will reduce the Price of a Solution.

**“Data Loss Prevention (DLP)”** means a set of strategies and tools used to ensure that sensitive or critical information does not leave the organizational boundaries.

“**Domain Name System” or “DNS**” means a system of mapping numeric IP addresses to text names.

**“Driver’s Record Check”** has the meaning set out in the Attachment 1 (Form of Agreement).

“**Effective Date**” has the meaning set out in Attachment 1 (Form of Agreement).

“**EFT**” is the abbreviation for Electronic Funds Transfer.

**“eIDAS Regulation”** is the acronym for the "Electronic Identification, Authentication, and Trust Services Regulation."

“**Encryption**” is the translation of data into a secret code, generally using some form of mathematical algorithm.

**“EPS”** is the acronym for “events per second”.

**“Equivalent”** means a product or material, or a part of a manufactured product, or a technical standard that: (i) is of a similar size and quality, (ii) works and performs in substantially the same way, and (iii) accomplishes substantially the same result, to that of a particular product or material forming part of the Work [is this term defined?], of a manufacturer named or referred to in the Contract Documents [not defined], or to a technical standard referred to in the Contract Documents.

**“EST”** is the acronym for “Eastern Standard Time”.

“**Existing Solution**” or **“Existing Product”** means a EIM that is the same as, or an earlier version of, a Solution and has been acquired, or was in the process of being acquired by a Client, on or before the Effective Date of the Agreement.

“**Failover**” refers to a backup operation that automatically switches to a standby server or network if the primary system fails or is temporarily shut down for servicing.

“**FAQ**” is the acronym for “frequently asked questions".

“**FIPPA”** has the meaning set out in the Attachment 1 (Form of Agreement).

“**File Transfer Protocol” or “FTP**”is a protocol designed for transferring files over the Internet.

**“Flexible Signature Methods”** means the support for various signature methods, including electronic signatures, typed signatures, and uploaded signatures, to accommodate different user preferences and scenarios.

“**Fragment” or “Fragmentation**”with respect to computer networking, refers to the dividing of packets into smaller pieces for transmission over a medium where the entire packet is too large to be transmitted at once. Each part of a divided packet is referred to as a Fragment.

“**GDPR**” is the abbreviation for General Data Protection Regulation.

**“GO-ITS” refers to the “**[**Government of Ontario Information and Technology Standards**](https://www.ontario.ca/page/information-technology-standards)**”** and has the meaning set out in Attachment 1 (Form of Agreement).

“**GUI**” is the abbreviation for Graphic User Interface.

“**HTML**” See "Hypertext Markup Language".

“**Host**” refers to a device connected to a computer network (e.g., server/workstation) on which the software will be installed.

“**Hypertext Markup Language**” is the standard markup language for documents designed to be displayed in a web browser.

“**HTTP**” See “Hyper Text Transfer Protocol”.

“**Hyper Text Transfer Protocol**” is a set of rules for exchanging files on the Internet.

**“IaaS”, or “Infrastructure as a Service**”, is on-demand access to cloud-hosted physical and virtual servers, storage and networking - the backend IT infrastructure for running applications and workloads in the cloud.

**“IAM” or “Identity and access management”** is a set of processes, policies, and tools for defining and managing roles and access privileges.

“**IFIS**” is the abbreviation for Integrated Financial Information System.

**“Incident Management”** means incidents identified to the enterprise wide and OPSIT Service Desk(s) (“Tier 1”) by a user or through electronic monitoring tools of the technology environment are escalated to the Vendor as the service provider (“Tier 2”) to be resolved as quickly as possible to restore service. An incident is an event that disrupts the proper performance or operation of the desktop environment and that impacts the Customer.

“**Incident response**” as it relates to SIEM is the process, procedure, retention and action of any network security incident handled by the CSOC or any group using the Solution.

“**Infrastructure Technology Services” or “ITS**” is a business unit within the OPS responsible for managing all OPS technology infrastructure systems and services.

