TOWN OF GLASTONBURY
PROFESSIONAL SERVICES PROCUREMENT NOTICE
REQUEST FOR QUALIFICATIONS FOR
INFORMATION SYSTEMS SECURITY RISK ASSESSMENT AUDIT
RPGL-2019-34

The Town of Glastonbury will be accepting proposals from qualified firms and individuals who can provide an Information Systems (IT) security risk assessment audit for the Town. Interested firms and individuals should request the proposal instructions and details from the Purchasing Agent, 2155 Main Street, Glastonbury, CT 06033 or via the Town's website at www.glastonbury-ct.gov.

Proposals must be submitted to the Purchasing Agent no later than **April 23, 2019 at 11:00 AM**. **LATE PROPOSALS WILL NOT BE CONSIDERED.**

The Town reserves the right to waive informalities or reject any part of, or the entire proposal, when said action is deemed to be in the best interests of the Town.

An Affirmative Action/Equal Opportunity Employer. Minority/Women/Disadvantaged Business Enterprises are encouraged to bid.

Mary F. Visone
Purchasing Agent

TABLE OF CONTENTS **PAGE NO.**

Attachments

I. GENERAL INFORMATION

A. OVERVIEW

The Town of Glastonbury (Town) is soliciting a Request for Qualifications (RFQ) from qualified individuals and firms who can provide an Information Systems (IT) security risk assessment audit for the Town. The purpose of this RFQ is to request an independent assessment of the Town's IT operations, internal controls and its policies and procedures, including a review of systems. During the course of the engagement it is expected that the Consultant will:

- Audit critical systems security model and workflows to identify vulnerabilities and threats.

- Conduct a physical security assessment of the premises of the Town and any potential Application Service Providers (ASP). Recommend the corrective and preventative solutions, should they be required, for the Town to implement in an effort to improve the informational environment.

- Recommend appropriate security policies and procedures.

- Enter into a contract to provide periodic on-site risk management and review of Information Systems security procedures, analysis of system output data to identify potential breaches, suggest best practice, and apprise the Town Manager and Director of Finance of known threats.

The awarded Consultant shall allow other Town of Glastonbury entities (e.g. Glastonbury Board of Education and Glastonbury Housing Authority) to "piggy-back" this RFQ. While this clause in no way commits any other municipal entity to contract with the awarded Consultant, nor does it guarantee any additional orders will result, it does allow them, at their discretion, to make use of the Town of Glastonbury's competitive solicitation process (provided said process satisfies their own procurement guidelines) and contract directly from the awarded Consultant. Any contract made by other municipal entities shall be understood to be transactions between that municipal entity and the awarded Consultant. The Town of Glastonbury shall have no legal obligation or responsibility for any contracts between the awarded Consultant and any other municipal entity.

B. BACKGROUND

The Town of Glastonbury serves an area of 52.5 +/- square miles with an estimated population of 34,584. The Town's fiscal year begins on July 1 and ends on June 30. The Town of Glastonbury provides the following services to its citizens:

General Government
Public Safety
Human Services
Community Development
Physical Services
Leisure/Culture
Administrative
Sanitation
Education

The Town of Glastonbury is organized into several departments and divisions which use many internal and external systems for the processing of data and information. The Town's external auditor performs an annual IT audit as part of its overall audit of the Town. The selected Respondent will provide the following IT consulting /audit services:

- **IT General Controls**
  Make recommendations on policies and procedures for IT general controls that may be needed in order to become more closely aligned with common standards and leading industry practices. It is the goal of the Town to develop controls that focus on logical and physical security, IT operations, and software development and change management.

- **IT Security Risk Assessment Audit**
  Review and advise the Town Manager and Director of Finance on security controls for systems, policies and processes.

C. MINIMUM REQUIREMENTS

To be considered, interested firms and individuals must satisfy the following requirements:

- Experience and competency in providing IT security risk assessment audits with security technologies, including planning, architecture, policies and procedures within the last five (5) years, municipal or government experience preferred.

- Project Manager should possess one or more of the following certifications: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Systems Manager (CISM), or Certified Computer Examiner.

- Proof of Certified in Risk and Information Systems Control (CRISC) certification.

