Capitol Region Council of Governments (CRCOG)

REQUEST FOR PROPOSALS:

Cybersecurity Model Policies and Consulting Services

Proposal Deadline

SUBMITTALS MUST BE RECEIVED BY:
September 10th, 2018
12:00pm EST

Submit Proposals to:
Brian Luther
Capitol Region Council of Governments
241 Main Street, Fourth Floor
Hartford, CT 06106

I. INTENT

The Capitol Region Council of Governments (CRCOG) seeks proposals from qualified and experienced consultant/firms to provide a range of Model Cybersecurity Policies. The model policies are intended to serve as templates for internal Cybersecurity procedures for Connecticut municipalities.

CRCOG's IT Services Cooperative member cities and towns will have the option to contract directly with the selected consultant to customize the provided Model Cybersecurity Policies**.** CRCOG's IT Services Cooperative consists of members of CRCOG's Capitol Region Purchasing Council, members of the Council of Small Towns (COST) and direct IT Services Cooperative members.

II. INTRODUCTION/BACKGROUND INFORMATION

On February 21st, the CRCOG Policy Board received a briefing on Cybersecurity from Arthur House, the State of Connecticut's Chief Cybersecurity Risk Officer. The Cybersecurity Action Plan called on Connecticut municipal leaders to take proactive effort to mitigate the growing Cybersecurity risk. In response to the briefing, the CRCOG staff proposed the addition of a Cybersecurity Program as part of the IT Services Cooperative. This program will be managed by both the CRCOG Municipal Services and Public Safety Departments and aims to provide resources to municipalities to assist in the protection of municipal network assets and data.

The Cybersecurity Program consists of two major components, Cybersecurity Information Technology Services and Model Cybersecurity Policies secured through this RFP. CRCOG has a previously established partnership with Novus Insight and currently provides a suite of Cybersecurity IT services that allows municipalities to assess, remediate, and maintain municipal network assets and test and train staff.

The consultant selected from this RFP will work closely with CRCOG and a committee of municipal leaders and other stakeholders to draft Model Cybersecurity Policies. The goal of this RFP is to develop model cybersecurity related municipal procedures and policies that align with industry best practices. The pilot process will provide feedback to ensure the Model Cybersecurity Policies are adequately implementable and customizable for a variety of different size municipalities.

III. CONSULTANT SCOPE OF WORK

The selected consultant shall possess extensive experience and expertise in drafting Cybersecurity Policies for municipalities and other public organizations. Respondents should be prepared to demonstrate a strong background in and understanding of the processes, policies, procedures, systems, practices, and professional standards of Cybersecurity. Respondents should also be prepared to demonstrate their knowledge of the industry best practices and relevant legal requirements to ensure that all materials produced under resulting contracts comply with federal and Connecticut laws. Any respondent shall have a minimum of three (3) years of relevant experience.

The consultant will work with CRCOG and CRCOG member stakeholders to draft the Model Cybersecurity Policies. CRCOG will draw from its members' professional experience to provide insight of their individual procedures and resources and make recommendations that will guide the consultant.

Once the Model Cybersecurity Policies are completed, IT Services Cooperative members may choose to hire the consultant to customize/modify the policies. Through the consultant, CRCOG intends to assist the CRCOG members with customization. Customization may require intimate knowledge of member city and town ordinances.

Model Cybersecurity Policies are separated into four groups and will include, but are not limited to:

On-going Cybersecurity Policies and Procedures

Anti-Virus Software Policy: Policy for protecting municipal hardware and assets against malware, worms, viruses, trojan horses, and other malicious software.

Backup Data Policy: Policy for identifying data deemed necessary for backup protection and the process to upload and store that data.

Confidential Data Policy: Procedure for the collection, storage, protection, use, and deletion of confidential data.

Data Classification Policy: Policy that clearly classifies data based on collection method, confidential status, importance, or other factors.

Data Loss Prevention Policy: Procedure to prevent the loss of data during normal use and in the event of a breach.

Data Security Audit Policy: Procedure to monitor and maintain the number and type of network connections, prevent addition of malicious software, monitor and maintain existing software.

Guest Access and/or Third-Party Connection Policy: Procedure that clearly identifies the procedure and limitations of granting third party and guest access to municipal network assets.

Network Security Policy: Policy that establishes the protocol for securing the municipal network and assets connected to the network.