“**Installation**” means a security product either acquired from the Catalogue resulting from this RFB, or is the same as, or an earlier version of, a Solution that has been acquired, or was in the process of being acquired by a Client, on or before the Effective Date of the Agreement.

**“Integrity”** means guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity

**“Intelligent Organization and Compliance”** means the automated organization and categorization of documents based on content, ensuring compliance with regulatory standards through regular audits.

“**IT**” is the acronym for “Information technology”.

“**ITS**” See "Infrastructure Technology Services".

“**KPI**” means Key Performance Indicators.

“**Local Area Network” or “LAN**” refers to a computer network that lies within a limited spatial area, generally confined to a single building or group of buildings.

“**M&TS**” is the acronym for "Maintenance and Technical Support".

**“Malware”, or Malicious Software,** is a blanket term for any kind of computer software with malicious intent.

“**Mandatory Requirement**” means a Requirement that is obligatory to be met if a Solution is to be considered qualified in the Category into which the Solution is being proposed by the Bidder.

“**Manufacturer’s Suggested Retail Price” or “MSRP**” is the price that the product’s or solution’s manufacturer recommends.

**“Material Deviation”** means a deviation which, in the Supply Ontario’s opinion, affects in any substantial way the scope, quality, schedule or performance of the work, or which limits in any substantial way the Supply Ontario’s rights or Bidder's obligations under the Agreement.

**“Maximum Time Period for Negotiations”** means the time period specified in section [1.5.3] of Attachment 3 Terms and Conditions of this RFB within which Supply Ontario requires Negotiations to be completed. Supply Ontario may at any time extend the time period.

**“Measurement Period”** means the time frame over which uptime and service performance are measured, typically on a monthly basis.

**“Metadata”** refers to structured information that describes and provides context for other data, making it easier to retrieve, manage, and use. This can include data definitions, origins, relationships, and quality rules, ensuring data integrity and consistency across different solutions.

**“Master Data Management (MDM)”** refers to the practices and technologies used to ensure the uniformity, accuracy, and consistency of key shared data assets across an organization. It centralizes critical data into a single source of truth, ensuring consistent usage across different business units and systems.

**“MFA”** Multi-factor Authentication is an authentication method that requires more than one type of authentication method, for example username/password, and Short Message Service (SMS) verification.

“**Minimum Discount**” means the minimum percentage as set out in the Bid Form, by which a Vendor will reduce the Price of a Solution.

“**SO Representative**” means the individual designated as the point of contact within Supply Ontario for all contract management aspects of the Agreement.

“**MSRP**” See "Manufacturer’s Suggested Retail Price".

**“Mean Time to Recovery (MTTR)”** refers to the average time required to restore a service after a failure.

**“Monthly Service Fee”** refers to the agreed-upon recurring charge paid by the client for the ongoing delivery of services within a given month.

**“Negotiations”** means discussions that occur after all evaluation stages and before execution of the Agreement between Supply Ontario and a Bidder on the Negotiable Topics as specified in the RFB for the purpose of reaching mutually agreed to terms. Negotiations will be conducted in English and each party shall bear its own costs.

**“Negotiable Topics”** means the proposed changes the Bidder identifies in the Negotiable Topics Form as part of their Bid.

“**Non-OPS Entity**” has the meaning set out in Attachment 1-1 Schedule A Definitions.

“**OAuth**” **or** “**Open Authentication**” is an open-standard authorization protocol or framework that provides applications the ability for “secure designated access.

“**OEM**” means Original Equipment Manufacturer.

**“On-prem”, “On-Prem”, “On-premise” or “On-Premise”** means within a Client’s hosting environment.

**“Other Security Screening Checks”** means higher level checks that may be required when the duties or tasks establish a risk level greater than can be addressed through a CRJMC, Driver’s Record or Out of Country check. Other security screening checks which may be conducted in addition to the CRJMC are those included in the Police Record Checks Reform Act, out of scope of the Act or permitted by regulatory exemption to the Act. Checks are determined on the basis of a ministry risk assessment.

