Questions Submitted

Barry County Michigan

Network Security Audit and Vulnerability Assessment RFP

1. If we cannot attend the September 27 pre-bid meeting in-person, will there be conference call capability so we can call in to the meeting? Yes
2. Does the County have a desired/required timeframe for completing this project (ie: a required date by when the project must be completed, and a desired start date)? We would like to have the project completed in 2018.
3. In the RFP, it states that the service provider must have CISA or equivalent certification with "on-site presence." Can the County clarify what is meant by "on-site presence" (ie: does the County mean that they expect this person(s) to be on site throughout the project, or does it mean that the County expects this person(s) to be involved in performing the work, including when the work is performed on site)? The county expects the qualified personnel to be involved in performing the work, on site preferred but not required.
4. Related to the scope of work to "review wireless security settings to validate security measures in place":
    a. Does the County desire the service provider to use automated tools to assess wireless network security for the County's active wireless access points (WAPs)? Service Provider can use their digression
    b. How many WAPs does the County have, and where are they located? 24, all within 5 miles
    c. Does the County use lite access control points with a central management solution for its WAPs (eg: Cisco WCS, Cisco Prime, etc.)?The County manages its AP's with a Unifi Software Controller.
5. The Appendix indicates that the County has seven "physical" servers and three physical servers in the VMWare Cluster. Are the three VMWare cluster servers a sub-set of the seven physical servers, or in addition to the seven physical servers (ie: there are 10 total physical servers)?Correction on this count: 7 total Physical servers.
6. The scope of work asks that <u>all</u> servers and workstations in the environment be reviewed. Given that a point in time scan of active systems might not include any workstations that are not powered on and active, would it be acceptable to the County if some workstations were not captured in the review? Yes.
7. What operating system and version is in place for the County's servers (eg: Windows server 2012)? Windows Server 08, 12, 16.
8. What operating system and version is in place for the County's workstations (eg: Windows 10)? Windows 10
9. Does the County use a standard image for all workstations? No.
10. Does the County use Active Directory for authentication and identity and access management?Yes.
11. How many internal IPs does the County have that are in-scope for review (internal vulnerability scanning), and approximately how many of them are active?
12. Can all internal IP addresses be accessed from a single location (ie: there is no network segmentation that would require multiple scans from multiple locations to scan all internal IP addresses in-scope)?Not currently as configured
13. Does the County desire un-credentialed or credentialed scans of the internal network/IPs?TBD
14. Are there any restrictions on the time(s) when external and internal scans can be performed (ie: can all external and internal scans be performed during normal "business hours")? Yes
15. The RFP describes this scope of work as an "audit." Does the County expect that this project will be an actual audit that is performed under relevant auditing standards (such as the AICPA attestation standards or government auditing standards)? No. The term "audit" was used in terms of its dictionary definition; "the inspection or examination of a building or other facility to evaluate or improve its appropriateness, safety, efficiency, or the like."
16. Does the County have documented policies and procedures for information security and/or network security that define expected security controls? The County has an information security policy, it does define basic security controls.

17. Has the County had an assessment similar to the one requested by this RFP performed previously? If so, when was it performed and by who? Yes. Not exactly the same but similar, performed in Spring of 2013, Pondurance LLC.
18. Does the County manage its own infrastructure, or is any part of infrastructure management outsourced or performed by a contractor? The County manages its own infrastructure.
19. Is the County's infrastructure (network devices and servers) hosted on premise and/or in a data center that is managed by the County? Yes. Or is any part of the infrastructure hosted in a third-party data center that would require coordination of scanning and reviews with a third-party? No.
20. Is any Federal Tax Information (FTI) stored on a county system or file share that contains IV-D data (ie: are any of the in-scope systems required to be assessed against IRS *Publication 1075* Section 9 as outlined in OCS Exhibit 2017-011E1)? No.

1. Is Barry County looking for an audit confirming the presence of controls or a technical test of control effectiveness or somewhere in the middle? We are looking for something in the middle.
2. Does Barry County also want a vulnerability scan of internal systems? (Specifically asked for in Edge Security but left out of the internal security sections.)Yes
3. How many VLANs / network segments does Barry County have in place? 17
4. Is there a particular compliance framework / program this audit is meant to satisfy other than Section 4.33(b) of the fiscal year(FY) 2017 Cooperative Reimbursement Program (CRP) Agreement. No, there is not.

1. Is attendance at the pre-bid meeting mandatory? NO, it is not mandatory.
2. Will contractor be able to dial into the pre bid meeting as opposed to attending I person? Yes
3.

. For the review of the authentication methods, do you want a review of critical applications? If so, how many are there? No

2. How many high privilege domain groups need to be reviewed, beyond the normal built-in AD groups?None

3. For the password auditing exercise, would you like us to attempt to crack passwords captured or provided to us? No

4. How many different types of remote access are used?Appendix

5. Besides vulnerability scans, does the county wish to have any penetration testing performed (exploitation of vulnerabilities discovered)? List as optional item on pricelist

6. Can you provide more information regarding #4 of the scope of work to meet Independent Security Audit requirements from the OCS guidance? Will post a link on website

5. For step 3.viii, can you describe more of what you are looking for? Analyzing file share permissions/roles/etc. can be very time consuming. Would it be OK to assume we can take a sample of users (e.g. 25 users) to analyze what they can access based on the job duties? Yes. Please specify in quote.

6. The pricing section mentions approximate hours per task, per county. What does the per county mean? Are there additional counties as part of this assessment? Typo.

Would the County consider extending the due date by 1 - 2 weeks? This would allow additional time for responders to consider the questions and answers provided at (or subsequent to) the pre-bid meeting. This would be considered if the number and quality of submissions at the deadline is not acceptable.

