Service | Innovation | Value

SHARED SERVICES CANADA

Request for Information
for the Procurement Process for
Electronic File Transfer for Statistics Canada

Request for Information No.	R66454	Date	September 25, 2020
GCDocs File No.	R66454	GETS Reference No.	PW-20-00927879

Issuing Office	Shared Services Canada 180 Kent Street, 13th Floor Ottawa, Ontario K1P 0B5	
Contracting Authority (The Contracting Authority is SSC's representative for all questions and comments about this document.)	Name	Sandra Ladouceur
	Telephone No.	(613) 302-0766
	Email Address	Sandra.ladouceur2@canada.ca
Closing Date and Time	November 9th, 2020 @ 2:00 PM (EST)	
Time Zone	Eastern Standard Time (EST)	
Destination of Goods/Services	Not applicable – Request for Information Only	
Email Address for Submitting your Response by the Closing Date	Sandra.ladouceur2@canada.ca	

SHARED SERVICES CANADA

Request for Information for the Procurement Process for Electronic File Transfer

TABLE OF CONTENTS

SHARED SERVICES CANADA

Request for Information for the Procurement Process for Electronic File Transfer

1. General Information

1.1 Introduction

a) **Phase 1 of Procurement Process**: This Request for Information (RFI) is the first phase of a procurement process by Shared Services Canada (SSC) for Electronic File Transfer (the "**Project**"). Suppliers are invited to submit responses to assist Canada in refining its requirements for the Project. Suppliers are not required to submit a response to this RFI in order to participate in any later phases of the procurement process for the Project.

b) **RFI Phase is not a Bid Solicitation**: This RFI is not a solicitation of bids or tenders. No contract will be awarded as a result of the activities undertaken during this RFI. Canada reserves the right to cancel any of the preliminary requirements described as part of the Project at any time during the RFI or any other phase of the procurement process. Given that the RFI process and any related procurement activity may be partially or completely cancelled by Canada, it may not result in any subsequent procurement processes.

c) **Response Costs**: SSC will not reimburse any supplier or any of its representatives for any overhead or expenses incurred in participating in or responding to any part of the RFI phase. Suppliers are also responsible for carrying out their own independent research, due diligence and investigations (including seeking independent advice) that they consider necessary or advisable in connection with their participation in the RFI process and any future procurement process.

1.2 Overview of the Project

a) **Overview of Project**: To replace Statistic Canada's current end of life secured Commercial off the shelf (COTS) to transfer files with partners.

b) **Scope of Anticipated Procurement:**

i) **Potential Client Users**: This RFI is being issued by SSC. It is intended that the contract resulting from any subsequent solicitation would be used by SSC to provide shared services to Statistics Canada. Any subsequent procurement process will not preclude SSC from using another method of supply for any of its clients with the same or similar needs, unless a subsequent solicitation for this Project expressly indicates otherwise.

ii) **Number of Contracts**: Canada is currently contemplating the award of a contract.

iii) **Term of any Resulting Contract**: Canada is currently contemplating a contract for a period of 5 years, plus two option periods of one year each.

c) **Applicable Trade Agreements**: The following trade agreements will apply to the procurement process:

Trade Agreements	Yes/No
Agreement on Internal Trade (AIT)	x
Canada-United States-Mexico Agreement (CUSMA)	
World Trade Organization Agreement on Government Procurement	x
Canada-Chile Free Trade Agreement	x
Canada-Colombia Free Trade Agreement	x
Canada-Peru Free Trade Agreement	x
Canada-Panama Free Trade Agreement	x
Canada-Honduras Free Trade Agreement	x
Canada-Israel Free Trade Agreement	x
Canada-Korea Free Trade Agreement	x

d) **Preference for Canadian Goods and Services**: The requirement may be subject to a preference for Canadian goods and/or services. This will be set out in any subsequent solicitation.

e) **Aboriginal Set-Aside**: The procurement process for the Project may be set aside for Aboriginal business under the federal government's Set-Aside Program for Aboriginal Business.

f) **Controlled Goods Program**: This procurement may be subject to the Controlled Goods Program. The final status of the procurement will be confirmed in any subsequent solicitation.

1.3 Submitting Questions

a) Questions about this RFI can be submitted to the Contracting Authority at his or her email address identified on the cover page up until five (5) working days before the closing date and time indicated on the cover page of this document. Canada may not answer questions received after that time.

b) To ensure the consistency and quality of information provided to suppliers, significant questions received and the answers will be posted on the Government Electronic Tendering Service (GETS) as an amendment to this RFI.

2. Information Requested by Canada

2.1 Comments on Preliminary Documents

This RFI includes the following documents with respect to which Canada is seeking comments from suppliers:

a) Annex A – Electronic File Transfer

All documents reflecting Canada's anticipated requirements for this Project that are provided to suppliers during the RFI process are preliminary or draft requirements only and are subject to change. These requirements, or parts of them, may be updated before or during any subsequent solicitation.

