TOWN OF
NORTH KINGSTOWN, RHODE ISLAND

100 Fairway Drive
North Kingstown, RI 02852-6202
Phone: (401) 294-3331
Fax: (401) 583-4140
www.northkingstown.org

REQUEST FOR PROPOSALS

INFORMATION SYSTEMS SECURITY
RISK ASSESSMENT AUDIT

*Sealed proposals for the above will be accepted in the Office of the Purchasing Agent, Town Municipal Offices, 100 Fairway Drive, North Kingstown, RI 02852, until 10:00am on Tuesday, December 3, 2019, and will then be publicly opened read aloud.

NO BIDS WILL BE ACCEPTED AFTER THE TUESDAY, DECEMBER 3, 2019 10:00AM DEADLINE.

IT IS THE RESPONSIBILITY OF THE PROSPECTIVE BIDDERS TO MONITOR THE TOWN'S WEBSITE FOR ANY SUBSEQUENT BID ADDENDUM. NO ADDENDA WILL BE ISSUED OR POSTED WITHIN FORTY-EIGHT (48) HOURS OF THE BID SUBMISSION DEADLINE.

The bid will be evaluated as to R.I.G.L. 45-55-5. (2) "Competitive Sealed Bidding" and the award shall be made on the basis of the lowest evaluated or responsive bid price.

Specifications may be obtained at the Purchasing Agent's Office at address listed above.

A certificate of Insurance showing $1 million General Liability and $1 million Any Auto, with the Town being named as an additional insured, Worker's Compensation, with a waiver of subrogation will be required of the successful bidder.

The Town of North Kingstown reserves the right to reject any or all proposals or parts thereof; to waive any formality in same, or accept any proposal deemed to be in the best interest of the Town.

The Town of North Kingstown will provide interpreters for the hearing impaired at any pre-bid or bid opening, provided a request is received three (3) days prior to said meeting by calling 294-3331, ext. 142.

Purchasing Agent

***PLEASE SUBMIT ONE (1) ORIGINAL AND ONE (1) COPY ALONG WITH FLASHDRIVE**

SELECTION CRITERIA

The bid will be evaluated as to R.I.G.L. 45-55-5.(2) "Competitive Sealed Bidding", and the award shall be made on the basis of the lowest evaluated or responsive bid price.
The proposal will be evaluated as to R.I.G.L. 37-2-64; 37-2-66; 37-2-67 and 37-2-68 , and the award shall be made on the basis of the highest qualified firm

The following factors will be considered in determining the lowest evaluated or responsive bid price:

Competence to perform the services as reflected by technical training and education; general experience; experience in providing the required services; and the qualifications and competence of persons who would be assigned to perform the services;

Ability to perform the services as reflected by workload and the availability of adequate personnel, equipment, and facilities to perform the service expeditiously;

Past performance as reflected by the evaluation of private persons and officials of other governmental entities that have retained the services of the firm with respect to such factors as control of costs, quality of work, and an ability to meet deadlines;

Ability to meet the proposal requirements and to demonstrate an understanding of the scope of the projects;

Experience of the Firm in similar projects;

Services offered;

Quality of the work previously performed by the Firm for the Town of North Kingstown, if any;

All documentation that must be included with the proposal to allow for the evaluation of the highest qualified firms is as follows:

- Performance Data Form, enclosed;
- Qualification Statement, enclosed;
- Proof of Errors and Omissions Insurance coverage as outlined in "Information to Vendors," enclosed;
- Personnel assigned to the project; resumes; qualifications; licenses and professional registration; and
- Description of services to be provided.

TOWN OF NORTH KINGSTOWN, RHODE ISLAND
INFORMATION FOR BIDDERS

ARTICLE 1. RECEIPT AND OPENING OF BIDS

Sealed bids must be submitted in SEALED ENVELOPES, addressed to the **Purchasing Agent, Town Hall, 100 Fairway Drive, North Kingstown, Rhode Island 02852,** and clearly marked with the name of the item bid, and the date and time of opening. Bids will be received by the Purchasing Agent up to the specified time as noted on the Invitation to Bid, and publicly opened and read aloud at the specified time.

Proposals submitted for a specified item must not be combined under the same cover with any other bid item.

It is the bidder's responsibility to see that their bid is delivered within the time and at the place prescribed. Proposals received prior to the time of opening will be securely kept unopened. No responsibility will attach to any officer or person for the premature opening of a proposal not properly addressed and identified.