Online Currency Collection Policy: Procedure for the handling, storage, and disposal of online payment and currency data.

Physical Security Audit Policy: Procedure to maintain physical assets and prevent the addition of malicious hardware.

Physical Security Policy: Procedure that protects municipal network assets from a physical

attack.

Recover Time and Recovery Point Policy: This policy will clearly define recovery time and recovery points needed to restore potential data loss.

Remote Access and/or Virtual Private Network (VPN) Policy: Procedure that clearly defines acceptable off-site access of the municipal network.

Retention Policy: Policy that clearly defines data types and groups, and which data is retained for how long.

Sensitive Data Protection and Encryption Policy: Defines what is considered sensitive data that is gathered, stored, protected, used, or destroyed and establishes proper protocol to protect it from potential threats.

Municipal Staff Cybersecurity Policy Acknowledgments

Acceptable Use Policy: Procedure and limitations for staff to utilize network resources, not limited to the use of the internet, intranet, email, and other municipal network assets.

Data Security Training Policy: Procedure to ensure the effective training of municipal staff. This policy should outline the process in which staff is trained, curriculum, and the timeframe for staff retraining.

Email Policy: Policy that defines the appropriate use of municipal email accounts. This policy should clearly state that municipal emails are public information under the Freedom of Information Act.

Employee Termination Security Policy: Procedure that clearly defines how terminated/exiting municipal employees are debriefed and scrubbed of network access.

Mobile Device / Bring Your Own Device (BYOD) Policy: Defines the appropriate use of mobile devices, (i.e. laptops, smart phones, tablets, etc.) and the responsibility of municipal staff to protect the information and data created and accessed on mobile devices. This policy will also define the parameters to which staff is permitted to use their personal Mobile Devices for municipal work/tasks and the security protocol for municipal staff utilizing personal Mobile Devices.

Municipal Website Privacy Policy and Customer Notice Policy: Outlines the terms of use for municipal websites or websites hosted/maintained by the municipality. It applies to users who visit/use the municipal website/s and what user information is gathered, stored, protected, and used.

Network Access Policy: Policy to establish rules and limitations for accessing municipal network assets.

Password Policy: Policy that clearly defines password security guidelines for municipal staff.

Staff Social Media Conduct Policy: Outlines the appropriate use of personal and municipal social media accounts for municipal staff. This policy will also set parameters for what is considered appropriate content to be posted on municipal social media accounts.

Wireless Policy: Policy that clearly defines the appropriate use of the municipal wireless network.

Cybersecurity Breach Protocol

Breach Notification Policy: Procedure for the dissemination of information during and after a cyber-attack and breach.

Business Continuity Plan: Policy that clearly identifies security priorities of time-sensitive or critical municipal functions. This plan will also outline the list of service protection priorities in the event of a cyber-attack or breach and plan how to protect those services.

Formalized Incident Response Plan: Procedure that clearly identifies priorities and actions in response to an incident.

Cybersecurity Post-Breach Protocol

Disaster Recovery Plan: Procedure to assess damage and implement remedial action once a disaster has occurred with the intent of recovering lost data and/or assets. This plan should also define a disaster.

Post-Breach Investigation Policy: Policy that clearly defines the nature of investigative measures to identify the scope of impact, failed control, attack vector, and remedial action to better prepare for potential attacks.

Each individual Model Cybersecurity Policy should include the following, where applicable:

Purpose: A statement/statements that details the reasons for which the policy exists and is necessary.

Scope: A statement/statements that details the devices, staff, procedures, or practices in which this Policy is applicable or limited.

Policy: A statement/statements that details the principals, rules, and guidelines that influence decisions and actions of the organization.

Exceptions: A statement/statements that details devices, procedures, practices, or circumstances

in which the policy does not apply.

Expected Impact: This statement/statements outlines the goal for the establishment of the policy, if implemented correctly.

Approval: A statement/statements that confirms the policy from the authority responsible for its implementation and practice.

IV. FEE STRUCTURE

Please provide a one-time fee for the creation of the Model Cybersecurity Policies outlined above in Section III. This fee should include all costs related to the creation of the Model Cybersecurity Policies, including direct and indirect costs.

Please provide an hourly rate or rates for customization services. These rates may be tiered according to consultant staff skill levels, include descriptions of these rates. The hourly rate should be fixed for the life of the contract (two or three years).