E. TERM OF SERVICE

The Consultant will be expected to commence services on or before May 15, 2019 subject to contract execution. It is anticipated the initial assessment audit will be completed no later than 45 days after contract execution. Subsequent periodic assessments shall be completed as mutually agreed upon by the Town and the Consultant; and the Consultant shall only proceed with subsequent assessments if authorized by the Town. There is no guarantee of future work and the Town reserves the right to solicit and contract separately for future assessments as deemed in the Town's best interest. The term of the appointment is for two (2) years with the option to extend for an additional one (1) year term or beyond at the discretion of the Town of Glastonbury upon mutual agreement with the selected firm.

II. SCOPE OF SERVICES

A. SPECIFIC SERVICES

- Perform a confidential assessment of security controls for systems, policies and processes. The assessment is to be conducted to systematically identify programmatic weaknesses and where necessary, establish targets for continuing improvement of Town's operations, internal controls and its current policies and procedures pertaining to its current IT environment.

- A comprehensive and best practice Security Audit to include, but not limited to, the areas of concern below. Any additional materials and documentation can be referenced and attached with your submission.

  The project's scope includes:

  1. **Third Party On-Site Security Audit**: Assist Town in performing a 3rd party security audit to confirm that security and data protection controls are in place and compliant to Town's business needs and in alignment with industry standards such as NIST 800-53 or other applicable industry acceptable standards.

  2. **Review existing IT Security Policies/Practices and Procedures**: The Selected Consultant will review current state of Information security policies and standards and benchmark against Town's business needs and commonly accepted industry standards such as International Standards Organization (ISO), National Institute of Standards and Technology (NIST), Open Web Application Security Project (OWASP), Payment Card Industry (PCI) and System Administration, Networking, and Security Institute (SANS) to enhance the current policy set where there are gaps to the common standards, build new policies to match where existing controls are in place within the Town, and to make recommendations for additional policies that may be needed in order to become more closely aligned with the common standards and leading industry practices.

     Deliverables -

     - Review currently implemented information security policies and standards

     - Benchmark current policies and standards against ISO, NIST, OWASP, PCI and SANS standards

     - Review the discovered gaps and observations with Town management

     - Develop and finalize revised information security policies and standards

  3. **Vulnerability Assessment**: Perform in-depth IT security vulnerability assessment and penetration testing of Town's logical and physical IT infrastructures:

- Internal Network - All internal corporate systems to include workstations, servers, switching/routing infrastructure, virtualization and storage infrastructure, and other connected IT devices. Including all Demilitarized (DMZ) systems to include flow controls from external to internal systems.

- External Network - All external public facing systems to include firewalls, load balancers, web servers, file transfer protocol (FTP) servers, and web service interface points.

- Wireless Network – All wireless systems to include internal touch points from all Service Set Identifier (SSID), broadcast or hidden, as well as encryption levels.

- Physical access controls testing - Determine if the current physical security is effective by conducting physical access assessments;

- Remote Access/External Partners – Assess remote access and security of network connections and data traffic to and from external partners.

- Social Engineering - perform social engineering procedures to verify the existence and effectiveness of procedural controls to prevent unauthorized physical and electronic access to Town's IT systems. These procedures should be performed without the knowledge of Systems staff at a time to be coordinated with Town's Town Manager and Director of Finance.

- Internet usage – Asses URL/web filtering and access restrictions.

- Host based security – Assess security of critical systems at operating system and database layers and associated identity and access management controls.

Key Deliverables – The Consultant will be required to present to the Town Manager and Director of Finance a confidential detailed report on testing and attack scenarios used, vulnerabilities discovered, including the risk rating. The final report provided will remain confidential.

- Executive Summary with overall severity findings and risk exposure.

- Detailed technical results for vulnerabilities discovered, exploited vulnerabilities and proof of concepts/screenshots.

- Detailed explanations of the implications of findings, business impacts, and risks for each of the identified exposures.

- Remediation recommendations to close the deficiencies identified.

- Detailed steps (wherever/whenever applicable) to be followed while mitigating the reported deficiencies.

4. **Penetration Testing**: Perform non-volatile exploit procedures designed to determine how well Town's security systems can withstand up-to-date malicious exploits launched via dial-in, internet, and internal network connections.

    - Testing will attempt to compromise networks and operating system to identify vulnerabilities to the system.

    - Assess the provided network(s) to identify potential vulnerabilities.