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

3. Supplier Responses

3.1 Submitting a Response

a) **Time and Place for Submission of Responses**: Suppliers interested in providing a response should submit it by email to the Contracting Authority at the email address for submitting a response identified on the cover page by the closing date and time identified on the cover page of this document.

b) **Responsibility for Timely Delivery**: Each supplier is solely responsible for ensuring its response is delivered on time to the correct email address.

c) **Identification of Response**: Each supplier should ensure that its name and return address, the solicitation number, and the closing date are included in the response in a prominent location. The supplier should also identify a representative whom Canada may contact about the response, including the person's name, title, address, telephone number and email address.

3.2 Confidentiality

If a supplier considers any portion of its response to be proprietary or confidential, the supplier should clearly mark those portions of the response as proprietary or confidential. Canada will treat the responses in accordance with the *Access to Information Act* and any other laws that apply.

4. Canada's Review of Responses

4.1 Review of Responses

Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify any draft documents provided with this RFI and its procurement strategy. Canada will review all responses received by the RFI closing date and time. Canada may, in its discretion, review responses received after the RFI closing date and time.

4.2 Review Team

A review team composed of representatives of Canada will review and consider the responses. Canada may hire any independent consultant(s), or use any Government resource(s), to review any response. Not all members of the review team will necessarily participate in all aspects of the review process.

4.3 Follow-up Activity

a) Canada may, in its discretion, contact any suppliers to follow up with additional questions or for clarification of any aspect of a response. Canada's follow-up may involve a request for a further written response or for a meeting with representatives of Canada.

ANNEX A - ELECTRONIC FILE TRANSFER

Acronyms and Abbreviations

Acronym	Description
COTS	Commercial Off The Shelf
EFT	Electronic File Transfer
PWGSC	Public Works and Government Services Canada
RFI	Request for Information
SSC	Shared Services Canada
STC	Statistics Canada

1 BACKGROUND

As Canada's central statistical agency, Statistics Canada exchanges millions of files with external parties. Individual divisions within the Agency receive up to 2 million files per year.

In 2005 Statistics Canada acquired a single point solution to better manage the exchange of electronic file transfers with external parties. The product title Digital Vault was acquired from CyberArk and operated as a network security vault for electronic file transfers.

At that point in time and over the years, the solution met the Agency's requirements. Currently the acquired solution is still operational but is closing in on its end of life.

Statistics Canada would like to replace its current product with a more modern solution capable of adapting to today's new file mediums and storage facilities. The targeted date for deployment of the new solution is March 31, 2021.

2 OBJECTIVE

Statistics Canada, is releasing this Request for Information (RFI) in order to obtain information from the industry regarding a possible product or solution that can permit secure uploading and downloading of Electronic File by external and internal parties over the Internet. The solution should:

1. Enable, support and manage access to an Internet accessible web based file upload and download portal.
2. Enable and support security for all files processed by the Solution.
3. Provide an easy to use web interface with minimal installation requirements for the external parties.

The objective of this RFI is to solicit information from industry so that Statistics Canada can better define its requirements for a possible solicitation. This feedback will assist Statistics Canada in ensuring that its requirements can be best met by a cost effective solution.

Statistics Canada is also looking to solicit comments, concerns and where applicable, alternative recommendations from interested parties regarding how the basic requirements or objectives described in this RFI could be satisfied. Respondents should explain assumptions they make in their responses.

3 NATURE OF REQUEST FOR INFORMATION

This is not a bid solicitation. No commitment exists under this RFI and no award will be granted. The opportunity is published solely for the purposes of collecting market information. Based on the information obtained, Statistics Canada may develop a procurement strategy that may be in the form of competitive bidding, which may lead to a contract award for a solution to meet Statistics Canada needs as it relates to its Electronic File Transfer project.

This RFI will not result in the award of any contract; therefore, potential suppliers of goods or services described in this RFI should not earmark stock or facilities, nor allocate resources, as a result of any information contained in this RFI. Nor will this RFI result in the creation of any source list; therefore, whether or not any potential supplier responds to this RFI will not preclude that supplier from participating in any future procurement. Also, the procurement of any of the goods and services described in this RFI will not necessarily follow this RFI. This RFI is simply intended to solicit feedback from industry with respect to the matters described in this RFI.

This RFI is not a pre-selection process. There will be no short listing of firms for purposes of undertaking future work as a result of this RFI. Similarly, participation in this process is not a condition or prerequisite for participation in an eventual Request for Proposal (RFP). This RFI is neither a Call for Tenders, nor a Request for Proposal, and no agreement or contract will be entered into with any contractor, based on responses to this RFI. The issuance of this RFI is not to be considered in any way as a commitment by Canada, or as authority for the respondent to undertake any work which could be charged to Canada, nor is this RFI to be considered a commitment to issue eventual RFP's or award eventual contracts in relation to this project.

Respondents are asked to identify if their response, or any part of their response, is subject to the Controlled Goods Regulations. Canada shall not be bound by anything stated in this RFI. Canada reserves the right to change all or any part of this RFI as deemed necessary.

4 ENVIRONMENT

4.1 Statistics Canada Networks

Statistics Canada maintains two separate networks. A secure network (Network A) is prohibited from connection to public communications facilities and is permitted to process data that is confidential under the Statistics Act. An accessible network (Network B) permits public access under controlled conditions but there is no processing of confidential data. A store-and-forward service for secure transfer of files between the two networks is provided.