Any bid received after the time and date specified shall not be considered, by messenger or by mail, even if it is determined by the Town that such non-arrival before the time set for opening was due solely to delay in the mails for which the bidder is not responsible. Conditional or qualified bids will not be accepted.

ARTICLE 2. PREPARATION OF BID

Each bid must be submitted on the prescribed form. All blank spaces for bid prices must be filled in, in ink or typewritten, both in words and figures. Erasures or other changes must be explained or noted over the signature of the bidder.

Each bid must be submitted in sealed envelopes, clearly labeled, so as to guard against opening prior to the time set therefore.

The Town may consider any bid not prepared and submitted in accordance with the provisions hereof and reserves the right to reject any or all proposals in whole or in part, toward any item, group of items, or total bid; to waive any technical defect or formality in same, or to accept any proposal deemed to be in the best interest of the Town.

ARTICLE 3. TELEGRAPHIC MODIFICATION

Telephonic, telegraphic or oral bids, amendments or withdrawals will not be accepted.

ARTICLE 4. WITHDRAWAL OF BIDS

Bids may be withdrawn personally or by written request at any time prior to the time specified for the opening. Bids may be modified in the same manner. Negligence on the part of the bidder in preparing the bid confers no right of withdrawal or modifications of their bid after such bid has been opened.

ARTICLE 5. QUALIFICATIONS OF THE BIDDER

The Town reserves the right to request each bidder to present evidence that they are normally engaged in purveying the type of product or equipment bid on. No bid shall be considered from bidders who are unable to show that they are normally engaged in purveying the type of product or equipment specified in the bid proposal.

To receive full consideration, the bidder must submit literature and necessary details, when applicable, on the material or service he proposes to furnish in order that the Town may have full information available when analyzing the proposals.

ARTICLE 6. OBLIGATIONS OF THE BIDDER

At the time of opening of bids, each bidder will be presumed to have inspected the Specifications and Contract Documents (including all addenda) which has been sent to the address given by such bidder. The failure or omission of any bidder to receive or examine any form, instrument, or document shall in no way relieve any bidder from any obligation in respect to their bid.

Any exceptions or deviations from the provisions contained in this Specification must be explained in detail and attached to proposal. If such deviations do not depart from the intent of this notice and are in the best interest of the Town, the proposal will receive careful consideration.

ARTICLE 7. "OR EQUAL" BIDDING

The Town intends to permit liberal scope in bidding and specifically does not intend to limit bidding to any one make or model. Whenever a material, article or piece of equipment is identified by reference to manufacturers' or vendors' names, trade names, catalogue numbers, etc., it is intended merely to establish a standard; and any proposed material, article, or equipment of other manufacturers and vendors which will perform adequately the duties imposed by the general design will be considered equally acceptable provided it is in the opinion of the Town to be of equal substance and function.

ARTICLE 8. PRICES

Bidders shall state the proposed price in the manner as designated in the Bid Proposal Form. In the event that there is a discrepancy between unit prices and the extended totals, the unit prices shall govern. In the event that there is a discrepancy between the price written in words and written in figures, the prices written in words shall govern.

The prices in this bid shall be irrevocable for ninety (90) days, or until the bid is awarded by the Town Council. After award by the Town Council, said prices shall then remain firm for the duration of the Contract.

ARTICLE 9. TAX EXEMPTIONS

The Town is exempt from payment of the Rhode Island Sales Tax under the 1956 General Laws of the State of Rhode Island, 44-18-30 Para. I, as amended. The Town is exempt

from payment of Federal Excise Taxes. The prices bid must be exclusive of taxes and will be so construed. Exemption certificates will be completed as required by the successful bidder.

ARTICLE 10. CONTRACT PERIOD AND TERM OF AGREEMENT *(When Applicable to Bid)*

Contract period is found in the Standard Form of Agreement. If financially advantageous to the Town of North Kingstown, these contracts may be renewed or extended, from time to time, when agreed to, in writing, by both parties.