V. PROPOSAL REQUIREMENTS

A. Submission

Sealed responses must include one (1) physical copy and one (1) electronic copy (via disc or flash drive) in a sealed envelope, labeled *Response to Model Cybersecurity Policies RFP* and addressed to:

Brian Luther
Program Manager
Capitol Region Council of Governments
241 Main Street, 4th Floor
Hartford, CT 06106

Responses are due no later than **September 10th, 2018** at 1:00pm

Note that the submission of any proposal indicates acceptance by the respondent of the terms and conditions contained herein, unless otherwise specifically noted in the proposal itself and confirmed in resulting contracts.

B. Questions

Questions concerning the Request for Proposals must be made to: **bluther@crcog.org**.

No oral interpretations shall be made to any respondent as to the meaning of any of the proposal documents. Every request for an interpretation shall be made in writing via email to **bluther@crcog.org**, with the subject heading *Questions Regarding Cybersecurity Model Policies and Consulting Services RFP***.** To receive consideration, such questions must be received by **Tuesday, August 28th 2018 1:00 PM.**

CRCOG's staff will arrange an addendum, which shall be made a part of this RFP and any resulting contracts, all questions received following the above procedure and the decisions regarding each. CRCOG will post a copy of any addenda to CRCOG's website, located at www.crcog.org**.** It shall be the responsibility of each respondent to determine whether any addenda have been issued and if so, to download copies directly from the CRCOG website.

C. Proposal Format

Respondents are asked to organize their responses in the order requested, in accordance with the following format:

Part 1: Consultant Overview and Plan

1. **Cover Letter**: A letter signed by an officer of the consultant or individual, binding the respondent to all of the commitments made in the proposal. The cover letter should be addressed to:

   Brian Luther
   Program Manager
   Capitol Region Council of Governments
   241 Main Street 4th Floor
   Hartford, CT 06106.

2. **Contact Information**: The name, address, and other contact information of the respondent(s) submitting the proposal. Please include telephone and fax numbers, as well as email and website addresses.

3. **Letter of Introduction**: Provide a letter of introduction with a brief description of your organization/firm, experience in the industry, and number of years drafting similar Cybersecurity Policies.

4. **Qualifications**: Include a detailed description of your organization's qualifications as they relate to this project. Provide the resume and qualifications of the proposed personnel. Include a description of at least three (3) projects completed by the proposed personnel with references to demonstrate successful experience with similar projects, preferably in municipal settings. Include company name, address, contact name, title, phone number, fax number, email and website address of projects listed. This section should include some examples of the required cybersecurity policies listed in Section III.

5. **Project Overview, Plan, and Schedule**: Provide a work plan and schedule, identifying all tasks that will be performed to satisfy the needs and requirements described in Section III. The schedule should not assume a project start date.

6. **Cost Proposal**: Provide figures for all costs relative to the creation of the Model Cybersecurity Policies. CRCOG will not be responsible for expenses incurred in preparing and submitting a response to this RFP. Such costs should not be included in the proposal. The cost proposal should include all information requested in Section IV.

7. **Response Page and Attachments**: Provide completed copies of the response page and attachments included in the RFP.

VI. SELECTION CRITERIA

A selection committee comprised of CRCOG staff and members, will be charged with evaluating the proposals submitted. At its sole discretion, the Committee reserves the right to request additional clarifying information, to conduct interviews with any finalists and to negotiate pricing and services proposals when such action is in the agency's best interest.

The Selection Committee will recommend a single consultant for approval by CRCOG's Policy Board. The recommendation will be based on the following:

- Completeness of the RFP
- Proven, relevant experience of the consultant
- Experience, expertise, and qualifications of the personnel to be assigned
- Understanding of the desired scope of work and proposed approach
- References and feedback from clients
- Cost proposal

VII. PROCRUREMENT SCHEDULE: SUMMARY OF KEY DATES

The following schedule has been prepared for this RFP process. Note that project constraints may cause the evaluation and selection related dates noted below to change.

RFP Release Date:	**August 16th, 2018**
RFP Questions Due to CRCOG:	**August 28th, 2018**
Proposals Due:	**September 10th, 2018**

VIII. ADDITIONAL TERMS AND CONDITIONS

Compliance with Applicable Laws

The successful consultant shall comply with all applicable federal, state and local laws and regulations as may be applicable. The consultant must consider compliance with all regulations applicable. Respondents are advised to review all applicable federal and state regulations prior to submitting a proposal.