“**Original Equipment Manufacturer” or “OEM**” means the developer of the hardware or software that is being proposed in a Solution.

“**Ontario Public Service” or “OPS**” has the meaning set out in Attachment 1-1 Schedule A Definitions.

“**Ontario Tenders Portal” or “OTP**” is the online bidding portal for procurement competitions within the government of Ontario.

“**Open Systems Interconnection” or “OSI**” was created by the International Standards Organization to help standardize communication between computer systems. It divides communications into seven different layers, each of which include multiple hardware standards, protocols, or other types of services.

“**Other Security Screening Checks**” has the meaning set out in Attachment 1 (Form of Agreement).

**“OTP” and “Ontario Tenders Portal eTenderingSystem”** means the Ontario Tenders Portal electronic tendering system currently hosted by Jaggaer.

**Out-of-Country Driver’s Record Check (US and/or International)** has the meaning set out in Attachment 1 (Form of Agreement).

**“Out-of-Country Police Certificate (US and/or International)”** has the meaning set out in Attachment 1 (Form of Agreement).

**“PaaS”, or “Platform as a Service”,** is on-demand access to a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications.

**“P-Card**” means Purchasing Card.

“**Per Diem**” is a daily allowance given to employees by a company to pay for certain expenses while traveling for business.

“**Performance Warranty Period**” has the meaning set out in Attachment 1 (Form of Agreement).

“**Performance Warranty Services**” has the meaning set out in Attachment 1 (Form of Agreement).

“**Personal Information**” has the meaning set out in Attachment 1 (Form of Agreement).

“**PHIPA**” is the abbreviation for Personal Health Information Protection Act.

**"Preferred Bidder"** means the Bidder (or Bidders in the case of a multiple vendor opportunity) who has the highest cumulative score at the conclusion of the evaluation process set out in the Qualification Envelope.

“**Pricing” or “Price**” is the amount that a Bidder assigns to each of its proposed Solutions in its Catalogue, which Price may be based on the MSRP. Price does not include the Minimum Discount.

**“Problem Management”** means the management discipline that handles a problem from its detection through its final resolution;

“**Product**” has the meaning set out in Attachment 1 (Form of Agreement).

“**Professional Services**” has the meaning set out in Attachment 1 (Form of Agreement).

**“Qualification Envelope”** means Section 1 of the RFB as set out on the Ontario Tenders Portal eTendering System.

“**Qualification Response**” means the content of a Bidder’s Bid in the Qualification Envelope, and any related attachments, including the Form of Offer.

“**Rated Requirement**” a Requirement that is not obligatory but that is assigned a point score for the purposes of the RFB evaluation process. Each Rated Requirement has a point score threshold that must be met or exceeded for the Solution to be considered qualified in the Category into which the Solution is being proposed by the Bidder.

**“RBAC”** Role Based Access Control is an approach to restricting system access to authorized users.

**“Recordkeeping and Access”** the management of information to support the legislative requirements and business needs of ministries and provincial agencies along with facilitating access to information.

“**Refresh**”, “**Refresh Process” or “Vendor Refresh”** has the same meaning as Annual Refresh, which will be used to qualify additional Vendors.

“**RWP**” is the abbreviation for Respectful Workplace Policy

“**Requirement**” means the business and technical requirements for the RFB, and each Category as detailed in this RFB.

“**REST API**” is an architectural style for an application programming interface that uses HTTP requests to access and use data.

“**RFB**” has the meaning set out in Attachment 1 (Form of Agreement).

**“RFB Closing Date and Time”** means the Bid submission date and time as set out in the RFB and as may be amended from time to time in accordance with the terms of the RFB.

**“RFB Contact”** means the person listed in Section 1.1 – Procurement Details.

“**RFx**” is a generic acronym referring to any “Request for ‘x’“. Also see “RFB”.