Question # 1	Has a Prior Network Security Audit and Vulnerability Assessment been performed on Barry County IT Network Infrastructure?
Response	YES
Question # 2	If so, can you share the prior findings and remediation if any that has been performed?
Response	NO
Question # 3	How many IT employees/contractors support the Barry County IT Network Infrastructure and Systems?
Response	3
Question # 4	Are the IT network and systems in a single location only? If not, describe the multiple locations.
Response	12 buildings across 5 miles also with a remote location
Question # 5	Are any IT operations co-located or support processes performed by a third party?
Response	No
Question # 6	How many physical locations/facilities are to be included for the assessment? What is the approximate square footage of the buildings / facilities?
	TBD
Question # 7	How many external/internal web application interfaces are supported, if any?
Response	3
Question # 8	What are the internal and external address ranges?
Response	TBD
Question # 9	The RFP defines internal network and system scanning to be performed, do you wish to have an External Penetration Scan performed? If not, have you had an external penetration scan performed in the last 12 months?
Response	Pen Test can be listed as an optional service
Question # 10	Do you have any systems or applications residing in a cloud-computing environment? If so, then could you please specify the Virtual Private Cloud (VPC) addresses or ranges (if any).
Response	Yes , No
Question # 11	How many Workstations, Terminals, Point of Sale, Kiosks included in this assessment?
Response	Approx. 200
Question # 12	What are the Application Suite(s) to be included in the assessment (In house, C#, SQL Server, PHP, MySQ)?
Response	
Question # 13	What are the Application Database(s) to be included in the assessment (Microsoft SQL Svr 2014, 2016)?

Response	
Question # 14	Are there any particular network components or services that you would like us to especially focus on or pay attention to, beyond the RFP descriptions?
Response	TBD
Question # 15	Will there be a desire to have any web-based applications assessed? If yes, How many?
Response	No
Question # 16	If yes, there are web-based applications that will be assessed. For the web-based systems that require logins, will any of the testing be authenticated or will all testing be unauthenticated?
Question # 17	Is it okay to use SQL Injection (SQLi) attacks against web-based applications?
	TBD
Question #18	Does client want Cross Site Scripting (XSS) attacks performed against web-based applications?
	TBD
Question # 19	How many physically separate wireless environments are to be tested?
	TBD
Question # 20	For Wireless, do you want to include active exploitation of identified vulnerabilities (penetration testing) or a vulnerability security assessment (vulnerability validation only)?
Response	Validation Only, Pen testing optional
Question # 21	Are you interested in conducting a Social Engineering test? If so, answer the remaining questions in the Social Engineering section.
Response	No
Question # 22	What type of social engineering tests are you interested in? o E-Mail Phishing Attack o Physical Access o USB Drop o Pre-Text Calling How many scenarios for each test selected would you like?
Response	
Question # 23	Regarding the configuration reviews of the server systems to be conducted? How many systems, operating system types, and of what function does the organization want to be tested as part of this assessment?
Response	System info provided in appendix
Question # 24	Regarding Firewall reviews, what make is the firewall, also include the approximate number of firewall rules that are in place on each of the relevant systems.
Response	This information will be provided to contracted service provider.
Question # 25	Which Regulatory or Compliance requirements is IT Services required to follow or meet certification under?
Response	CJIS
Question # 26	Do you maintain or transmit protected health information or medical records (HIPPA) within the IT Operations in electronic format?
Response	Yes
Question # 27	Do you maintain or transmit credit card information (PCI-DSS) or within the IT Operations or Assets in electronic format?
Response	No
Question # 28	What is the approximate number of IT Policies or Control Standards in place?
Response	1

Question # 29	Can you provide System and Application Data Flow diagrams?
Response	No
Question # 30	Can you provide a high level and/or detailed level network diagram?
Response	Yes
Question # 31	Do you have a Disaster Recovery Plan and Incident Management Plan in place?
Response	In Development
Question # 32	Are there any unique requirements for the standard deliverables beyond the RFP description?
Response	No
Question # 33	If a formal presentation of findings is desired, who will be the audience of this presentation? (Executive, Technical, Non-Technical, etc.)
Response	Technical
Question # 34	How many presentations are we expected to give (ex. one executive and one technical, etc.)?
Response	One Technical

1. What is the business driver of the assessment? Meeting the requirements of the IS Policy and MiOCS compliance mandate.
2. Is there a certain compliance mandate driving the assessment?
3. Is this testing focused on the external perimeter, internal network, or both? external perimeter
4. Has the customer conducted a vulnerability assessment or penetration test before? YES
5. Describe the perimeter or topology in scope? (owned by client, outsourced, ISP)
6. How many external hosts are in scope? (respond to network traffic)
7. How many internal hosts are in scope? See RFP Appendix
    a. Servers
    b. Endpoints (workstations, desktops, laptops)
    c. How many remote locations?
    d. Can the remote locations be accessed from the primary location/HQ? (MPLS, P2P VPN, etc.)
8. Does the customer own the hardware, network, and all assets associated with the in-scope assets? YES
    a. Many websites and other hosts are hosted in outsourced environments.
9. Is Social engineering in scope? NO
    a. How many total employees are there (those with an email address)?
10. Internal Assessments:
    a. Are Physical Assessment tests in scope (gaining physical access to restricted areas; data center, research and dev, etc.)No
    b. How many wireless networks are in scope for the wireless security testing? 21 AP
    c. Is the customer open to having CBI ship a “Frag” box which allows CBI to conduct the internal testing remotely? This can be used to eliminate travel costs. YES