4.1.1 Current Solution - Context Diagram

The Electronic File Transfer Solution will incorporate components in the Internet accessible zone (DMZ) and in the Operations Zone. The Web Server must be hosted in the DMZ zone. The File Server must be hosted in the Operations Zone. The File Transfer Solution includes a File Mover component which will automatically move files between the Operations Zone File Server's file store and the DMZ Web Server's file store. (See Figure 1)

Figure 1 – Statistics Canada Network Structure

4.1.2 Preferred Solution - Context Diagram

The solution should allow for vendor components and client transfer files that can be managed, processed and stored on a Service Management Solution that is cloud compatible with all of the necessary security features intact. The services must interact with the various zones by abiding to the Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG 22) Standards.

The diagram below illustrates one possible example of a solution that may be adapted within the current environment where distinct zones are incorporated to host services. The Solution should include a file management components that will automatically move files between different zones and secure cloud storage. (See Figure 2)

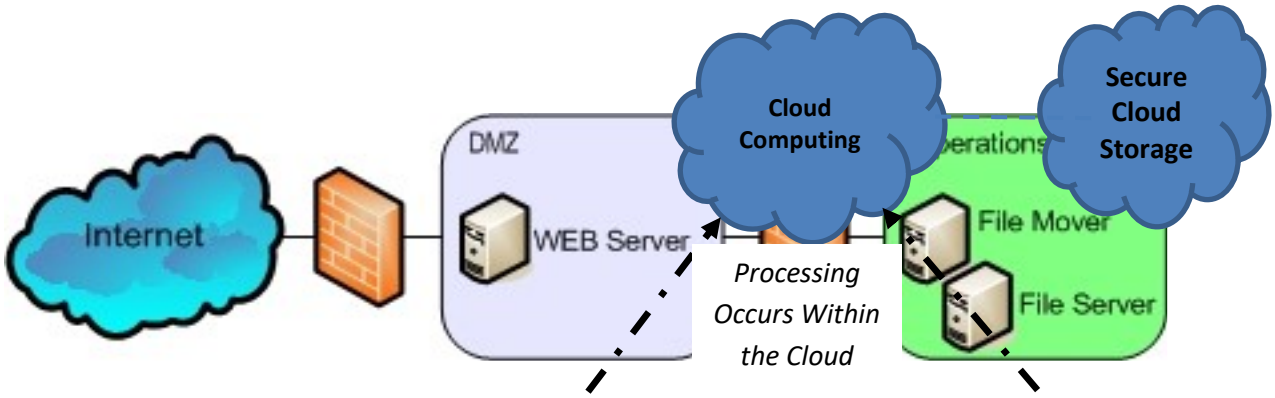

Figure 2 – Example of Statistics Canada Preferred Solution

5 STATISTICS CANADA REQUIREMENTS

To better describe what Statistics Canada is looking for in a solution to its Electronic File Transfer project, the following requirements categories have been identified.

The requirements are grouped into distinct categories. By placing them in their most appropriate category, the process also simplifies the understanding of these requirements. In other words, the set of requirements within each distinct category has a pertinent association to that grouping.

- Account Management Requirements
- Functionality Requirements
- Monitoring and Reporting Requirements
- Configuration Requirements
- File and Data Requirements
- Platform and Environment Requirements
- Security Requirements
- Service Continuity Requirements
- Support Requirements
- Usability Requirements

Respondents can propose a different approach to accommodate Statistics Canada's requirements, provided the results produced are in accordance with the essence of what the requirements must addresses.

5.1 Account Management Requirements

The management of Account and their associated permissions must be facilitated by the EFT solution. In order to accomplish account management, three different concepts must be present in the Solution:

1. **User** – A user is a single account on the EFT Solution. Each user will have a username and password. Each user may be a member of one or more groups.
2. **Group** – A collection of one or more users for which a set of logical Destination permissions can be defined. Each user may be a member of multiple groups.
3. **Logical File Drop Location** – The EFT Solution will consist of a hierarchy of logical destinations. Any user who logs in to the EFT Solution will have the option to upload and/or download files to one or more logical destinations. Each logical destination will have a set of permissions defined.

The solution must have the capability to manage accounts and their associated privileges such that it will accommodate the functionality described in the table below.

Specifics	Account Management Requirement
Creation (Account)	The solution must support the functionality that allows for the creation of a single user account or a bulk creation of user accounts, including passwords, and group memberships.
Creation (Group)	The solution must support the functionality that allow for the concept of a group accounts. A group is a collection of one or more users account for which a set of Logical File Drop Location with permissions can be defined. Each user account may be a member of multiple groups. See Mapping in Account Management.
Creation (Logical File Drop Location)	The solution must support the functionality that allows for the creation of a Logical File Drop Location, with a set of permissions defined. The Logical File Drop Location will consist of either a single destination or a hierarchy of Logical File Drop Locations. Any user who logs in to the solution will have the option to upload and/or download files to one or more logical destination.
External Accounts Management	The solution should have the ability to allow external organizations to manage their own accounts (e.g. password resets).
Passwords	The solution must have the ability to manage user passwords: • Allow password reset/recovery option on web portal in a self-serve fashion • Requesting password reset in web portal, • Advise users of password expiry, • Setting permanent passwords • Notification features before, during and after password renewal
Privileges	The solution should have the ability to assign and manage user access permissions, for both internal and external entities. It must have the ability to set up permissions at the user level to execute file transfers and workflows such as reporting.