The consultant also agrees that it will hold CRCOG harmless and indemnify CRCOG from any action which may arise out of any act by the consultant concerning lack of compliance with these laws and regulations.

Ownership of Proposals/Freedom of Information

All proposals submitted in response to this RFP are to be the sole property of CRCOG, and shall be subject to the provisions of Section 1-210 of the Connecticut General Statutes (re: Freedom of Information). Reports and materials developed by the successful respondent under a contract that

may result from this RFP are considered public information and may not be copyrighted.

Copies of information resulting from this RFP are generally not available until a contract has been formally awarded. Please note that financial statements or other similar information submitted with such response may remain confidential, to the extent permitted by law, if provided in a separate envelope clearly marked "Confidential".

Incurred Costs

This request for proposals does not commit CRCOG to award a contract or to pay any costs incurred in the preparation of a response to this request. CRCOG is not liable in any way for any costs incurred by respondents in replying to this RFP.

Severability

If any terms or provisions of this Request for Proposal shall be found to be illegal or unenforceable, then such term or provision shall be deemed stricken and the remaining portions of this document shall remain in full force and effect.

Oral Presentation

Respondents who submit a proposal in response to this RFP may be required to give an oral presentation of their proposal to the review committee. This provides an opportunity for the respondent to clarify or elaborate on the proposal. These are fact-finding and explanation sessions only and do not include negotiation. CRCOG will schedule the time and location of these presentations. Oral presentations are an option of CRCOG and may or may not be conducted.

Subcontracting

The successful respondent may utilize the services of specialty subcontractors on those portions of the work that under normal contracting practices are performed by specialty subcontractors. The successful respondent shall not award any portion of the work to a subcontractor without **prior written approval** of CRCOG. The acceptance of any and all subcontractors shall reside with CRCOG, and CRCOG's decision shall be final. The successful respondent shall be fully responsible to CRCOG for the performance, finished products, acts, and omissions of his subcontractors and persons directly or indirectly employed thereby.

Assigning/Transferring of Agreement

Any successful respondent is prohibited from assigning, transferring, conveying, subletting or otherwise disposing of the resulting agreement or its rights, title, or interest therein or its power to execute such an agreement to any other person, company or corporation without prior consent and approval in writing from CRCOG.

Amending or Canceling Request

CRCOG reserves the right to amend or cancel this RFP, prior to the due date and time, if it is deemed to be in its best interest to do so. CRCOG reserves the right to decide not to consider any or all of the consultants submitting information in response to this request.

Waiver of Informalities

CRCOG reserves the right to accept or reject any and all responses to this Request for Proposals, or any part thereof, and to waive any informalities and/or technicalities that are deemed to be in its best interest.

Collusion

By submitting a proposal, the respondent implicitly states: that his/her proposal has not been made in connection with any other competing respondent submitting a separate response to this RFP; is in all respects fair; and has been submitted without collusion or fraud. It is further implied that the respondent did not participate in the RFP development process, had no knowledge of the specific contents of the RFP before its issuance, and that no employee of CRCOG either directly or indirectly assisted in the consultant's proposal preparation. Respondent consultants will be required to sign the certificate incorporated in this RFP (see Attachment B) relative to non-collusion.

Termination

CRCOG may terminate any contract(s) or any part of any contracts resulting from this process at any time for: cause, default or negligence on the part of the selected respondent; or if the selected respondent fails, in the opinion of CRCOG , to meet the general terms and conditions of any resulting contract or to provide a level of service that is deemed to be in the best interest of CRCOG .

Ethics

The conduct of any contracted consultant shall be subject to the CRCOG Ethics Policy (found online at: http://ww.crcog.org/rfprfq).

Affirmative Action

CRCOG**,** through its policies on Equal Employment Opportunity and Affirmative Action, pledges its support and cooperation to private and public agencies that are promoting public policy in this vital area of human relations. Respondent consultants will be required to sign the certificate incorporated in this RFP (see Attachment C) relative to Equal Employment Opportunity and Minority/Female Business Enterprise and return it with their response.