ARTICLE 11. LABOR REGULATIONS *(When Applicable to Bid)*

The following paragraphs regarding nondiscrimination in employment shall be included and become part of these specifications:

a. Contractors shall comply with the provisions of the General Laws of Rhode Island and attention is called to Title 37, Chapter 13, Section 1-16, relative to the payment of wages, obligations and charges by Contractors on public works projects.

b. Non-resident Contractors are subject to Section 44-1-6 of the Rhode Island General Laws, as amended. (OUT OF STATE CONTRACTORS.)

c. The successful bidder will be required to comply with the Davis-Bacon Act (40USC 2 to a-7) as supplemented by Department of Labor regulations (29CFR Part 5).

d. The successful bidder will be required to comply with the Contract Works Hours and Safety Standards Act (40 USC 327-330) as supplemented by Dept. of Labor Regulations (29CFR, Part 5).

e. The successful bidder will be required to comply with Executive Order 11246, entitled Equal Employment Opportunity, as amended, and as supplemented in Department of Labor regulations (41 CFR Part 60).

f. The successful bidder will be required to comply with the Copeland "Anti-Kickback" Act (18 USC 874) as supplemented in Department of Labor regulations (29 CFR, Part 3).

g. The successful bidder will be required to comply with the Safety and Health regulations (29 CFR, Part 1926 and all subsequent amendments) as promulgated by the Department of Labor.

h. The successful bidder will be required to comply with Title VI of the Civil Rights Act of 1964 (P.L. 88-352).

ARTICLE 12. INSURANCE *(When Applicable to Bid)*

The Vendor shall assume responsibility and liability for all injuries to persons or damages to property, directly or indirectly due to, or arising out of, their operations under the contract and shall be responsible for the proper care and protection of all work performed until completion and final acceptance by the Town.

The Vendor shall also indemnify and save harmless the Town of North Kingstown against any and all claims of whatever kind and nature due to, or arising out of, their breach or failure to perform any of the terms, conditions, or covenants of the contract resulting from acceptance of their bid.

The Vendor shall furnish the Purchasing Agent with certificates of insurance from companies acceptable to the Town of North Kingstown. All insurance companies listed on certificates must be licensed to do business in the State of Rhode Island. The Vendor shall provide a certificate of insurance as specified in the bid specifications. Contracts of insurance (covering all operations under this contract) shall be kept in force until the contractor's work is acceptable by the Town.

The limits of the insurance must be at least in the amounts specified below;*

1. Commercial General Liability-Occurrence Form $1,000,000/$1,000,000.

2. Automobile Liability - $1,000,000. With both of the above naming the Town as additional insured.

3. Worker's Compensation (if legally allowed and available). Waiver of subrogation applies to Worker's Compensation

The Vendor shall secure, pay for and maintain insurance as necessary to protect themselves against loss of owned or rented capital equipment and tools, with provision for waiver of subrogation against the Owner, and shall secure, pay for and maintain insurance as necessary to protect against errors and omissions which may result from this project.

ARTICLE 13. LAWS, ORDINANCES, AND CODES

All applicable Federal and State Laws, Ordinances and Codes of the Town of North Kingstown and regulations of all authorities having jurisdiction over this Project shall apply to this contract the same as though written herein in full.

The Town of North Kingstown will not award the Contract to any Contractor who is, at the time, ineligible under the provisions of any applicable regulations issued by the Secretary of Labor, United State Department of Labor, or is not qualified under applicable Ordinances of the Town of North Kingstown, or the laws of the State of Rhode Island.

TOWN OF NORTH KINGSTOWN
INFORMATION SYSTEMS SECURITY
RISK ASSESSMENT AUDIT

GENERAL INFORMATION

OVERVIEW

The Town of North Kingstown (Town) is soliciting a Request for Proposals (RFP) from qualified firms who can provide an Information Systems Security Risk Assessment Audit for the Town. The purpose of this RFP is to request an independent assessment of the Town's IT operations, internal security, and compliance controls and related policies and procedures. This assessment should include a review of on-premise systems and cloud-deployed solutions.

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 Application Service Providers (ASP), As-A-Service, and Cloud offerings.
- Recommend 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 Information Systems Director of threats.

BACKGROUND

The Town of North Kingstown serves an area of 58.3 square miles, with an estimated population of 26,320. The Town's fiscal year begins July 1st and ends June 30th. The following services are provided to its residents:

- General Government
- Public Safety
- Human Services
- Recreation and Leisure Services
- Public Works
- Online permitting
- Code Enforcement/Planning
- And more…

The Town is broken down into several departments and divisions which use different internal and external systems for processing data and information.

