Contents
1. INTRODUCTION ......................................................................................................................................... 2
2. BACKGROUND INFORMATION .................................................................................................................. 2
   A. Initial Assessment ................................................................................................................................. 3
   B. Security Review ..................................................................................................................................... 4
   C. Risk Management Plan ......................................................................................................................... 4
   D. Information Assurance (IA) plan - Security Plan ................................................................................... 4
   E. Internal Audit Plan ................................................................................................................................ 5
   F. Not Included .......................................................................................................................................... 6
3. SUBMISSION REQUIREMENTS ................................................................................................................... 6
   Letter of Transmittal: ................................................................................................................................ 6
   Profile: ....................................................................................................................................................... 6
   Support: ................................................................................................................................................... 7
   Proposal: ................................................................................................................................................... 7
   Reports: ..................................................................................................................................................... 8
   Cost of Services ......................................................................................................................................... 8
4. Evaluation Criteria ..................................................................................................................................... 8
   A. Approach and Methodology ................................................................................................................. 8
   B. Experience of the Firm .......................................................................................................................... 8
   C. Project Staffing and Experience ............................................................................................................ 8
   D. Satisfaction of Clients/End Users .......................................................................................................... 8
   E. Pricing .................................................................................................................................................... 8
5. Miscellaneous ........................................................................................................................................... 9
REQUEST FOR PROPOSAL INFORMATION TECHNOLOGY SECURITY SERVICES

Proposals will be received by <company name> for Information Technology Security Services. Interested vendors should submit one copy of their proposal response documentation before deadline as stated in the project timeline.

IT SECURITY SERVICES

Vendors are required to provide as much detail as possible in this proposal, regarding scope of services, approach to protecting and securing the technology used by <company name> users, and their capability and experience. <COMPANY NAME> will utilize evaluation and selection criteria, based on <COMPANY NAME>’s standard proposal process, to determine an acceptable vendor. <COMPANY NAME> reserves the right to reject any or all proposals or to accept any proposal considered most advantageous.

REQUEST FOR PROPOSAL INFORMATION TECHNOLOGY SECURITY SERVICES

1. INTRODUCTION

<COMPANY NAME> is requesting proposals from qualified, professional technology vendors for Information Technology SECURITY Services. The qualified vendor would provide necessary technical services, which would enable <COMPANY NAME> to:

- Protect and secure its technology facilities
- Ensure the secure operation of its data processing networks and related computer systems in a defined user community
- Enhance security awareness for departments defined in the enclosed schedules

The ideal vendor will resolve security issues in regard to computer systems and network infrastructure in accordance with security standards and acceptable Best Practices for <COMPANY NAME>. The successful vendor will be expected to provide solutions to continuously monitor systems to safeguard against security threats. In addition the successful vendor will ensure all security controls follow security governance frameworks associated with <COMPANY NAME>. Areas of immediate concern for <COMPANY NAME> include: monitoring and analysis, networks and communication, risk, response and recovery, and security operations.

- The vendor is expected to report on status of technology security issues and communicate effectively with <COMPANY NAME> departments.

2. BACKGROUND INFORMATION

<COMPANY NAME> does NOT have an IT Department and is currently using an outside vendor service to provide security maintenance and support on an as needed basis for its user community.

There are two (2) Microsoft Windows server being utilized throughout <COMPANY NAME>’s departmental infra-structure. These servers use Windows server 2008 r2, VMWare ESX, and have
various memory and hard drive sizing. Other detailed information about the specifications is available for review, as necessary.

There are: 46 desk top computers, 20 Laptops, five (5) iPads, and 20 Smart phones in the departmental areas to be covered under the service and support agreement with the successful vendor. These PC’s are located throughout the first and second floor of the building. These PC’s vary by manufacturer, aging, specifications, software, and service pack versions. Windows 7 and Windows 8 are the prevalent systems used on the workstations. <COMPANY NAME> deploys Trend Micro as its prevalent anti-virus software and uses various versions of Windows software.

**Figure 1 Data Center Layout**

Attached please find Schedule A, depicting the equipment and software in summary form. The detail describing the inventory is available to all bidding parties per request.

This section summarizes the services to be provided to <COMPANY NAME> in this RFP. We are looking for content, organized effort, and solution-oriented procedures.

