

Request for Proposal

Network Security Assessment

February 13, 2012

Region 5 Network Security Assessment

Request for Proposal (rev. 02/10/2012)

Introduction

The Counties of Region Five Homeland Security provide Information Technology services to internal departments, citizens and businesses 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.

The Counties are 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. This assessment should be based on industry standards and best practices as described by the Computer Security Institute (CSI) and the SANS Institute. 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 Counties should focus on to improve its security model.

RFP Submission

All quotes must be submitted in both electronic and print formats (please include ten copies). Please include the original Scope of Work document, a Statement of Work as described below, the pricing breakdown worksheet, and a signed signature page.

Van Buren County on behalf of Region 5 Homeland Security Planning Board will accept proposals and bids from Monday, February 13, 2012 and will close the RFP on March 16, 2012. The bid opening will be at the Van Buren County Sheriff's Office on March 19, 2012 at 10:00 a.m.

Region 5 Homeland Security Board 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 the Region 5 Homeland Security Board.

Sealed proposals will be accepted no later than 5:00PM on March 16, 2012, at the Van Buren County Sheriff's Office, 205 S. Kalamazoo St, Paw Paw, MI 49079.

Any questions may be directed in writing to Brigitte Vegter via;
E-mail: brigittev@vbco.org

Please submit questions by February 24, 2012 so that we have time to address them before the RFP's are due. All questions will be answered by March 5, 2012, via email attachment.

Request for Proposal

Network Security Assessment

February 13, 2012

Vendor Requirements

The service provider must submit an executive summary, which outlines its proposal, including the proposed general management philosophy. The executive summary shall, at a minimum, include an identification of the proposed project team, the responsibilities of the project team, and a summary description of the services proposed. Highlight any aspects of the proposal which make it superior or unique in addressing the needs of the Counties. The vendor should also provide sample reports similar to the ones expected to be delivered (see list of deliverables below).

The service provider must submit a Statement of Work and proposed timeline, that describes tasks associated with the services including the vendor and Counties' 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 3 former customers as references for which similar services were performed (preferably local government).

Scope of Work

Each county should be considered a separate project with its own deliverables and point of contact.

The vendor will perform a Network Security Audit and Vulnerability Assessment review that will address the following areas of the Participating Counties 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

Request for Proposal

Network Security Assessment

February 13, 2012

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 select workstations(see appendix A) 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. 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

Request for Proposal

Network Security Assessment

February 13, 2012

Deliverables

- A findings 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

The EMHSD Region 5 is requesting a **fixed price** quote for all eight individual projects as well as a grand total. 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, with the total cost for each county listed.

Evaluation Criteria

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

Request for Proposal

Network Security Assessment

February 13, 2012

Appendix A

County	# servers	# workstations	# wireless AP
Allegan	45	1	30
Barry	20	2	5
Berrien	37	1	5
Branch	20	0	2
Cass	20	1	5
Kalamazoo	43	1	16
St. Joseph	9	0	3
Van Buren	40	2	11