ADVANCE CONTRACT AWARD NOTICE

AGRICULTURE AND AGRI-FOOD CANADA – No. 01B68-19-0170

The Department of Agriculture and Agri-food Canada (AAFC) has a requirement for for the provision of a one (1) year contract with two (2) one (1) year option periods for a Simulated Phishing Program to provide AAFC with simulated phishing exercises to assess AAFC employee's cyber security readiness, provide training to those that require it, and produce statistics and detailed reporting to allow AAFC to evaluate its state of readiness against real attacks.

The purpose of this Advance Contract Award Notice (ACAN) is to signal the government's intention to award a contract for these services to;

TJ5 Technologies
225 Mistral Way
Stittsville, ON
K2S 0G7

Before awarding a contract, however, the government provides other suppliers with the opportunity to demonstrate that they are capable of satisfying the requirements set out in this Notice, by submitting a statement of capabilities during the fifteen (15) calendar day posting period.

If other potential suppliers submit a statement of capabilities during the fifteen (15) calendar day posting period that meet the requirements set out in the ACAN, the government will proceed to a full tendering process on either the government's electronic tendering service or through traditional means, in order to award the contract.

If no other supplier submits, on or before the closing date, a statement of capabilities meeting the requirements set out in the ACAN, a contract will be awarded to the pre-selected supplier, as referenced above.

BACKGROUND & SCOPE OF WORK

Email is the single most important business enablement tool for any organization while simultaneously representing the biggest threat to business continuity. Phishing is responsible for 95% of targeted cyber-attacks on organizations and has been responsible for the delivery of ransomware and espionage which can force the shutdown of an organization's email system and connection to the internet for extended periods of time. Phishing is also rapidly evolving and is growing to include SMS Text phishing (aka Smishing). There is currently no technical solution to prevent phishing. Therefore, this 'social engineering' problem is a people problem that requires a simplified non-technical human approach to educate employees.

The primary objectives of conducting Simulated Phishing Exercises are to assess our employee's cyber security readiness and to provide those who require it most, with real-time targeted training such as a "learning moment". We want to simultaneously protect our data while providing invaluable "street smarts" to our employees both at work and in their personal lives. These exercises will provide useful statistics and detailed reporting which will allow us to evaluate our state of readiness against real attacks. The training portion of the program will provide relevant information and explanation on how to identify phishing emails and awareness on how to avoid being phished in future.

ESTIMATE OF COSTS

The proposed contract period will be from the date of signing until November 30, 2020 plus two one-year option periods. The estimated value of the contract is $121,701.00 (applicable taxes included).

MINIMUM ESSENTIAL REQUIREMENTS

Any interested supplier must demonstrate by way of a statement of capabilities that it has the capacity to provide a Simulated Phishing Program which provides:

- A library of exercises covering both SMS phishing simulations and email phishing simulations.
    - Level 1 Email Phishing Campaigns – Includes 3 Campaigns of equal complexity that are data capture based. This is a set of campaigns that requests that the employee click on a link within an email. Clicking then takes them to a spoofed landing page requesting credentials. The moment the employee attempts to enter credentials then the learning moment is presented. (No credentials are captured) Example: Employee is asked to reset their windows password and are diverted to a “Windows” branded landing page with data entry points.
    - Level 2 Email Phishing Campaigns – Includes 3 Campaigns of equal complexity that are attachment based. This is a set of campaigns that educates the employee to follow specific steps whenever they receive an unsolicited email with an attachment.
    - Level 3 Email Phishing Campaigns – Includes 3 campaigns of equal complexity that are difficult in terms of their content. These campaigns are Spear Phishing complexity and are link based. They include very compelling topics to GoC employees. The emails have the look and feel of a standard internal GoC communication including being bilingual. The clues are harder to spot but this promotes the requirement to look harder at their unsolicited emails.
- Agriculture and Agri-Food Canada branded custom landing pages by each simulation.
- The ability to customize the exercises;
- The ability to customize the real-time training sessions;
- Campaign Reports covering statistics;
    - Number of Employees trained – delivered as an aggregate number (excluding individual results by employee).
    - Number of Employees who did not require training – also delivered as an aggregate number.
    - Results by Region, Branch and directorate as well as any additional parameters requested by the client.
    - Benchmarking against trends for each exercise: Comparables for each exercise will be provided against the historical averages with other Government of Canada departments.
- Detailed Executive Reports after each set of 3 Campaigns;
    - Number of Employees trained in each of the 3 campaigns – delivered as an aggregate number (excluding individual results by employee).
    - A comparison of campaigns 2 and 3 with the Baseline (Baseline is the Campaign 1 results for that level or the SMS text Campaign)
    - Number of Employees who did not require training in each of the 3 campaigns – also delivered as an aggregate number.
    - Results by Region, Branch and directorate for each campaign as well as any additional parameters requested by the client.
    - Employee’s training rate: How many employees were trained in 0 of 3 exercises, 1 of 3 exercises, 2 of 3 exercises 3 of 3 exercises.