    - Exploit vulnerabilities and provide evidence of unauthorized access to approved subnets and systems.

    - Penetration testing should be performed from two perspectives:

        - An outside threat with no approved system access.
        - A malicious insider who has access to the system.

    - Evidence gathered as proof of access must not harm the confidentiality, integrity, or availability of the systems, application, and or data.

    - Special attention should be given to areas that contain high risk data.

    These procedures should be performed without the knowledge of Town staff at a time to be coordinated with the Town Manager and Director of Finance.

    If required and at the request of Town, an additional scan shall be performed to assess whether vulnerabilities identified during initial scanning have been remediated satisfactorily.

5. **Security Strategy and Systems**: Evaluate Town's security strategy and systems, including firewall hardware, software, placement and utilization. Perform an in-depth security scan and threat assessment to identify vulnerabilities. This should include, but not be limited to, port scans, host enumeration, and application/system identification.

6. **Connections to External Partners**: Review our connection and security posture to our external partners through wide area networks, dedicated circuits, ASP's, remote clients, and remote server technologies; Assess remote access and security of network connections and data traffic to and from external partners.

7. **Inbound and Outbound Remote Access Strategy**: Evaluate administration of remote access, both inbound and outbound. Review implications associated with the level of access that has been granted to authorized users including dial-up, Internet, Virtual Private Network (VPN), Citrix for ASP connection and staff

access as well as Town user access protocol and procedures. Examine security issues in remote data transfer and the extent of network access available remotely. Perform a threat assessment to identify vulnerabilities with existing remote access.

8. **Internet Usage**: Evaluate how the Town secures sensitive data and applications: how the Town blocks unnecessary and unauthorized websites: and the tools the Town uses for monitoring the URLs, links and Web pages that were visited. Identify any immediate problems. Asses URL/web filtering and access restrictions. Provide input on an action plan to handle potential on going or long-term problems.

9. **Virus Protection**: Evaluate the facility used to prevent impact from viruses. Perform a threat assessment to identify vulnerabilities.

10. **Logon Security**: Evaluate password and CRYPTO Card policies. Review current logon auditing practices. Examine current practices with regard to machine restrictions. Identify any potential weaknesses. Provide input on an action plan to deal with problems. Perform a threat assessment to identify vulnerabilities.

11. **Fraud and General Controls Objectives**: Assess the risk that a single trusted user, administrator or vendor of Town’s information systems can accomplish and/or conceal the improper diversion of assets using vulnerabilities found in Town’s information systems. Special attention should be given to:

    - segregation of duties,
    - documented and applied policies and procedures,
    - acquisition, development and change control practices,
    - database administration practices,
    - production control practices,
    - access and transaction authorizations,
    - monitoring practices, and
    - disaster recovery and incident response.

12. **Employee (user / administrator) Systems Control Vulnerabilities**: Assess the risk that a single trusted user, administrator or vendor of Town’s Information Systems can accomplish and/or conceal the improper diversion of assets using vulnerabilities found in Town’s user/administrator service systems.

13. **Employer reporting Service Systems Control Vulnerabilities**: Assess the risk that a single trusted user, administrator or vendor of Town's Information Systems can accomplish and/or conceal the improper diversion of assets using vulnerabilities found in Town's employer reporting service systems.

14. **Accounting and Administrative Systems Control Vulnerabilities**: Assess the risk that a single trusted user, administrator or vendor of Town's Information Systems can accomplish and/or conceal the improper diversion of assets using vulnerabilities found in Town's accounting and administrative systems.

15. **Develop a Vulnerability Assessment Plan**: The Consultant will conduct a comprehensive Information Systems security risk assessment using an objective and independent framework developed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) including Town's people, organizational structure, processes and supporting technology.

    The overall objectives of this phase will be to assist the Town in gaining an understanding of the existing maturity of the Information Systems security program in comparison to industry standards, develop sustainable controls, and provide observations and recommendations for overall program improvement.

    Key Tasks – Assess Town's ability to protect its information assets and its preparedness against cyber-attack on the following items:

    - Leadership and governance: Management and IT staff, their due diligence, ownership, and effective management of risk within the context of the organization's goals, objectives and the external threat/risk landscape.

    - Human factors: The level of security-focused culture that empowers and ensures the right people, skills, culture and knowledge.