Insurance Requirements

The consultant (CONSULTANT) shall be required to furnish a Certificate of Insurance evidencing the following insurance coverage prior to the execution of an Agreement. Failure to maintain insurance coverage as required and to name CRCOG as the Additional Insured will be grounds for termination of the contract. In addition:

A. The insurance requirements shall apply to all subcontractors and/or consultants.

B. All policy forms shall be on the occurrence form. Exceptions must be authorized by CRCOG unless the coverage is for Professional Liability where the common form is claims made.

C. Acceptable evidence of coverage will be on the ACORD form or a form with the same format.

D. All renewal certificates shall be furnished at least 10 days prior to policy expiration.

E. Each certificate shall contain a 30-day notice of cancellation.

F. Insurance shall be issued by an insurance company licensed to conduct business in the State of Connecticut which has at least an "A-" policy holders rating according to Best Publications latest edition Key Rating Guide.

Required insurance coverage:

a. General Liability Insurance, including Contractual Liability Insurance and Products/Completed Operations Insurance issued by an insurance company licensed to conduct business in the State of Connecticut with: limits not less than $1,000,000 per occurrence with an aggregate of $2,000,000 All, if any, deductibles are the sole responsibility of the contractor to pay and/or indemnify.

b. Automobile Liability Insurance issued by an insurance company licensed to conduct business in the State of Connecticut with: limits not less than $1,000,000 for all damages because of bodily injury sustained by each person as a result of any occurrence and $1,000,000 aggregate per policy year; and limits of $500,000 for all damages because of property damage sustained as the result of any one occurrence or $1,000,000 Combined Single Limit (CSL). All, if any, deductibles are the sole responsibility of the contractor to pay and/or indemnify.

c. Worker's Compensation Insurance in accordance with Connecticut State Statutes.

d. Professional Liability Insurance with a minimum $1,000,000 per occurrence and a $1,000,000 aggregate.

e. Any of the aforementioned policies written on a claims form shall have an extended reporting period not less than two years from the end of the project.

Hold Harmless and Indemnification

In addition to its obligation to provide insurance as specified above, the CONSULTANT, its subcontractors, agents and assigns shall indemnify and hold harmless CRCOG, including but not limited to, its elected officials, and its officers, from any and all claims made against CRCOG, including but not limited to, damages, awards, costs and reasonable attorney's fees, to the extent any such claim directly and proximately results from the negligent acts, errors, or omissions in performance of services by the CONSULTANT during the CONSULTANT's performance of this Agreement or any other Agreements of the CONSULTANT entered into by reason thereof. CRCOG agrees to give the CONSULTANT prompt notice of any such claim and absent a conflict of interest, an opportunity to control the defense thereof.

Additional Terms and Conditions

1. The consultant assigns to CRCOG all rights, title and interests in and to all causes of action it may have under Section 4 of the Clayton Act, 15 USC 15, or under Chapter 624 of the general statutes. This assignment occurs when the consultant is awarded the contract.
2. The consultant agrees that it is in compliance with all applicable federal, state and local laws and regulations, including but not limited to Connecticut General Statutes Sections

4a-60 and 4a-60a. The consultant also agrees that it will hold CRCOG harmless and indemnify CRCOG from any action which may arise out of any act by the consultant concerning lack of compliance with these laws and regulations. All purchases will be in compliance with Section 22a-194 to Section 22a-194g of the Connecticut General Statutes related to product packaging.

3. The contract arising from the RFP is subject to the provisions of Executive Order No. Three of Governor Thomas J. Meskill promulgated February 15, 1973 and Section 16 of P.A. 91-58 Nondiscrimination Regarding Sexual Orientation, and the provisions of Executive Order No. Sixteen of Governor John G. Rowland promulgated August 4, 1999 regarding Violence in the Workplace Prevention Policy.
4. The contract arising from the RFP may be subject to the provisions of §1-218 of the Connecticut General Statutes, as it may be modified from time to time. In accordance with this section, each contract in excess of two million five hundred thousand dollars between a public agency and a person for the performance of a governmental function shall (1) provide that the public agency is entitled to receive a copy of records and files related to the performance of the governmental function, and (2) indicate that such records and files are subject to the Freedom of Information Act and may be disclosed by the public agency pursuant to the Freedom of Information Act. No request to inspect or copy such records or files shall be valid unless the request is made to the public agency in accordance with the Freedom of Information Act. Any complaint by a person who is denied the right to inspect or copy such records or files shall be brought to the Freedom of Information Commission in accordance with the provisions of sections 1-205 and 1-206 of the Connecticut General Statutes. Incorporated by reference into the resulting contract is Section 4-61dd (g) (1) and 4-61dd (3) and (f) of the Connecticut General Statutes which prohibits contractors from taking adverse action against employees who disclosed information to the Auditors of Public Accounts or the Attorney General.