5.2 Requirements

The solution must be able to provide basic functionality similar to what is described in the table below. Additional characteristics and details about these features are described in more details in other sections within this document.

Specific	Functionality Requirement
Download / Upload	The solution must have the ability to handle file transfer process between Statistics Canada and external organizations without user intervention. The transfers should have the following features: • Automation and Scheduling • Transfers between different internal networks • Multiple Destinations • Parallel Transfers • Transfer of Data in Open Format
Monitoring and Notification (Arrivals and Transfers)	The solution **must** have the ability to monitor folders for arrival / existence of files to transfer. The solution **must** have the ability to notify the other party that content is being sent before sending data. The solution **must** have the ability to support the functionality to send e-mail file receipts to the user who uploads a file and to the owner of the folder where the file is uploaded.

5.3 Monitoring Requirements

The solution must have the capability to support the monitoring requirements mentioned below such that it will accommodate the functionality described in the table below.

Specific	Monitoring Requirement
Activities Business and System	The solution **must** have the ability to monitor business and system level activities and create the relevant log information for the activity; i.e. external organization status, schedules & actions, performance metrics, network & protocol monitoring.
Notification	The solution **must** have the ability to send notifications of successful or failed file transfers or when storage space is running out or empty.

5.4 Reporting Requirements

The solution must have the capability to support the reporting requirements mentioned below such that it will accommodate the functionality described in the table below.

Specific	Reporting Requirement
Activities (Business and System)	The solution **should** have the ability to report system and business level activities based on relevant log information; i.e. external organization status, schedules & actions, performance metrics, network & protocol monitoring.
Audit Log Export / View and Track	The solution **must** have the ability to allow audit logs to be: • Export for viewing in Excel, SQL, and other applications
Access	The solution should support the functionality to allow access to the activity database so that custom reports can be created. This may be accomplished using either an export feature or an industry supported query language

5.5 Configuration Requirements

The solution must have the capability to allow for the configuration of the solution such that it will accommodate the needs described in the table below.

Specific	Configuration Requirement
Browser (Zero Install)	The solution **must** have the ability to support the basic functionality to upload and download files from a web browser without the installation of any additional components to the web browser.
Define Logical File Drop Location	The solution **must** have the ability to add & remove File Drops locations: • Define a Logical File Drop Location; • Remove a Logical File Drop Location; • Modify a Logical File Drop Location.
Define Connection	The solution **must** have an admin interface to allow for configuration and management of internal and external connections.
File Transfer Configuration	The solution **should** include proprietary software which can be configured to automatically upload files from an external client at a specific time or interval with predetermined rules (i.e. ability to transfer the day before releasing a publication but only transferring once the publication is released) The solution **should** have the ability to quickly configure and manage ad hoc file transfer requests.
Deactivation of Non-Essential	The solution **must** have the ability to allow for non-essential services, logical ports, and protocols to be deactivated on components prior to deployment.

Define Notification	The solution **must** have the ability to set notifications:
	• At each Logical File Drop Location;
	• Ability to add/remove/modify email notifications for multiple distribution lists;
	• Incoming and outgoing transfer notification through emails;
	• Email notifications using a format that supports HTML templates;
	• Error notifications:
	  • Email notification on failure with specific error messages;
	  • Email notification on success to associated users (Internal & External).

5.6 File and Data Requirements

The solution must have the capability to support file and data requirements such that it will accommodate the needs described in the table below.

Specific	File and Data Requirement
Residency and Protected Zone	The new solution **must** guarantee that protected file transfer data are stored in Canada and placed on protected storage.
Sensitive Data	The solution **should** have metadata which is visible to users so that it is clear what the classification of the file is (e.g. Protected B).
Retention and Tracking	The solution **must** have the ability to specify a landing directory file retention period, before auto file deletion is triggered and have the ability to provide history tracking of files.
No Overwriting	The solution **must** support the functionality to handle simultaneous upload and download of files with identical filenames from the same user to the same Logical File Drop Location without overwriting a file.
Data Volume	The solution **must** have the ability to upload and download large size files (terabytes) of data. It **must** have the scalability to handle multiple terabyte (TB) of data per day between Statistics Canada and external organizations, to meet future business growth.
Automatic Restart	The solution **must** have the ability to allow file transmission with an Automatic Restart. It should have the ability to stop an upload or download, and then restart at a later time.
Integrity	The solution **must** have the ability to be able to verify the integrity of uploaded or downloaded files for all type of transmission (Regular and Automatic Restart). It must be able to differentiate between a fully uploaded file from a partially uploaded file and MUST not automatically move partially uploaded files until they are fully uploaded.
Formats	The solution **should** have the ability to receive data coming from open source data providers (Quebec G, NGOs in open format).
Transmission Speed/Time	The solution **must** allow for high speed upload and download transfers. The solution **must** have the ability to perform a file transfer service turnaround time between 5 minutes to a maximum of 24 hours.

