COLLIN COUNTY

Office of the Purchasing Agent
2300 Bloomdale Road
Suite 3160
McKinney, Texas 75071
www.collincountytx.gov

ADDENDUM No. FIVE (5)

IT Security Audit
RFP No. 2016-137

Effective: March 16, 2016

You are hereby directed to make changes to the Request for Proposal in accordance with the attached information:

Delete:

Specifications

Replace with:

Specifications (Revised 2) (Changes made in red)

Delete:

Attachment A, Questions & Answers

Replace with:

Attachment A, Questions & Answers (Revised)

Please note all other terms, conditions, specifications drawings, etc. remain unchanged.

Sincerely,
Michalyn Rains CPPO, CPPB
Purchasing Agent

4.0 EVALUATION CRITERIA AND FACTORS

4.1 The award of the contract shall be made to the responsible offeror, whose proposal is determined to be the best evaluated offer resulting from negotiation, taking into consideration the relative importance of price and other factors set forth in the Request For Proposals in accordance with Vernon's Texas Code Annotated, Local Government 262.030.

The Evaluation Committee will review all proposals received by the Opening date and time as part of a documented evaluation process. For each decision point in the process, the County will evaluate contractors according to specific criteria and will elevate a certain number of contractors to compete against each other. The proposals will be evaluated on the following criteria.

The County will use a competitive process based upon "selection levels." The County recognizes that if a contractor fails to meet expectations during any part of the process, it reserves the right to proceed with the remaining contractors or to elevate a contractor that was not elevated before. The selection levels are described in the following sections.

Level 1 - Conformance with Mandatory Technical Requirements

Criteria assessed during Level 1:

- The Offeror's professional personnel have received adequate continuing professional education within the preceding two years.
- The Offeror's has no conflict of interest with regard to any other work performed by the Offeror for Collin County.
- The Offeror's adheres to the instructions in this request for proposals on preparing and submitting the proposal.

The first part of the elevation process is to validate the completeness of the proposal and ensure that all the RFP guidelines and submittal requirements are met. Those offerors who do not meet all the requirements for the RFP may, at the discretion of the County, be contacted to submit the missing information within two business days. Incomplete or noncompliant RFPs may be disqualified.

Level 2 – Detailed Proposal Assessment

The Evaluation Committee will conduct a detailed assessment of all proposals elevated to this Level. Criteria evaluated in Level 2:

Technical Qualifications (Maximum Points - 80)

Expertise and Experience (Maximum Points- 40)

Technical experience of the Offeror to include, but not limited to:

- Recent auditing of local governments.
- Similar auditing, of the type under consideration, during the last three years.
- References.
- Classification of staff (including consultant) to be assigned to the audit. Education, including continuing education courses taken during the past two years, Certifications, position in the Offeror, and years and types of experiences will be considered.

Determination of the following from information submitted:

- Qualifications of the audit team.
- Supervision to be exercised over the audit team by the Offeror's management.

Size and structure of the Offeror to include, but not limited to:

- Capability to meet the services required.
- Additional skills and services.

<u>Meeting IT Audit Business Requirements (Maximum Points 40)</u>

Responsiveness of the proposal in clearly stating an understanding of the work to be performed to include, but not limited to:

- IT Audit coverage.
- Realistic time estimates of each major segment of the work plan and the estimated number of hours for each staff level, including consultants assigned.
- Documentation – hard and soft copies
- Workflow diagrams where applied

Offerors who score 56 points (70%) and above will be elevated to the next evaluation level.

Level 3-Cost

Points	**Description**
20	Cost

Offerors who are elevated to this level will have cost added to their score.

Level 4 –Best and Final Offer

Offerors who are susceptible of receiving award will be elevated to Level 4 for Best and Final Offer. Offeror will be asked to respond in writing to issues and questions raised by the County as well as any other cost and implementation planning considerations in the

proposal, and may be invited to present their responses on-site. Proposals will be re-evaluated based upon Criteria in level 2.

Based on the result of the Best and Final Offer evaluation, a single offeror will be identified as the finalist for contract negotiations. If a contract cannot be reached after a period of time deemed reasonable by the County, it reserves the right to contact any of the other contractors that have submitted bids and enter into negotiations with them.