A. Initial Assessment

Review of the inventory, assessment of the system architecture and equipment for security and current processes, and make recommendations for improving routine SECURITY criteria and eliminating
emergency maintenance situations. A report of this initial security assessment shall be submitted by Nov. 20, 13 and each Nov. 20, as long as the contract is in force. This is to allow for necessary budget planning for the upcoming year.

B. Security Review

<COMPANY NAME> is requesting proposals for a review of the information security status. The goal is to provide <COMPANY NAME> with a report identifying areas of weakness that should be addressed. This Request for Proposal (RFP) will be used to establish a contract or contracts for the services necessary to conduct the review and generate a detailed report.

See Appendix A for security review results.

C. Risk Management Plan

Define the risk management methodology to be used, the risk assumptions, the roles and responsibilities, the timeframes, risk rating/scoring techniques, establish risk thresholds, define risk communications, and develop a risk tracking process (H2a_Risk_Assessment_Matrix), to make available to <COMPANY NAME> personnel upon request.

D. Information Assurance (IA) plan - Security Plan

This plan shall include the following policy and procedures:

- Acceptable Use Policy
- Password Policy
- DB Password Policy
- Ethics Policy
- Information Sensitivity Policy
- Internal Lab Security Policy
- Internet usage Policy
- Personal Communication Devices and Voicemail Policy
- Anti-Virus Guidelines
- Lab Anti-Virus Policy
- Email Use
- Email Retention Policy
- Automatically Forwarded Email Policy
- Interconnection
- Internet DMZ Equipment Policy
- Extranet Policy
- Remote Access
- Remote Access Policy
- Virtual Private Network (VPN) Policy
- Wireless Communication Policy
- Firewall
- Server Security Policy
- Router Security Policy
- Server Malware Protection Policy
Maintenance and SECURITY of network equipment, including switches, firewalls, routers, and other security devices is included.

Proactive monitoring of network equipment, including performance indicators to report on threshold limitations; network performance and capacity management services; continuous troubleshooting are required.

Security assessment of networks and computer systems, including complex applications, databases, messaging, servers and associated hardware, software, communications, and operating systems, necessary for performance, security, reliability, and recoverability of the systems.

Scheduling of routine vulnerability assessments and security monitoring of equipment in the areas of coverage is properly and promptly performed; maintenance of records for all security reports will be maintained by <COMPANY NAME>. Quality assurance for backup plans and procedures are being followed.

Configuration management, including changes, upgrades, patches, etc. is maintained; management of user login’s and password security is documented; and support of software products relating to servers and workstation security.

Maintenance of network documentation for daily, weekly, and monthly security services is required.

E. Internal Audit Plan

This plan will include the following:

1.0 GENERAL INFORMATION
1.1 Purpose
1.2 Scope
1.3 System Overview
1.4 Project References
1.5 Acronyms and Abbreviations
1.6 Points of Contact

1.6.1 Information
1.6.2 Coordination
2.0 AUDIT PROCESS
2.1 Type of Internal Audit
2.2 Internal Audit Subject
2.3 Roles and Responsibilities
2.4 Method of Internal Audit
2.5 Schedule

3.0 EVALUATION

F. Not Included

The contract to be awarded does not obligate <COMPANY NAME> to purchase computer equipment, hardware devices, cabling, licenses, software et al from the successful vendor. Replacement parts and services are not part of this contract. The scope also does not include computer equipment and networks systems not owned by <COMPANY NAME> such as PRI, and OPS systems.

3. SUBMISSION REQUIREMENTS

<COMPANY NAME> is requesting that the proposal submitted address the subjects with specificity. We are looking for content, organized effort, and solution-oriented procedures. The goal is a secure, smooth operating, efficient process, and systems that use effective information security technology methods.

Due to the nature of this proposal, it is requested that each proposal be brief and to the point and consist of no more than thirty pages. Each proposal shall provide the following information:

Letter of Transmittal:

The letter of transmittal must contain the following statements and information:

1. Company name, address, telephone number(s), and website.
2. Name, title, email address, and telephone number of the person(s) to contact and who are authorized to represent the firm and to whom correspondence should be directed.
3. Federal and State taxpayer identification numbers of the firm.
4. A brief statement of your understanding of the services to be performed and make a positive commitment to provide services as specified.
5. The letter must be signed by a corporate officer or person authorized to bind the vendor to the proposal and cost schedule.
6. A statement indicating that the proposal and cost schedule will be valid and binding for ninety (90) days following the proposal due date, and will become part of the contract negotiated with <COMPANY NAME>.