5.7 Platform and Environment Requirements

The solution must be able to abide to the platform and environment requirements that are described in the table below. Additional characteristics and details about these requirements may be described in more details within other sections of this document.

Specific	Platform and Environment Requirements
Internal Network	The solution **must** have the ability to transfer files from Statistics Canada open internal network (NETB) to its secure internal network (NETA).
Applications Integration	The solution **should** be able to integrate through the use of API, SDK with other Statistics Canada application (i.e. Service Request Management (SRM), metadata repository (Colectica, Picasso) and CRM.
Software	The solution **must** have the ability to employ leading industry approved desktop platforms OS, OS - Server, Browsers, databases, and Virtual Desktop and MS Outlook email.
Cloud Computing/Storage Virtualization	The solution **must** have the ability to run in a virtual environment on premises and in the cloud. It must abiding to the Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG 22) Standards.

5.8 Security Requirements

In order to simplify the understanding of what Statistics Canada has is looking for in a solution, as it relates to security, the Agency has partitioned its security requirements into distinct groups.

5.8.1 Authentication Requirements

The solution must have the capability to support authentication such that it will accommodate the needs described in the table below.

Specific	Authentication Requirements
Identity Management System	The solution **must** support the functionality to authenticate users using an external standard Identity Management System such as LDAP directory but not limited to it, with strong multi-factor authentication. Especially for information rated as Protected B information.
By Roles / Function / Data	The solution **must** have the ability to authenticate by roles, with different access privileges for system functions and data, i.e. regular user versus administrator roles.
Identity and Access	The solution **must** uniquely identify clients prior to permitting access to regular or sensitive data and information assets. The solution **must** only permit access based on need to know & Least Privilege.
Privileges	The solution **must** accommodate Statistics Canada requirements so that incoming data may not be stored in a way in which anyone other than authorized Statistics Canada employees and the receiving party can recover the plaintext. Only users with proper authority must be able to recover the original content.
Restriction	The solution **must** provide the ability to control the assignment of privileged access entitlements (e.g. “Limited Administer” entitlement, or “Administer” entitlement) associated with roles.
Session Termination	The solution **must** ensure authenticated sessions must be terminated after a period of inactivity by the client, and require re-authentication to gain access to the solution.

5.8.2 Certification Requirements

The solution must be compliant with the certifications specified in the table below.

Specifics	Certification Requirements
Standards	The solution **must** be compliant with FIPS140-2, Soc1, SOC2, SOC3 and possibly other stringent data security requirements
Cryptography	The solution **must** be compliant with cryptographic standards specified by Canadian Centre for Cyber Security for Protected B or higher information (i.e. algorithms implemented such as AES256, RSA2048, SHA2, and possibly other stringent security cryptographic algorithms requirements).
Cryptography	The solution **must** have its cryptographic module on CMVP (Cryptographic Module Validation Program) managed by CSE and NIST.

5.8.3 Data Requirements

The solution must have the capability to support data security such that it will accommodate the needs described in the table below.

Specifics	Data Requirements
Encryption	The solution **must** accommodate Statistics Canada's requirements so that all incoming and outgoing data at rest and in transit **must** be encrypted at the appropriate level.
Malware Detection	The solution **must** have the ability to scan incoming and outgoing files for malware.
Protection	The solution **must** be able to safeguard or protect sensitive information in transit between the source and destination. If sensitive information is temporarily decrypted for processes such as malware scanning, safeguards must be in place to ensure it cannot be accessed.
Signature Integrity	When the solution **must** ensure non-repudiation of data, during transport or in storage, a digital signature is required. It **must** have the ability to respect Federal Government Standards such as the support for file integrity using signatures.
Sensitive Data	The solution **must** have the ability to handle protected B information
Verification	The solution **must** verify the integrity (e.g. accuracy) of data during transport or in storage (i.e. by possibly using a secure hash). The solution **must** have the ability to disallow metadata or data to be changed or used except by authorized staff.

5.8.4 Encryption Requirements

The solution must have the capability to support encryption such that it will accommodate the needs described in the table below.

Specifics	Encryption Requirements
Encryption Protocols	The solution **must** have the ability to transfer files over public and private networks using encrypted file transfer protocols. The solution **must** have the ability to support multiple industry file transfer protocols, including but not limited to: TLS, SSH, SCP, SFTP, AFTP, AS2, FTPS, HTTPS. Encryption methods **should** be integrated in the new solution or at least be highly flexible.
Encryption (Zero Install)	The solution's encryption methods **must not** force our data providers to install any proprietary software.
Encryption Constraint	The solution **must** ensure their encryption algorithms comply with the Statistics Canada IT Security Standard. Encryption and Integrity Protection mechanisms **must** use a Statistics Canada approved cryptographic algorithm and key-length.
Protocol (Cloud)	The solution **must** be cloud compatible. It **must** have the ability to support newer Cloud Service Protocols including but not limited to: (Microsoft AZURE, AWS, Google Services and possibly others).