    - Information risk management: Organization's approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners.

    - Operations and technology: The level of control measures implemented within organization to address identified risks, and minimize the impact of compromise.

    - Business continuity: Organizations preparations for a security incident and its ability to prevent or minimize the impact through successful crisis and stakeholder management.

    - Legal and compliance: Legal and regulatory compliance requirements relevant to the organization.

    Deliverables:

- Maturity and risk rating based on National Institute of Standards Cybersecurity Framework Guide (NIST CSF), including but not limited to:
    - Highlight successes and identify gaps based on CSF target maturity of “Implemented” or level 3.
    - Security maturity comparison against similar organizations (public sector) and similarly sized organizations
    - Rank criticality of gaps

- Identify security/privacy risks in current practices inclusive of:

    - Organizational/Personnel (Skill/Knowledge Level)
    - Policy/Process/Procedures
    - Tools, Methods, Implementation and Operations specific issues
    - Access, implementation of NIST, industry/leading practices
    - Dependencies between Town and other state agencies as well as IT infrastructure service providers

- Develop detailed recommendations to close gaps which includes:

    - Recommend mitigation solutions
    - Estimated Town budget requirements range for mitigation deployment and ongoing support
    - Town staffing requirements range for both deployment and ongoing support
    - Estimated deployment timelines

The Consultant shall propose a recommended periodic ongoing risk management and vulnerability review in which the Consultant will be on-site at the Town offices managing the vulnerability assessment program developed by them and approved by Town. The Consultant will communicate emerging threats and trends to the Town and be available for consultation on an “as-needed” basis throughout the contracted term of the engagement.

16. **Prepare a confidential final report**: Develop a report with the Consultant's assessment of the Town’s and its subcontractor’s IT risk management policies, practices, and procedures and present the findings to Town Manager and Director of Finance with a prioritized list of recommended or required improvements. The final report should contain an executive summary and presentation suitable for non-technical management. The report shall not be a public document.

17. **Provide a comprehensive Security Training to all Staff**: Upon completion of the assessment, the Consultant should provide a comprehensive training/presentation to all Town staff outlining best practices for security awareness. Online testing of employee comprehension of security awareness would be required for the Consultant to provide.

B. INSURANCE

The Respondent shall, at its own expense and cost, obtain and keep in force during the entire duration of the contract the following insurance coverage covering the Respondent and all of its agents, employees and sub-contractors and other providers of services and shall name the Town of Glastonbury and its employees and agents as an Additional Insured on a primary and non-contributory basis to policies except Workers Compensation and Professional Liability. All policies should also include a Waiver of Subrogation in favor of the Town. **These requirements shall be clearly stated in the remarks section on the Respondent's Certificate of Insurance.** Insurance shall be written with insurance carriers approved in the State of Connecticut and with a minimum Best's Rating of A-VIII. In addition, all carriers are subject to approval by the Town. Minimum Limits and requirements are stated below:

1) Worker's Compensation Insurance:

- Statutory Coverage
- Employer's Liability
- $1,000,000 each accident/$1,000,000 disease-policy limit/$1,000,000 disease each employee
- A Waiver of Subrogation shall be provided in favor of the Town and its employees and agents.

2) Commercial General Liability:

- Including Premises & Operations, Products and Completed Operations, Personal and Advertising Injury, Contractual Liability and Independent Contractors.
- Limits of Liability for Bodily Injury and Building Damage
  Each Occurrence $1,000,000
  Aggregate $2,000,000 (The Aggregate Limit shall apply separately to each job.)
- A Waiver of Subrogation shall be provided in favor of the Town and its employees and agents.

3) Automobile Insurance:

- Including all owned, hired, borrowed and non-owned vehicles
- Evidence a Combined Single Limit of Liability for Bodily Injury and Property Damage: Per Accident $1,000,000
- A Waiver of Subrogation shall be provided in favor of the Town and its employees and agents.

4) Data Breach Liability:

- $1,000,000 Occurrence/$1,000,000 Aggregate

5) Errors and Omissions Liability or Professional Services Liability Policy

- Provide Errors and Omissions Liability or Professional Services Liability Policy for a minimum Limit of Liability $1,000,000 each occurrence or per claim. The awarded respondent(s) will be responsible to provide written notice to the Owner 60 days prior to cancellation of any insurance policy.