Profile:

1. Provide a short profile of the firm including at a minimum:
   a) Length of time in business.
   b) Length of time in providing proposed services.
c) Number of clients.

d) Number of clients in the public sector.

e) Number of full-time employees and area of involvement: Technical Support, Programming, Consulting, Sales Support, Administrative Support:

1. Location of office to service the account.
2. Small, Minority-owned, and Woman-owned business, if applicable.

Proposal:

1. Description of the approach the firm will use in providing the services requested. Description of how the firm is positioned to provide the services requested, with a history of experience on providing similar services.

2. Name, title, address, and telephone number of three references for clients, whom similar services have been provided, including information referencing the actual services performed, number of users, and length of tenure.

3. Naming of staff resources, with identification of principals and key personnel,
   1. who are available to provide the services;
   2. experience and expertise of staff;
   3. local availability of staff is an important consideration
   4. Role and responsibilities that each staff member will have.

4. SECURITY services questions to be addressed:
   - The security risks and threats to the organization.
   - What are existing and potential attacks and exploits
   - Use a variety of security and incident data to design administrative, physical, and network control plans.
   - Support availability (days of week and time)
   - Toll free number
   - Structure of charges for support
   - Response time and goal for resolving security issues
5. Scope of services beyond the RFP that the firm provides which may be of interest to <COMPANY NAME>.

6. Proposal summary, including why the firm is pursuing the work and how it is uniquely qualified to perform the services.

Reports

The vendor shall submit security reports on a quarterly basis, summarizing vulnerability assessments and IT security policy issues. The Vendor must be available to meet with the Director of Finance and Administration and/or the President and CEO to review quarterly reports and discuss issues.

Cost of Services

<COMPANY NAME> is requesting that the vendor submit a FIXED FEE service contract for a twelve month period, with an option to renew for a second twelve months. Each twelve month period must be shown separately. Payment schedule should also be included (ie monthly, quarterly)

Vendors must list, specifically, any services which would not be covered in the proposal price. The vendor shall indicate the impact, if any, of changes in <COMPANY NAME>’s IT infrastructure (number of servers and PC’s) on the fixed fee. Identify the following for those services not under the fixed fee:

a) A fee schedule containing the vendor hourly rates

b) A description of how services will be billed

c) A description of additional charges, as in out-of-pocket expenses for travel, subsistence, etc.

4. Evaluation Criteria

A selection committee, appointed by <COMPANY NAME> Finance Committee, will review the vendors’ qualifications. From this review, an evaluation and selection process will be completed using the following criteria as a benchmark for making a recommendation. <COMPANY NAME> will award the contract. The criteria are shown below:

A. Approach and Methodology

B. Experience of the Firm

C. Project Staffing and Experience

D. Satisfaction of Clients/End Users

E. Pricing

A rating system, based on pre-defined points and percentages, will be used to evaluate the proposals. The award of the contract will be made to the firm, whose proposal receives a favorable evaluation, recommendation of the selection committee, and approval of the Board of Directors.
5. Miscellaneous

<COMPANY NAME> Board and committee reserve the right to reject any or all proposals for failure to meet the requirements contained herein, to waive any technicalities, and to select the proposal which, in <COMPANY NAME>’s sole judgment, best meet the requirements of the program.

The RFP creates no obligation on the part of <COMPANY NAME> to award a contract or to compensate the Bidder for any costs incurred during proposal presentation, response, submission, presentation, or oral interviews. <COMPANY NAME> reserves the right to award a contract based on proposals received without further discussion or negotiation. Vendors should not rely upon the opportunity to alter their qualifications during any discussions.

<COMPANY NAME> further reserves the right to make such investigation as it deems necessary, to determine the capability of the vendors to furnish required services, and vendors shall furnish all such information for this purpose as <COMPANY NAME> may request.

Vendors must specifically identify any portions of their submittals, deemed to contain confidential and proprietary information, or trade secrets. The vendors may be required to justify why <COMPANY NAME> should not, upon written request, disclose such materials.

All requests from the vendor for additional information must be made in writing (includes email), and this information provided will be made available to all vendors at the discretion of <COMPANY NAME>.