Emploi et Développement social Canada | Employment and Social Development Canada

NOTICE OF PROPOSED PROCUREMENT (NPP)
For
Security Awareness Solution (SaaS and Professional Services) in support of the Cybersecurity Awareness and Training Team (CATT)

UNSPSC: 81162000 – Cloud-based software as a service

Reference Number :	100019420	**Solicitation Number :**	100019420
Organization Name:	Employment and Social Development Canada		
Solicitation Date:	May 10th 2023	**Closing Date:**	June 19th 2023
Anticipated/Estimated Start Date:	July 31st 2023	**Estimated Level of Effort:**	1 Solution and Professional Services on an as and when requested basis
Estimated Delivery Date:	N/A		
Contract Duration:	The period of the Contract is from date of Contract for a period of two (2) years, with the irrevocable option to extend the term of the Contract by up to four (4) additional one (1) year periods.		
Solicitation Method:	Competitive – Open Tender	**Applicable Trade Agreements:**	CFTA, CCFTA, CPTPP, CCoFTA, CETA, CHFTA, CKFTA, CPAFTA, CPFTA, Canada-UK TCA, CUFTA, WTO-GPA
Comprehensive Land Claim Agreement (if applicable):	N/A	**Number of Contracts:**	1

Requirement Details:

Tendering Procedure:

Open Tendering

Description of the Work:

The Cybersecurity Awareness and Training Team (CATT) of the Enterprise Operations of Innovation, Information and Technology of Employment and Social Development Canada (ESDC) requires access to a cloud-based Security Awareness Solution that includes a Software as a Service (SaaS) Training e-learning software library, and a phishing simulation engine, where ESDC can create training materials and conduct phishing simulations in-house. It is also meant to access professional services on an “as and when requested” basis, over a period of up to five (5)

years, to help ESDC with content development, graphic and interface design, planning, deployment, and updating of a bilingual security awareness training program for all ESDC employees.

Security Requirement:

1. The Contractor must, at all times during the performance of the Contract, hold a valid Designated Organization Screening (DOS) and obtain approved Document Safeguarding Capability at the level of PROTECTED A, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

2. The Contractor personnel requiring access to PROTECTED information, assets or sensitive site(s) must EACH hold a valid personnel security screening at the level of SECRET, or RELIABILITY STATUS, as required, granted or approved by the CSP, PWGSC.

3. The Contractor personnel requiring access to PROTECTED information, and assets, or sensitive site(s) with a Privileged User Account must EACH hold a valid personnel security screening at the level of SECRET, granted or approved by the CSP, PWGSC.

4. The Contractor MUST NOT utilize its facilities to process, produce, or store PROTECTED information or assets until the CSP, PWGSC has issued written approval.

5. The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CSP, PWGSC has issued written approval. After approval has been granted, these tasks may be performed at the level of PROTECTED A.

6. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CSP/PWGSC.

7. The Contractor must comply with the provisions of the:

    a. **Security Requirements Check List and Information Technology (IT) Related Security Requirements, attached at Annex E**;
    b. Contract Security Manual (Latest Edition); and,
    c. CSP website: Security requirements for contracting with the Government of Canada, located at www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html.

NOTE: There are multiple levels of personnel security screenings associated with this file. In this instance, a security guide must be added to the SRCL clarifying these screenings. The security guide is normally generated by the organization's project authority and/or security authority.

NOTE: Any Contractor, or third party delivering Cloud-Based Solutions must be approved by Canada. Contractors must comply with the security requirements in the GC Security Control Profile for Cloud-Based GC IT Services for Protected A, Low Integrity and Low Availability (PALL), for the scope of the proposed Software as a Service (SaaS) provided. Prior to contract award, the contractor must provide evidence, and confirmation to Canada of a Cloud Solution assessment using the Canadian Centre for Cyber Security (CCCS) - IT Assessment & Supply Chain Integrity (SCI) Assessment (ITSM.50.100) methodologies (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100) and the Treasury Board of Canada Secretariat defined security guardrails for cloud, performed by the Client Department, or CCCS.

Furthermore, the Client Department IT Security Authority must perform a local IT assessment against the required controls, Guardrails, and cloud security profiles as determined by CCCS. Suppliers must provide the required information to the IT Security Authority upon request. For more information, guidance, and training on how to conduct this local IT assessment contact CCCS at contact@cyber.gc.ca.

Contract Authority:

Email: nc-solicitations-gd@hrsdc-rhdcc.gc.ca

Inquiries:

Inquiries regarding this RFP requirement must be submitted to the Contracting Authority named above. BIDDERS ARE ADVISED THAT BUYANDSELL.GC.CA IS NOT RESPONSIBLE FOR THE DISTRIBUTION OF SOLLICITATION DOCUMENTS. The Crown retains the right to negotiate with any supplier on any procurement. Documents may be submitted in either official language.