ATTACHMENT A

RESPONSE PAGE

Capitol Region Council of Governments

REQUEST FOR PROPOSALS

DATE ADVERTISED: **August 16th, 2018**

DATE/TIME DUE: **September 10th, 2018 By 1:00 p.m.**

NAME OF PROPOSAL **RFP for Cybersecurity Model Policies and Consulting Services**

Type or Print Name of Individual	**Doing Business as (Trade Name)**
Signature of Individual	**Street Address**
Title	**City, State, Zip Code**
Date	**Telephone Number / Fax Number**
E-mail Address/Website	**SS # or TIN#**

ATTACHMENT B

CAPITOL REGION COUNCIL OF GOVERNMENTS (CRCOG)

NON-COLLUSION STATEMENT

The company responding to this Request for Proposals certifies that it is being submitted without any collusion, communication or agreement as to any matter relating to it with any other respondent or competitor. We understand that this response must be signed by an authorized agent of our company to constitute a valid response.

Date: _____

Name of Company: _____

Name and Title of Agent: _____

By (SIGNATURE): _____

Address: _____

_____

_____

Telephone Number: _____

ATTACHMENT C

CAPITOL REGION COUNCIL OF GOVERNMENTS (CRCOG)

EQUAL EMPLOYMENT OPPORTUNITY AND MINORITY/FEMALE BUSINESS ENTERPRISE CERTIFICATION FORM

The undersigned certifies that_____is an
(Name of Company)
Equal Opportunity Employer and is in compliance with federal and state rules and regulations pertaining to Equal Employment Opportunity and Affirmative Action.

_____
(Respondent's Signature)

IF APPLICABLE:
The undersigned also certifies that _____
(Name of Company)

is a Minority/Female Business Enterprise and is in compliance with federal and state rules and regulations pertaining to Minority/Female Business Enterprise designations.

_____
(Respondent's Signature)

_____ (Today's Date)

Attachment D.

Organizational Conflict of Interest Statement

Each entity that enters into a contract with the Capitol Region Council of Governments (CRCOG) is required, prior to entering into such contract, to inform CRCOG of any real or apparent Organizational Conflict of Interest (OCI).

An OCI exists when any of the following circumstances arise:

1. Lack of Impartiality or Impaired Objectivity. When the CONSULTANT *(proposer, bidder, etc)* is unable, or potentially unable, to provide impartial and objective assistance or advice to CRCOG due to other activities, relationships, contracts, or circumstances.
2. Unequal Access to Information. The CONSULTANT has an unfair competitive advantage through obtaining access to nonpublic information during the performance of an earlier contract.
3. Biased Ground Rules. During the conduct of an earlier procurement, the CONSULTANT has established the ground rules for a future procurement by developing specifications, evaluation factors, or similar documents.

Organizational Conflicts of Interest Prohibition and Non-Conflict Certification

The CONSULTANT warrants that, to the best of his/her/its knowledge and belief, and except as otherwise disclosed, there are no relevant facts or circumstances, which could give rise to organizational conflicts of interest. The proposer agrees that, if after award, an organizational conflict of interest is discovered, an immediate and full disclosure in writing must be made to CRCOG, which must include a description of the action, which the CONSULTANT has taken or proposes to take to avoid or mitigate such conflicts. If an organizational conflict of interest is determined to exist, CRCOG may, at its discretion, cancel the contract award. In the event the CONSULTANT was aware of an organizational conflict of interest prior to the award of the contract and did not disclose the conflict to CRCOG, CRCOG may terminate the contract for default. The provisions of this clause must be included in all subcontracts for work to be performed similar to the service provided by the prime consultant, and the terms "contract" and "CONSULTANT" modified appropriately to preserve CRCOG rights.

Organizational Conflict of Interest - Proposer's Signature and Certification

The undersigned on behalf of the CONSULTANT hereby certifies that the information contained in this certification is accurate, complete, and current.

Signature and date

Title of Request for Qualifications

Typed or Printed Name

Title

Company Name and Address