

REQUEST FOR PROPOSALS

NETWORK SECURITY VULNERABILITY ASSESSMENT

MADISON COUNTY, NEW YORK

STATEMENT OF PURPOSE

Madison County, New York (MC) is seeking a vendor that can make a positive contribution to MC's business efforts. This may be augmented by details on the approach the vendor would take in addressing and improving MC's business processes. MC recognizes the need to form a relationship with an organization that can assist us with the penetration testing of our assets.

MC's core philosophy is based on creating partnerships with our vendors. We are therefore serious about building and sustaining relationships with our vendors. MC is also focused on ensuring optimum returns and efficiencies with regard to our procurement spending on all goods and services.

We therefore expect our vendors to earn these higher value relationships in the same way that we set out to earn the relationships with our customers, namely with:

- A passion for quality, excellence, and great value;
- Innovative solutions in services and information;
- A capacity to understand, anticipate, and meet our most important needs; and
- Applying MC's values and standards in all we do.

SCOPE OF THE RFP

MC Objectives

Vendors should price proposals that will help MC meet the following objectives:

- To determine the amount of information that can be enumerated from public sources about MC networks and systems.
- To enumerate, validate, and document system vulnerabilities and rank them by risk.
- To exploit selected vulnerabilities so as to demonstrate the feasibility to compromise systems and applications and gain super user privileges.
- To pivot from an exploited system or application in order to gain access to other MC systems and applications.
- To generate and provide comprehensive output from each phase that can be utilized by MC to understand and remediate vulnerabilities and weaknesses.

Tasks/Tests to be Performed

Task 1: An external security assessment and penetration testing.

- Penetration testing that simulates a covert and hostile attack. Vendor will identify specific exploitable vulnerabilities and expose potential access to our systems or sensitive data. Vendor will attempt to gain access to MC's assets through the network resources, infrastructure, and web based applications. The results of the penetration test will clearly articulate security issues and provide sufficient evidence to assist MC with remediating vulnerabilities. The vendor should leave two distinct items to prove/document that system penetration had occurred. Additionally, screen shots must be captured that show the access to the systems compromised.
- It should also include information gathering, vulnerability assessment, and penetration testing of the security mechanisms and measures of technology, connectivity, or services directly related to the site's IT security infrastructure.

Task 2: Internal security assessment and penetration testing of servers and services on internal networks including the following (required task):

- Information gathering, vulnerability assessment, and penetration testing of internal servers including: servers, server services, mainframes, Internetworking devices, remote-access devices, terminal servers, modem servers, and middleware and backend services connected to the preceding devices.
- It should also include information gathering, vulnerability assessment, and penetration testing of the security mechanisms and measures of technology, connectivity, or services directly related to the site's IT security infrastructure.
- Any server accessible from an extranet or the Internet.

Deliverables for All Tasks

Each task will have the following deliverables:

- Documentation containing technician level detailed data and information revealed during the information enumeration, vulnerability assessment, and penetration testing phases.
- An engagement final report to be presented to MC management.
- PowerPoint presentation to MC management reviewing the final report.
- All raw data collected during tasks, including:
 - Data gathered and vulnerability data for each task.
 - Specific data related to exploits, techniques and tools used, and the detail of the process of exploitation.
 - Passwords, confidential data, etc. that was viewed or removed from the compromised systems.
- Explanations of data provided above as requested.
- All documents should contain recommendations to remediate all exposures as well as providing risk rankings for all vulnerabilities discovered and all vulnerabilities exploited.
- The executive presentation will be done at the County office facility in Wampsville, NY.

Not Within the Scope of this Test

- Physical access and security control mechanisms for the organization (security guards, physical access to servers and computing centers, physical access to workstations).
- Security mechanisms and measures relating to technology suppliers, connections, or services not directly related to MC's IT infrastructure.
- Implementation tasks concerning the remediation and solutions proposed as a result of the tests performed.
- Social engineering.
- DOS or any other type of attack that disables or damages any system, application, or end user account.

Other notes:

- Contractor will be required to enter into a standard contract and provide a Certificate of Insurance naming the County as additional insured.
- Point of contact is Mark Scimone, Assistant to the Chairman of the Board, mark.scimone@madisoncounty.ny.gov.
- All questions regarding this request for proposals should be submitted via email to Mark Scimone and all answers will be provided in writing, also via email.
- Please attach a rate schedule
- Sealed proposals will be received in the office of the Purchasing Agent, Madison County Office Building, 138 North Court Street, PO Box 635, Wampsville, NY 13163 until **Friday, February 17, 2012 at 11:00am.**