    - Benchmarking against trends for each exercise: Comparables for each exercise will be provided against the historical averages with other GoC departments.
- A different lesson for each simulation that speaks specifically to the clues inherent in the actual email or SMS the employee received;
- Analysis of the results of each exercise;
- Benchmarking against trends (i.e. Government of Canada, groups of similar size);
- Technical (dry run) testing before each exercise;
- Trusted domains which are controlled, managed and secured;
- Methodology aimed at obtaining results with a simplified and non-technical approach to knowledge transfer;
- Learning and knowledge transfer services in French and English;
- Learning and knowledge transfer that conforms to accessibility guidelines;
- Secure data storage in adherence to Government of Canada data privacy and data storage and residency policies.
- Document safeguarding Capability for Protected Level B

GOVERNMENT OF CANADA REGULATIONS EXCEPTION

The Treasury Board's Government Contract Regulations, Part 10.2.1 Section 6 states there are four exceptions that permit the contracting authority to set aside the requirement to solicit bids. The exception for related to this ACAN includes:

d. "only one supplier person or firm is capable of performing the contract."

LIMITED TENDERING PROVISONS IN ACCORDANCE WITH THE TRADE AGREEMENTS

The North American Free Trade Agreement, the World Trade Organization - Agreement on Government Procurement, and the Agreement on Internal Trade permit the contracting authority to set aside the requirement to solicit bids under the following condition:

b) "For works of art, reasons connected with protecting patents, copyrights, other exclusive rights, or proprietary information or where there is an absence for technical reasons, the goods or services can be supplied by a particular supplier and no reasonable alternative or substitute exists"

JUSTIFICATION FOR THE PRE-SELECTED SUPPLIER

The database, software and customized program is owned, manufactured, sold and distributed exclusively through TJ5 Technologies. TJ5 Technologies maintains all copyright and Intellectual Property privileges for the Program which can only be purchased directly from the company.

TJ5 Technologies Simulated Phishing Program uniquely provides:

- Complexity Levels with Multiple Baselines: TJ5's program mimics real world attacks by grouping simulations into complexity levels - starting with easy (beginner) then intermediate and eventually advanced simulations.

- Canadian Susceptibility Comparables: TJ5's presence in the Canadian Government ensures a meaningful phishing comparable is provided allowing AAFC to benchmark in relation to other Canadian Government organizations. Comparables are based on historical averages collected from over 40 contracts with the federal government, provincial government and crown corporations over the last 5 years.

- Canadian Government Security Clearance: TJ5 provides secure data storage in adherence to Government of Canada data privacy and data sovoreignty regulations. They have Document Safeguarding Capability with the Canadian Industrial Security Directorate to store and protect AAFC data exclusively within Canadian borders.

- Third Party Supply Chain Security: TJ5 does not advertise or market on the internet. Many high profile breaches have occurred through third party supply chain security weaknesses. Most Phishing attacks are initiated by a deep internet search to gather email addresses and a web presence that announces a program of this nature is a security liability.

SUPPLIERS RIGHT TO SUBMIT A STATEMENT OF CAPABILITIES

Suppliers who consider themselves fully qualified and available to meet the specified requirements, may submit a Statement of Capabilities in writing to the contact person identified in this Notice on or before the closing date of this notice.
The Statement of Capabilities must clearly demonstrate how the supplier meets the advertised requirements. Statements of Capabilities must be delivered to and received by the Contracting Authority on or before the closing date.
The closing date and time for accepting Statements of Capabilities is: **Wednesday Decmber 4th, 2019 at 12:00 P.M. (EDT)** to the following address:

Agriculture and Agri-Food Canada
Professional Services Contracting Unit
1341 Baseline Road, Tower 5, Floor 2,
Ottawa, Ontario K1A 0C5
Kyle Harrington
Tel: (613) 773-0732
Email: kyle.harrington@canada.ca

Statements of Capabilities must be sent on or before the closing date. Statement of Capabilities received on or before the closing date will be considered solely for the purpose of deciding whether or not to conduct a more extensive tendering process. Information provided will be used by the Crown for technical evaluation purposes only with respect to a decision to proceed to a further competitive process. Suppliers that have submitted a Statement of Capabilities will be notified in writing of AAFC's decision to proceed to award the contract without a further additional tendering process.
Should you have any questions concerning this requirement, contact the Contracting Officer identified above by email by or before the closing date.
The Crown retains the right to negotiate with suppliers on any procurement. Documents may be submitted in either official language of Canada.