5.8.5 Audit Log Requirements

The solution must have the capability to support audit log requirements such that it will accommodate the needs described in the table below.

Specifics	Audit Log Requirements
Logs Access	The solution **must** have the ability to restrict access to logs containing security events to only authorized individuals. It **should** have the ability to view audit logs (who uploaded which file and when, incorrect login attempts, when passwords were changed, when users were added to groups, and who accessed what, etc.) It should have the ability to access detailed logical file drop location activity & user activity.
Logs Encryption	Transmission of the log files outside of Statistics Canada **must** be encrypted.
Log Retention	The solution **should** have the ability to configure log data retention period to a specific configurable duration or “forever”.
Log Cyber Events	The solution **must** have the ability to detect and log cyber security events.
Logs Failures	The solution **must** have the ability to alert when there is a processing failure with the generation of a log.

5.8.6 Other Security Requirements

The solution must have the capability to support the additional features described in the table below.

Specifics	Other Security Requirements
Network Security Zone	Large volumes of Protected B/Confidential data, as identified through the Risk Assessment Framework (RAF) process, **must** only be stored in the Secure Restricted Zone. The solution **must** have the ability to place files on protected storage. Technology architecture **must** include network security zones.
Proxy Server	The solution **should** support proxy server deployment in the DMZ (PAZ) for better security.
Security Component Configuration	The solution **must** allow STC to take a snapshot of the components' security configuration settings and store them off-line for 1 year after the component is obsolete in accordance with Statistics Canada's Corporate Records Management and Retention Policy.
Document Security Component Configuration	The component's security configuration settings **must** be documented, and provide guidance for the following: a) Account roles and permissions; b) Settings for ports, protocols, services; c) Local, network, and remote connectivity; d) Operational support model.
Destination Verification	The solution **should** have the ability to ensure that contact information does not conflict with the incoming and outgoing expected location by performing data check (i.e. Geolocation). Any conflict should deny sending files outside the scope of Statistics Canada collection or intendent target.
Rule Processing	The solution **must** have the ability to apply rules based on the metadata content and determine if a file can be transmitted or not.
Transfer Attempts	The solution **must** have the ability to limit the number of file transmission attempts to a specified configurable number.
Vulnerability Compliance	The solution **must** be able to address vulnerabilities identified in a project-based scan following the Compliance Assessment Framework process.

5.9 Continuity Requirements

The solution must have the capability to allow for service continuity of the solution such that it will accommodate the needs described in the table below.

Specifics	Service Continuity Requirements
Backup and Recovery	The solution **should** have the ability to support Data Protection processes; i.e. data integrity checks, data replication, backup and recovery.
Disaster Recovery	The solution **should** have the ability to support Disaster Recovery processes. The solution must outline the processes for disaster recovery and restoration, if applicable. The Bidder **should** specify if any remote access is required for this solution, as well as details on primary & secondary site recovery requirements.
High Availability Recovery	The solution **must** be capable of operating in a high availability environment where failover mechanisms are deployed. The solution **must** detect failure and recover with minimum interruptions.
High Availability Redundancy	The solution **should** have the ability to support Disaster Prevention processes; i.e. fault tolerance between systems, local redundancy, and high availability.
Scalability and Performance	The solution **must** have a small footprint that does not overwhelm resources and is easily scalable without any noticeable performance degradation. It must be scalable so that it will continue to function as its context changes in size or volume. The solution MUST enable growth as the user base increases to support at least 100,000 distinct users and at least 5,000 distinct groups.
Compatible Updates	The solution **must** have the ability to accommodate solution updates with respect to industry standards that are upwards compatible to the newest version.

5.10 Support Requirements

The solution must have the capability to allow for support of the solution such that it will accommodate the needs described in the table below.

Specifics	Support Requirements
Locations Notification	The solution **must** have the ability to support users in multiple locations across Canada with service interruption.
Tier Level	The solution **must** have the ability to support Critical Tier level of availability and support.
External Client Training	There **must** be training and knowledge transfer provided to Statistics Canada users to setup schedule for ad hoc knowledge transfers to external users.
Internal STC Training	There **must** be training and knowledge transfer provided to the Statistics Canada support group in order to properly support the solution.

5.11 Usability Requirements

The solution usability must have be able to accommodate the needs described in the table below.

Area	Usability Requirements
Bilingualism Content and Interface	The solution **should** have the ability to support both English and French for both content and external facing user Interface.
Web Accessibility	The solution **must** support the Government of Canadian Standard on Web Accessibility on public facing web sites natively or by providing tool to achieve this requirement.
Interface Dashboard	The solution **should** have a visual user friendly interface such as dashboard for operation, reporting, and monitoring.
Open Standards	The solution **should** be interoperable at its component level allowing its interface to be an open standard to communicate with other products.

6 CONTENT OF RESPONSE

Respondents should explain all assumptions they make in their response.

Respondents are requested to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this RFI could be satisfied.

In addition to written submissions, private sector companies are invited to demonstrate the requested features of their proposed solution to the review team and senior subject-matter representatives involved in this project as outlined in the section titled “Solicited Key Features to Demonstrate”.