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), Chief Information Security Officer (CISO) or Certified Computer Examiner.

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

TERM OF SERVICE

The Consultant will be expected to commence services on or before May 15, 2020 subject to contract execution. It is anticipated the initial assessment audit will be completed no later than forty-five (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.

SCOPE OF 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.

    ✓ Deliverables:

    - Review and provide feedback on physical security
    - Review and provide feedback on information security
    - Review and provide feedback on identity management
    - Review and provide feedback on Cloud / ASP / SaaS applications

- Develop a plan / trajectory with recommendations to the Town
- Present and review the above and any discovered gaps and observations with Town Management

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 and provide feedback on currently implemented information security policies and standards
   - Benchmark current policies and standards against ISO, NIST, OWASP, PCI and SANS standards
   - Develop a plan/trajectory with recommendations to the Town
   - Develop and finalize revised information security policies and standards
   - Present and review the above and any discovered gaps and observations with Town management

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

   a. Internal Network – all internal corporate systems to include workstations, servers, switching/routing infrastructure, Active Directory Structure, virtualization and storage infrastructure, and other connected IT devices. Including all Demilitarized (DMZ) systems to include flow controls from external to internal systems.
   b. External Network – All external public facing systems to include firewalls, load balancers, web servers, file transfer protocol (FTP) servers, and web service interface points.
   c. Wireless Network – All wireless systems to include internal touch points from all Service Set Identifier (SSID), broadcast or hidden, as well as encryption levels.
   d. Physical access controls testing – Determine if the current physical security is effective by conducting physical access assessments;
   e. Remote Access/External Partners – Assess remote access and security of network connections and data traffic to and from external partners.
   f. 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 Information Systems Director.

g. Internet usage – Asses URL/web filtering and access restrictions.
h. Host based security – Assess security of critical systems at operating system and database layers and associated identity and access management controls.

✓ Deliverables – The Consultant will be required to present to the Information Systems Director 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.

a. Testing will attempt to compromise networks and operating system to identify vulnerabilities to the system.
b. Assess the provided network(s) to identify potential vulnerabilities.
c. Exploit vulnerabilities and provide evidence of unauthorized access to approved subnets and systems.
d. Penetration testing should be performed from two perspectives:

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

e. Evidence gathered as proof of access must not harm the confidentiality, integrity, or availability of the systems, application, and or data.
f. 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 Information Systems Director.

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) 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:

    a. segregation of duties,
    b. documented and applied policies and procedures,
    c. acquisition, development and change control practices,
    d. database administration practices,
    e. production control practices,
    f. access and transaction authorizations,
    g. monitoring practices; and
    h. 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:

1) Highlight successes and identify gaps based on CSF target maturity of "Implemented" or level 3.
2) Security maturity comparison against similar organizations (public sector) and similarly sized organizations
3) Rank criticality of gaps

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

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

- Develop detailed recommendations to close gaps which includes:

1) Recommend mitigation solutions
2) Estimated Town budget requirements range for mitigation deployment and ongoing support
3) Town staffing requirements range for both deployment and ongoing support
4) 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 the Information Systems Director 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.

SUBMISSION OF PROPOSAL

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 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 (3) 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

f. The Town reserves the right to contact these organizations regarding the services performed by the Respondent.
g. 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), Chief Information Security Officer (CISO) or Certified Computer Examiner, and ideally have demonstrable work history with technology audits and assessments.

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

j. 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.
k. 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.
l. 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.
m. 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.
n. A concluding statement as to why the Respondent is best qualified to meet the needs of the Town.
o. 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.

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:

    1) Certified Information Systems Security Professional (CISSP),
    2) Certified Information Systems Auditor (CISA),
    3) Certified Information Systems Manager (CISM),
    4) Chief Information Systems Officer (CISO)
    5) Certified Computer Examiner.
    6) 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:

    1) Identification of programmatic weaknesses,
    2) Establishment of targets for continuing improvement of operations,
    3) Internal controls and,
    4) 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.

SELECTION PROCESS

This Request for Proposals does not commit the town of North Kingstown award a contract or pay any cost incurred in the preparation of this proposal to this request. All proposals submitted in response to this Request for Proposals become the property of the Town of North Kingstown. The Town of North Kingstown 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 Proposals, and to waive any informality if it is in the best interests of the Town to do so.

