Network Security Audit and Vulnerability Assessment RFP

SEPTEMBER 17, 2018

BARRY COUNTY, MICHIGAN

Barrycounty.org

Introduction

Barry County Information Technology Department provides technology services to internal departments and partner agencies with a focus on providing a secure, protected network infrastructure dedicated to the protection, reliability, and availability of the County's data. We are looking for a service provider to help determine the maturity of the County's information security program, while providing expert technical insight that will assist us in improving efficiency and security in the future, as well as meeting our compliance requirements in regards to the new Michigan State Office of Child Support Independent Security Audit Requirements.

Barry County is soliciting proposals from qualified independent service providers with security assessment experience sufficient to perform a Network Security Audit and Vulnerability Assessment in accordance with the specifications outlined in this document. Deliverables from the assessment must include a findings document to include any non-compliant network vulnerabilities; a risk analysis listing the priority of each risk or vulnerability identified (i.e. high/med/low) and a roadmap document outlining technologies and best practices that the County should focus on to improve its security model.

RFP Submission

All quotes may be submitted via electronic and/or print formats. Please include the original Scope of Work document, a Statement of Work as described below, the pricing breakdown worksheet, and a signed signature page.

Barry County will accept proposals and bids from Monday, September 17, 2018 and will close the RFP on October 5, 2018, at 12:00pm. The RFP opening will be at the Barry County Administration Office on Monday, October 8, 2018 at 10:00 a.m.

Email submission: ldennison@barrycounty.org (please include "IT Security RFP" in subject line)

Hard copy submission: Barry County Administration
IT Security RFP
220 W State St
Hastings, MI 49058

Barry County retains the right to accept or decline any proposal or bid. The bid award will be determined by what best meets the needs and interest of Barry County.

Any questions will be addressed at a pre-bid meeting, located at the Tyden Center, 121 S Church St., Hastings, MI 49058. Thursday September 27, 2018 10:AM. If you cannot attend this meeting, please submit any questions you have previous of the meeting, so that the answers can be shared.

Vendor Requirements

The service provider must submit an executive summary, which outlines its proposal, including the proposed general management philosophy. The executive summary should include an identification of the proposed project team, the responsibilities of the project team, and a summary description of the services proposed. The vendor should also provide sample reports similar to the ones to be delivered (see list of deliverables below).

The service provider must submit a Statement of Work and proposed timeline, which describes tasks associated with the services including the vendor and Countys' responsibilities along with the deliverables for each task of the project. Any County responsibilities identified should indicate the required skills needed.

The service provider must have Computer Information Security Audit (CISA) certified security experts (or equivalent certifications) with an onsite presence.

The service provider must provide three former customers as references for which similar services were performed (preferably local government).

Scope of Work

The vendor will perform a Network Security Audit and Vulnerability Assessment review that will address the following areas of the County's infrastructure:

1. Edge Security
    a. Perform ping sweep and port scan of external IP addresses
    b. Perform vulnerability scan of all external IP addresses
    c. Review configurations of demilitarized zone (DMZ) including access lists
    d. Review ingress and egress firewall policies
    e. Review network address translation rules for publishing internal systems
    f. Verify firewall inspection layer - application layer / stateful inspection
    g. Determine if reverse proxy is in place for inspecting encrypted traffic and pre-authentication
    h. Determine if any unified threat management is configured for the edge security
    i. Review current auditing policies and practice for edge security devices
2. Network Security
    a. Review switch configurations to determine if network segmentation configured between networks
    b. Determine if any internal firewalls are in place between workstations and servers
    c. Determine if encryption is configured to protect internal communications
    d. Review wireless security settings to validate security measures in place
    e. Validate port security and whether or not network ports are active by default and if port security enforces based on MAC address
    f. Determine if any network intrusion detection or prevention systems are providing network scanning
3. Systems Security
    a. Perform ping sweep and port scan of internal IP addresses
    b. Review all servers and workstations(see appendix) in the environment to determine if the following configurations have been made or security measures are in place
        i. Have any unnecessary services been disabled?
        ii. Is an existing patch management solution in place to ensure the latest operating system security updates are installed?
        iii. Review the auditing policies and procedures in place for each system
        iv. Does each system have an updated Endpoint protection application installed to provide for:
            1. Anti-malware
            2. Host IDS/IPS
        v. Are host based firewalls enforced and centrally managed on each endpoint?

vi. Is the local Administrators group membership restricted to privileged accounts?
vii. Are local Administrator and Guest user accounts renamed or disabled?
viii. File shares
    1. Are default file shares still enabled?
    2. What share permissions are configured

4. Audit must meet necessary requirements so as to meet with the requirements Office of Child Support. The Office of Child Support (OCS) offers the following guidance related to the Independent Security Audit requirement contained in Section 4.33(b) of the fiscal year(FY) 2017 Cooperative Reimbursement Program (CRP) Agreement.

5. Access Management
    a. Review the methods of authentication currently in place
    b. Review domain group membership for high privilege groups
    c. Determine policy for using separate accounts for user level access and privileged access
    d. Review the current password policy enforced on the domain
    e. Perform password auditing for existing user passwords on the domain
    f. Review remote access methods and security

Deliverables

- A findings document Assessment document that details and demonstrates all threats and vulnerabilities that are identified. A risk and severity level will be assigned for threats and vulnerabilities identified.

- A risk analysis listing of recommendations based on risk severity, probability, cost, and scope of work. This should also include recommendations that address policy or procedural vulnerabilities.

- A Security Roadmap that lists the technology recommendations for the next 3-5 years and includes a strategic direction in support of the Counties' security infrastructure.

Pricing

Pricing MUST include all aspects of the Project. Service providers should provide a summary sheet including approximate hours per task per county, based on the requirements and terms set forth in the Scope of Work. Pricing must be all-inclusive and cover every aspect of the Project.

Evaluation Criteria

The project will be awarded by consensus of County IT/Administration Departmental representatives. Factors to be considered; demonstrated competence in network security assessment/audit, ability to handle a project of this size, references, examples of completed projects, cost.

Appendix

Network Resources

VMWare Cluster physical servers (3), virtual (35), SAN (1)

Domains (1) Controllers (5)

Physical Servers (7)

External IPs (21)

Firewall (1)

Routers (5)

Layer 2 Switches (40)

Endusers (200)

Email on prem (Exchange)

IIS and Apache in use