To facilitate the review of the responses to this RFI, respondents are asked to address and present the requested information in the order in which the topics are presented. Such topics are described in the following subsections.

6.1 Respondent Information

The respondent should provide background information on the company (or consortium members that would be created to deliver such a solution), company/consortium management team and company/consortium experience in the delivery of similar services.

The respondent shall provide the name, telephone number, and email address of a representative who may be contacted for clarification or other matters related to the response.

6.2 Type of Solution

Considering the requirements provided by Statistics Canada in this RFI, please identify which of the approaches below best describes your proposed solution that will allow Statistics Canada to proceed in the implementation of this project. You may wish to provide a short overview describing your proposed solution to clarify any deviation from the list below.

- COTS product ready for execution by Statistics Canada;
- Hybrid solution involving COTS product and some development by solution provider;
- Service Management Solution - Cloud Computing and Storage (Full or Partial)
- Other (please specify)

6.3 Technical Information

The respondent should provide a description of the product or service(s) that may be proposed to meet or exceed any or all of the requirements stated in the section title “Statistics Canada Requirements”. This description should provide, in sufficient depth, technical evidence that the proposed solution would meet or exceed Statistics Canada’s minimal requirements. The respondent shall specifically comment on and describe the following:

1. Statistics Canada has requested a solution to address its needs as it related to its Electronic File Transfer project. Please describe the minimum technology infrastructure requirements needed that will allow Statistics Canada to meet its objectives.
2. If the proposed solution can operate in a similar fashion on other storage devices such as “Cloud/Shared Folders/Drives”? If so, please also provide a general explanation of what is required to have your solution function on such other mediums, and under which service provider the solution is operating.
3. Any process or transformation that would need to be applied to very large data in order to meet the transmission requirements requested.
4. The data requirements needed for running the solution.
5. Any professional service required to put in place the solution.
6. The resources and availability of technical support.
7. Any professional training service required, if training is required.
8. Identify all requirements set out in your proposed solution that your organization cannot meet or provide. For each element that your organization cannot meet or provide, describe in your opinion why that is and if possible propose an alternative solution.
9. Your opinion of the technical feasibility of meeting all requirements identified.
10. Alternate ways of meeting all requirements (e.g. possibility of multiple solutions).
11. Any other idea or suggestion that may be relevant to the functionality.

6.4 Solicited Key Features to Demonstrate

The respondent is asked to demonstrate how their product or service(s) meet or exceed the key feature requested below. The demonstration should provide, in sufficient depth, technical evidence that the proposed solution would meet or exceed Statistics Canada’s minimal requirements.

1. **Demonstrate Features Related to Basic Functional Requirements:**
   - Automatic Downloads and Uploads
   - Multiple Destination Downloads and Uploads
   - Parallel Transfers
   - Schedule Transfers
   - Monitor Arrivals and Transfers

2. **Demonstrate Features Related to Monitoring and Reporting Requirements:**
   - Monitor business level activities (Actions …)
   - Monitor system level activities (Performance …)
   - Notifications of Transmissions and Storage (Failure /Success, Limited Storage)
   - Allow access to log database to create basic reports and for exports for custom reports

3. **Demonstrate Features Related to Configuration Requirements:**
   - Use of Web Browser without the installation of any additional components (Zero Install)
   - Adding, removing and modifying logical file drop locations
   - Defining how connections and file transmission (time and interval) are performed for regular and ad hoc requests
   - Deactivations of Non Essential Components
   - Defining conditional rules for file transfer
   - Set notifications via email and/or text at file drop location or distribution lists for failures or success with correct message

4. **Demonstrate Features Related to File and Data Requirements:**
   - Protected storage of sensitive data and Residency in Canada
   - Identification of sensitive data to clients data
   - Data retentions mechanism for Auto delete
   - File History Tracking
   - File duplication handling for Upload and Download
   - Daily transmission of large file (terabytes) between peers in various formats i.e. open source
   - Automatic Restart of transmission at last point of termination as defined data requirement
   - File Integrity verification for upload, download and automatic restart
   - Transmission speed and turnaround time metrics for upload and download.

5. **Demonstrate Features Related to Platform and Environment Requirements:**
   - Transmission within distinct LAN internal networks (NetB, NetA)
   - Application Integration with other systems (API, SDK)
   - Use of leading industry approved Software (Browser, Database, MS Outlook, Desktops OS, Server OS, Virtual Desktop, Mobile)
   - Service Management Solution - Cloud Computing/Storage (Full or Partial) with all of the security features intact, using Cloud Service such as Microsoft AZURE, AWS, Google Services and/or possibly others

6. **Demonstrate Features Related to Security Requirements:**
   a. **Authentication Requirements:**
      - Standard identity and account verification using LDAP directory with multi-factor authentication
      - Authentication by Roles and privileges, with administrator control and restrictions
      - Control Access and session termination

   b. **Certification Requirements:**
      - Compliant with FIPS140-2, Soc1, SOC2, SOC3
      - Cryptographic standards Canadian Centre for Cyber Security for Protected B
      - Cryptographic module on CMVP (Cryptographic Module Validation Program)

   c. **Data Requirements:**
      - Data at rest or in transit must be encrypted
      - Ability to scan incoming and outgoing files for malware.
      - Ability to handle protected B information with safeguards for malware scanning without access
      - Federal Government Standards such as the support for file integrity using signatures
      - Digital signature for Non-repudiation of data, during transport or in storage
      - Data integrity (Data and Metadata) during transport and storage (i.e. secure hash).