The Information Technology Advisory Committee (ITAC) 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 Information Systems 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 Information Systems Director shall review said proposals and negotiate an agreement based on those discussed.

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

TOWN OF NORTH KINGSTOWN
INFORMATION SYSTEMS SECURITY
RISK ASSESSMENT AUDIT

PERFORMANCE DATA FORM

The undersigned certifies under oath that the information provided herein is true and sufficiently complete so as not to be misleading.

RESPONDENT: _____

Experience of the firm in **like projects completed**. Please provide a listing of at least three (3) references pertaining to like projects completed. If more space is required, please attach additional sheets.

Project/Description/Cost	Status/ When completed	Name/Address Of Owner	Name & Phone # of Contact at Owner

Listing of references pertaining to like projects **currently in progress**, which you feel will qualify you for this work. If more space is required, please attach additional sheets.

Project/Description/Cost	Status	Name/Address Of Owner	Name & Phone # of Contact at Owner

TOWN OF NORTH KINGSTOWN
INFORMATION SYSTEMS SECURITY
RISK ASSESSMENT AUDIT

QUALIFICATION STATEMENT

The undersigned certifies under oath that the information provided herein is true and sufficiently complete so as not to be misleading.

1. Respondent: _____

   Address: _____

   _____

2. Submitted to: _____

   Address: _____

   _____

3. Name of Project: _____

4. Organization: _____

4.1: The submitting company is a ( ) Corporation ( ) Individual
( ) Partnership ( ) Joint Venture ( ) Other _____

4.2: If your firm is a corporation, answer the following:

4.2.1: Date of Incorporation: _____

4.2.2: State of Incorporation: _____

4.2.3: President's Name: _____

4.2.4: Vice President's Name: _____

4.2.5: Secretary's Name: _____

4.2.6: Treasurer's Name: _____

4.3: If your firm is a partnership, answer the following:

4.3.1: Date of Organization: _____

4.3.2: Name of General Partners: _____

_____

_____

4.4: If your firm is individually owned, answer the following:

4.4.1: Date of Organization: _____

4.4.2: Name of Owner: _____

4.5: How many years has your firm been in business and how many years of experience does your firm have with similar projects? _____

_____

5 EXPERIENCE:

5.1: Claims and Law Suits: (If the answer to any of the following questions is YES, please attach details.)

5.1.1: Has your firm ever failed to complete any work awarded to it? _____

5.1.2: Are their any judgments, claims, arbitration proceedings or suits against your firm, its principals or officers? _____

5.1.3: Has your firm filed any lawsuits or requested arbitration with regard to any contracts within the last five years? _____

5.2: List the people that will be assigned to this project and indicate their specialties. Attach their resumes and field experience. Identify their experience and relation to your firm.

Name:	Specialty:
_____	_____
_____	_____
_____	_____
_____	_____

TOWN OF NORTH KINGSTOWN
INFORMATION SYSTEMS SECURITY
RISK ASSESSMENT AUDIT

SUBMITTED this _____ day of _____, 2019.

NAME OF FIRM: _____

SIGNED BY: _____ TITLE: _____

PRINT NAME: _____

Subscribed and sworn to before me this _____ day of _____, 2019.

_____
Notary Public

My commission expires _____

TOWN OF NORTH KINGSTOWN
INFORMATION SYSTEMS SECURITY
RISK ASSESSMENT AUDIT

The undersigned hereby authorizes any person, firm or corporation to furnish information requested by the Town of North Kingstown, Rhode Island in verification of the recitals comprising this Statement of Qualifications and Performance Data form.

FIRM NAME: _____

BY: _____

NAME/TITLE: _____
(Please Print)

DATE: _____ TELEPHONE NO: _____

TERMINATION, SUSPENSION OR ABANDONMENT

This Agreement may be terminated by either party upon not less than thirty (30) days' written notice should the other party fail substantially to perform in accordance with the terms of this Agreement through no fault of the party initiating the termination.

This Agreement may be terminated by the Owner upon not less than fourteen days' written notice to the Consultant in the event that the Project is permanently abandoned. If the project is abandoned by the Owner for more than ninety (90) consecutive days, the Consultant may terminate this Agreement by giving written notice.

Failure of the Consultant to provide the required services in the defined time frame shall be considered substantial nonperformance and cause for termination.