- The respondent agrees to maintain continuous professional liability coverage for the entire duration of this Project, and shall provide for an Extended Reporting Period in which to report claims for seven (7) years following the conclusion of the Project.

The respondent shall provide a Certificate of Insurance as "evidence" of General Liability, Auto Liability including all owned, hired, borrowed and non-owned vehicles, statutory Worker's Compensation and Employer's Liability and Professional Services Liability coverage.

The respondent shall direct its Insurer to provide a Certificate of Insurance to the Town before any work is performed. The awarded Respondent(s) will be responsible to provide written notice to the Town 30 days prior to cancellation or non-renewal of any insurance policy. The Certificate shall evidence all required coverages including the Additional Insured on the General Liability and Auto Liability policies and Waiver of Subrogation applies on all policies. The respondent shall provide the Town copies of any such insurance policies upon request.

Note: The above insurance requirements are the Town’s general requirements. Insurance requirements with the awarded respondent are subject to final negotiations.

C. INDEMNIFICATION

To the fullest extent permitted by law, the Respondent shall indemnify and hold harmless the Town and its consultants, agents, and employees from and against all claims, damages, losses and expenses, direct, indirect or consequential (including but not limited to fees and charges of engineers, attorneys and other professionals and court and arbitration costs) to the extent arising out of or resulting from the performance of the Respondent’s work, provided that such claim, damage, loss or expense is caused in whole or in part by any negligent act or omission by the Respondent, or breach of its obligations herein or by any person or organization directly or indirectly employed or engaged by the Respondent to perform or furnish either of the services, or anyone for whose acts the Respondent may be liable.

The above insurance requirements are the Town’s general requirements. Insurance requirements with the awarded respondent are subject to final negotiations.

III. SUBMISSION OF PROPOSAL

A. PROPOSAL INSTRUCTIONS

By submitting a proposal, you represent that you have thoroughly examined and become familiar with the scope of services outlined in this RFQ and you are capable of performing the work to achieve the Town's objectives.

All Respondents are required to submit a **clearly marked** original and seven (7) copies of their proposal to Mary F. Visone, Purchasing Agent, Office of the Purchasing Agent, 2155 Main Street, Glastonbury, CT. All proposals will be opened publicly and recorded as received. Proposers may be present at the opening; however, there will be no public reading of Proposals. Proposals received later than the time and date specified will not be considered. The proposal must be submitted in a sealed envelope or package and the outside shall be clearly marked with the Respondent's Company Name, Address and the following:

SEALED REQUEST FOR QUALIFICATIONS
PROFESSIONAL SERVICES PROCUREMENT NOTICE
INFORMATION SYSTEMS SECURITY RISK
ASSESSMENT AUDIT
RPGL-2019-34
DATE – April 23, 2019
TIME - 11:00 A.M.

All respondents are required to submit the information detailed below. **Responses shall be organized and presented in the order listed below to assist the Town in reviewing and rating proposals (any boiler plate information that Respondents wish to share shall be inserted at the end of the proposal submission).** Responses should be presented in appropriate detail to thoroughly respond to the requirements and expected services described herein and presented and clearly marked in the order within this written proposal.

a. Table of Contents to include clear identification of the material provided by section and number.

b. A letter of transmittal indicating the Respondent's interest in providing the service and any other information that would assist the Town in making a selection. This letter must be signed by a person legally authorized to bind the Consultant to a contract. This letter also must affirm that the firm or their representative has made themselves knowledgeable of those matters and conditions in the Town which would influence this Proposal.

c. Name and telephone number of person(s) to be contacted for further information or clarification.

d. A background and qualifications statement, including description and history of your firm and the servicing office. The Respondent shall provide proof of Certified in Risk and Information Systems Control (CRISC) certification. The Respondent shall indicate, if any, experience in providing these services to municipalities or government agencies.

e. Include a list of not less than three current client references from whom services similar to those outlined herein have been provided or are currently being provided. This list shall include the following information:

1. Name of the organization
2. Approximate gross cost of contract, (initial assessment and ongoing annual cost if any)
3. Dates services encompass
4. Services being provided
5. Name, address, and telephone number of the responsible official of the organization

The Town reserves the right to contact these organizations regarding the services performed by the Respondent.