**“Royal Canadian Mounted Police (RCMP) accredited Third Party Agency”** has the meaning set out in Attachment 1 (Form of Agreement).

**“RPC”** means Remote Procedure Call.

**“Recovery Point Objective (RPO)”** means the maximum acceptable amount of data loss in terms of time, measured from the time of the last successful data backup to the time of service disruption.

**“Recovery Time Objective (RTO)”** refers to the maximum acceptable downtime for a service, measured from the time of disruption to the restoration of service. **"SaaS" or “Software as a Service”** is on-demand access to ready-to-use, cloud-hosted application software.

“**Second-Stage Selection**” is the process more particularly described in the Agreement used by Clients to procure Solutions within Categories from Vendors.

**“Security Clearance”** means a decision made by CSS, SO following receipt of the Security Screening Check documents that will permit the person being cleared toengage in the performance of the services.

**“Security Screening Check”** is the process set forth in Attachment 1 (Form of Agreement).

“**Selected Bidder**” means a Bidder who has been selected by Supply Ontario to enter into the Agreement.

“**Service**” has the definition given to it in Attachment 1 (Form of Agreement).

“**Service Levels”** has the definition given to it in Attachment 1 (Form of Agreement).

**“SKU”** means Stock Keeping Unit.

“**SLA**” means Service Level Agreement.

“**SMS**” means Short Message Service.

**“SOC”** means System and Organization Controls.

**“SOAP”** meansSubjective, Objective, Assessment, and Plan

“**Solution**” has the definition given to it in Attachment 1 (Form of Agreement).

“**SSO**” means Single Sign-On.

“**Statistics Canada**” is an agency of the Canadian Federal Government ([Statistics Canada website](https://ontariogov-my.sharepoint.com/personal/daniel_eugen_ontario_ca/Documents/Documents/O365%20Migrated/_EPB/Projects/ITSec%202019/Statistics%20Canada))

**“Streamlined Signing”** means the provision of electronic signing capabilities that eliminate the need for physical documents, thereby removing the necessity of printing, scanning, and mailing. This functionality significantly reduces processing time and increases efficiency in document handling.

**“Subjective, Objective, Assessment, and Plan”** means structured method used by healthcare providers to document patient encounters.

“**Suite**” means a collection of software that is intended to function together to provide the features and functionality required for the proposed Solution.

**“SO”** is the abbreviation for Supply Ontario

**“TCV number”** means the Bidder’s tax compliance verification number, obtained by following the instructions set forth in Section 1.6.3 of the Qualification Envelope.

**“Technical Envelope”** means Section 2 of the RFB as set out on the Ontario Tenders Portal eTendering System.

**“Technical Response”** means the Bidder’s response to the Technical Envelope and any related attachments.

**“Tenant”** is a term commonly used in cloud computing to refer to a customer’s cloud resources or cloud environments that are distinct and separate from other cloud tenants.

“**Term**” has the definition given to it in Attachment 1 (Form of Agreement).

“**Training**” has the definition given to it in Attachment 1 (Form of Agreement.

“**TTY**” means teletypewriter.

**“Uptime Commitment”** means the percentage of time during a given period (measured per month) that a service is expected to be operational and available.

**“Vendor”** means the Selected Bidder that has entered into the Agreement with Supply Ontario.

**“VOR”** is the abbreviation for Vendor of Record.

**“Vendor of Record for Security Screening Check Services (VOR**)” has the meaning set out in Attachment 1 (Form of Agreement).

“**Vulnerability Management**” means the cyclical process of identifying, classifying, prioritizing, remediating, mitigating software vulnerabilities.

**“Vulnerable Sector Check (VSC)”** has the meaning set in in Attachment 1 (Form of Agreement).

“**WVPP”** is the abbreviation for Workplace Violence Prevention Policy.

**[End of Definitions]**