d. Encryption Requirements:

- Ability to transfer files over public and private networks using encrypted file transfer protocols such as: TLS, SSH, SCP, SFTP, AFTP, AS2, FTPS, HTTPS
- Integrated highly flexible encryption that does not force our data providers to install any proprietary software (zero footprint)
- Complies with Statistics Canada approved cryptographic algorithm, key-length and standards.
- Cloud compatible Service (Microsoft AZURE, AWS, Google Services, others)

e. Audit Log Requirements

- Restrict Access to logs for (viewing user activities (upload, login, passwords changes ...)
- Control log retention, encryption
- Detect cyber events, log failures with notification

f. Other Security Requirements

- Architecture with Network security zones – protected restricted zones for sensitive information
- Architecture supporting proxy server deployment in DMZ (PAZ)
- Allow snapshot of configuration for off-line safe keeping
- Documentation on Security Component Configuration
- Destination data check verification – no conflict with incoming and outgoing location - conflict deny sending to target
- Rule Processing - apply rules based on the metadata to determine transmitted or not
- Limit number of transmission attempts based on configurable settings
- Address vulnerabilities identified in a scan following the Compliance Assessment Framework process.

7. Service Continuity Requirements

- Support Data Protection Processes, data integrity checks, and Backup and Recovery
- Outline processes for disaster recovery including if remote access for recovery is available
- Operate in high availability with failover mechanism and fault tolerance
- Size of solution footprint that is easily scalable
- Scalable to support at least 100,000 distinct users and at least 5,000 distinct groups
- Minimum impact on current resources with no noticeable performance impact if scale up
- Accommodate update that are compatible with industry standards and are compatible to the latest release

8. Support Requirements

- Support in multiple location with service interruption notification
- Critical Tier level of availability and support
- External Client - Training and knowledge transfer
- Statistics Canada Support group – Training and knowledge transfer

9. Usability Requirements

- Support for bilingualism – English and French on external facing user interface
- Support for Government of Canadian Standard on Web Accessibility on public facing web sites
- Visual user friendly interface such as dashboard for operation, reporting, and monitoring
- Interoperable - Open standard to communicate with other products at its component level

6.5 Schedule and Lead Time

Keeping in mind the Agency's targeted date of March 31, 2021 for deployment, respondent should provide an estimate of the timeframe required for the implementation including any estimate on the development time for the design and creation of any required data, if applicable.

The respondent should also clearly identify and describe all assumptions that could impact the delivery.

6.6 Cost Estimates

Based on the proposed solution, the respondent should provide a cost breakdown for all COTS product, licensing, training, and professional services associated to their services. This should also include the following:

- Annual Maintenance cost;
- Service Support cost (i.e. help Desk);
- Configuration and Deployment costs;
- Software as a Service (if applicable).

Where a custom or hybrid solution is being proposed, the respondent should also provide any development and implementation cost.

The respondent should also answer the following questions:

- What is the pricing model and associated pricing structure for all products and services offered (e.g. licensing fees)?
- Does your pricing model provide for a guaranteed fixed cost over a predetermined time period
- What type(s) of contract (e.g. firm unit price; limitation of expenditure; or combination) and method of payment (e.g. monthly; lump sum upon completion) do you feel would be most appropriate for any resulting contract?

The respondent should indicate any significant underlying assumption used to establish these costs estimates and any area that could be potential cost risks.

6.7 Recommendations, Suggestions or Comments

The respondent may provide general feedback and/or any recommendation, input or comment (including technical information) that could assist Statistics Canada in developing a RFP document or refining a statement of work.

The respondent may provide general feedback and/or any recommendation, input or comment that could assist Statistics Canada in minimizing the costs and risks.

7 TREATMENT OF RESPONSES

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

(b) Review Team: A review team composed of representatives of Statistics Canada will review the responses on behalf of Canada. Canada reserves the right to hire any independent consultant, or use any Government resource that it deems necessary to review any response. Not all members of the review team will necessarily review all responses.

(c) Confidentiality: Respondents are advised that any information submitted to Canada in response to this RFI may be used by Canada in the development of a subsequent competitive RFP. Respondents should mark any portion of their response that they consider proprietary or confidential. Canada will treat those portions of the responses as confidential to the extent permitted by the Access to Information Act.

(d) Activity: Canada may, in its discretion, contact any respondent to follow up with additional questions or for clarification of any aspect of a response.

8 RESPONSE COSTS

Respondents will not be reimbursed for any cost incurred by participating in this RFI.

9 CONSTRAINTS

1. Statistics Canada will provide the necessary storage and processing power to accommodate a respondent's solution, provided it is a cost effective and timeliness solution.
2. Respondents must be willing to abide by the provisions of the Statistics Act. The Statistics Act can be viewed at http://laws-lois.justice.gc.ca/eng/acts/S-19/FullText.html