f. List of personnel to be assigned to this project, including years of experience in their current position, municipalities served (if applicable) and their roles in providing services. Please provide their resumes, and document the chain of command for these individuals. The Project Manager assigned to this project should possess one or more of the following certifications: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Systems Manager (CISM), or Certified Computer Examiner, and ideally have demonstrable work history with technology audits and assessments.

g. Detail the specific data your firm would require from the Town to begin servicing this account.

h. Understanding of the Scope of Work. Include information that explains your firm's ability to perform, implement and administer these services, emphasizing familiarity and experience with other similar IT security risk assessment audits. Including demonstrated recent successful performance on other accounts for the following:

- Identification of programmatic weaknesses,
- Establishment of targets for continuing improvement of operations,
- Internal controls and,
- Development of new policies and procedures pertaining to IT environment.

i. The Respondent's privacy policy including demonstration of the Respondent's best practices for ensuring data security, periodic security and HIPAA training of the Respondent's staff, a disaster recovery plan and the use of encryption technology.

j. Describe the approach that will be used to perform the initial risk assessment audit and any ongoing periodic assessments if directed by the Town. Describe the anticipated role that the Town will play in this process.

k. Respondent shall provide a draft project work plan with suggested timeline for completion of the initial risk assessment audit. Specific project work plan and completion dates to be determined with Town upon contract execution with selected Respondent.

l. Respondent shall provide a general description of cost range and what services are covered within the range of fees. The resulting contract will be structured as a fixed price contract for IT security assessment audit and consulting services and not time and materials based. Additional pricing and fees that could be expected should also be referenced for services beyond the initial audit. Actual fee proposal is not required to be submitted with the proposal response.

m. A concluding statement as to why the respondent is best qualified to meet the needs of the Town.

n. Description of any exceptions taken to this RFQ. If any proposal involves any exception from the stated requirements and specifications, they must be clearly noted as exceptions and attached to the proposal.

o. Proposal Response Page (ATTACHMENT A)

p. Respondent is required to review the Town of Glastonbury Code of Ethics adopted July 8, 2003 and effective August 1, 2003 and revised October 29, 2013 and effective November 8, 2013. Respondent shall acknowledge that they have reviewed the document in the area provided on the attached Ethics Acknowledgement form included on **ATTACHMENT A**. The selected respondent will also be required to complete and sign an Acknowledgement Form prior to award. The Code of Ethics and the Acknowledgment Form can be accessed at the Town of Glastonbury website at www.glastonbury-ct.gov. Upon entering the website click on the **Bids & Proposals Icon** which will bring you to the links for the **Code of Ethics** and the **Acknowledgement Form**.

q. The Town of Glastonbury is dedicated to waste reduction and the practice of using and promoting the use of recycled and environmentally preferable products. Respondents are encouraged to submit RFQ responses that are printed double-sided (except for the signed proposal page) on recycled paper, and to use paper dividers to organize the RFQ for review. All proposal pages should be secured with a binder clip, staple or elastic band, and shall not be submitted in plastic binders or covers, nor shall the proposal contain any plastic inserts or pages. We appreciate your efforts towards a greener environment.

B. TOWN CONTACTS

1. All technical inquiries relative to this RFQ must be directed in writing to Julie Twilley, Director of Finance at julie.twilley@glastonbury-ct.gov. For administrative questions concerning this proposal, please contact Mary F. Visone, Purchasing Agent, at (860) 652-7588, or by email at purchasing@glastonbury-ct.gov. All questions, answers, and/or addenda, as applicable, will be posted on the Town's website at www.glastonbury-ct.gov. (Upon entering the website click on Bids & Proposals icon, click on the Bid Title to view all proposal details and document links). It is the respondent's responsibility to check the website for addenda prior to submission of any proposal. Note: Responses to requests for more specific contract information than is contained in the RFQ shall be limited to information that is available to all respondents and that is necessary to complete this process. The request must be received at least five (5) business days prior to the response deadline.

2. No other Glastonbury Town employee, elected official, or evaluation committee member should be contacted concerning this RFQ during the proposal process. Failure to comply with this requirement may result in disqualification.

C. EVALUATION CRITERIA

- The following factors will be considered by the Town when evaluating the proposals:
  - Accuracy, overall quality, thoroughness and responsiveness to the Town's requirements as summarized herein.
  - Respondent's approach that will be used to perform the initial risk assessment audit and any ongoing periodic assessments if directed by the Town. Understanding of the Town's needs and objectives.
  - The qualifications and experience of the Respondent and the designated account executive and other key personnel to be assigned to the account. Project Manager shall possess one or more of the following certifications:
    - Certified Information Systems Security Professional (CISSP),
    - Certified Information Systems Auditor (CISA),
    - Certified Information Systems Manager (CISM), or
    - Certified Computer Examiner.
    - Certified in Risk and Information Systems Control (CRISC) certification.
  - Experience and competency in providing IT security risk assessment audits with security technologies, including planning, architecture, policies and procedures within the last five (5) years, municipal or government experience preferred.

- Familiarity and experience with IT security risk assessment audits, including demonstrated recent successful performance on other accounts for the following:

    - Identification of programmatic weaknesses,
    - Establishment of targets for continuing improvement of operations,
    - Internal controls and,
    - Development of new policies and procedures pertaining to IT environment.

- Provision of adequate privacy policy including demonstration of the Respondent’s best practices for ensuring data security, including periodic security, and HIPAA training of the Respondent’s staff, a disaster recovery plan and the use of encryption technology.

- Draft project work plan with suggested timeline for completion of the initial risk assessment audit.

D. <u>SELECTION PROCESS</u>

- This request for qualifications does not commit the Town of Glastonbury to award a contract or to pay any costs incurred in the preparation of a proposal to this request. All proposals submitted in response to this request for qualifications become the property of the Town of Glastonbury. The Town of Glastonbury reserves the right to accept or reject any or all proposals received as a result of this request, to negotiate with the selected respondents, the right to extend the contract for an additional period, or to cancel in part or in its entirety the request for qualifications, and to waive any informality if it is in the best interests of the Town to do so.

- A Selection Committee, appointed by the Town Manager, will evaluate all proposals received for completeness and the respondent’s ability to meet all requirements as outlined in this proposal. The Committee will then short list the specific Respondents whose proposals best meet all criteria required and may conduct interviews with these Respondents. Upon completion of interviews, the Selection Committee will forward to the Town Manager a list of Respondents recommended for further consideration.

- Top rated Respondents will be asked to submit a specific Scope of Services and associated fee   proposal along with any exceptions taken to the Town’s form of agreement. The Town Manager shall review said proposals and negotiate an agreement based on those discussions.

- Additional technical information may be requested from any respondent for clarification purposes, but in no way changes the original proposal submitted.

D. TIMELINE

The following schedule is anticipated. The Town intends to adhere to this schedule as closely as possible but reserves the right to modify the schedule in the best interest of the Town as required.

Publicize RFP	April 4, 2019
RFP Due Date	April 23, 2019 at 11 AM
Shortlist of Proposals Received	April 26, 2019
Interviews with Top Respondents	April 30, 2019
Fee Proposal and Scope of Services	TBD
Contract Effective Date	TBD

ATTACHMENT A

PROPOSAL RESPONSE PAGE

BID / PROPOSAL NO:	**RPGL-2019-34**	**DATE DUE:**	**04-23-19**
DATE ADVERTISED:	**04-04-19**	**TIME DUE:**	**11:00 AM**
NAME OF PROJECT:	**INFORMATION SYSTEMS SECURITY RISK ASSESSMENT AUDIT**		

The Respondent acknowledges receipt of the following Addenda:

Addendum #1 ___________(Initial/Date) **Addendum #2** ___________ (Initial/Date) **Addendum #3** ____________(Initial/Date)

It is the responsibility of the respondent to check the Town's website for any Addenda before submitting the proposal.

NON-COLLUSION STATEMENT:

By submission of this proposal, the Respondent 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 proposal must be signed by an authorized agent of our company to constitute a valid proposal.

CODE OF ETHICS:

I / We have reviewed a copy of the Town of Glastonbury's Code of Ethics and agree to submit a Consultant Acknowledgement Form if I /We are selected. Yes ____ No ____ *

***Respondent is advised that effective August 1, 2003, the Town of Glastonbury cannot consider any proposal where the respondent has not agreed to the above statement.**

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	**SS # or TIN#**

(Seal – If proposal is by a Corporation)
Attest