5.0 SPECIAL CONDITIONS AND SCOPE OF SERVICES

5.1 Authorization: By order of the Commissioners' Court of Collin County, Texas sealed proposals will be received for **IT Security Audit.**

5.2 Intent of Request for Proposal: Collin County's intent of this Request for Proposal (RFP) and resulting contract is to provide offerors with sufficient information to prepare a proposal for comprehensive technical security audit of information technology infrastructure and resources.

5.3 Term: Provide for a term contract commencing on the date of the award and continuing until project is complete.

5.4 Pre-Proposal Conference: A pre-proposal conference will be conducted by Collin County on Friday, February 26, 2016 at 9:30 a.m. at 2300 Bloomdale Road, Suite 3207, McKinney, TX 75071 in the I.T. Conference Room. This is to provide an opportunity for all interested vendors to ask questions. All prospective offerors are requested to have a representative present. It is the offeror's responsibility to review documents to gain a full understanding of the requirements of the RFP. There will be a telephone conference available for the pre-proposal conference, interested vendors may begin calling on 02/26/2016 at 9:15 a.m. CST, by dialing (972) 547-1833.

5.5 Funding: Funds for payment have been provided through the County budgetary process. State of Texas statutes prohibit the County from any obligation of public funds beyond the fiscal year for which a budget has been approved. Therefore, anticipated orders or other obligations that arise past the end of the current Collin County fiscal year shall be subject to budget approval.

5.6 Price Reduction: If during the life of the contract, the vendor's net prices to other customers under the same terms and conditions for items/services awarded herein are reduced below the contracted price, it is understood and agreed that the benefits of such reduction shall be extended to Collin County.

5.7 Completion/Response Time: Contractor shall place product(s) and/or complete services at the County's designated location within the number of calendar days according to the schedule proposed by offeror in section 6.6.

5.8 Delivery/Setup/Installation Location: Locations for delivery and installation will be stated on the Collin County Purchase Order(s). Delivery shall include assembly, setup and installation and shall be included in proposal. Below is the address for work to be completed.

5.9 Testing: Testing may be performed at the request of Collin County, by an agent so designated, without expense to Collin County.

5.10 Samples/Demos: When requested, samples/demos shall be furnished free of expense to Collin County.

5.11 Background Check: All Contractor employees that will be working on site or by VPN shall pass a criminal background check performed by Collin County before any work may be performed. The selected offeror shall be provided the required documents to submit required information for background checks.

5.12 **PROPOSAL SCHEDULE**

RFP released:	**February 16, 2016**
Pre-Proposal Conference:	**February 26, 2016 at 9:30a.m.**
Deadline for submission of contractor questions:	**March 4, 2016 at 5:00p.m.**
Proposals due:	**March 24, 2016 at 2:00p.m.**
Award of Contract:	**July 2016**
Effective date of contract:	**Upon award**

Collin County reserves the right to change the schedule of events as it deems necessary.

5.13 **PURPOSE**

Collin County, Texas (hereafter referred to as the "County") seeks proposals for a comprehensive technical security audit of information technology infrastructure and resources. The County data systems are the heart of County business and audits are necessary to ensure that the IT department operates on a solid foundation. The County views the security assessment and audit as an essential tool to maintain network health, uncover possible vulnerabilities in our voice and data architecture and identify mitigation strategies. The County requires a qualified vendor to perform a complete security audit and assessment. Respondents must have a proven history of successfully completing similar services and functionality for other counties, municipalities, and governmental entities. The County will require that the vendor has acquired the appropriate tools and the required technical certified expertise to aid the County in developing and maintaining a higher degree of threat analysis and prevention for internal and external threats. The scope for this effort, identified in greater detail later in this document, includes:

- Complete network and server security assessment
- Threat analysis and prevention

- Assessment of externally exposed network access points
- Intrusion detection and prevention
- Network account access and security

5.13.1 SCOPE OF WORK

The scope of the audit and analysis engagement, with respect to both the data and voice networks, includes:

- Review the county IT infrastructure from an external perspective through the firewalls to check for intrusion issues and deficiencies
  - Investigate DMZ environment for vulnerabilities
  - Perform non-destructive penetration test of any external identified vulnerabilities to measure ease of exploitation to compromise County systems
  - Verify that external facing services are implemented securely following industry standard best practices
    - Includes servers, connections to third party services and ancillary networks utilized to fulfill the scope of County services
- Complete network and server security assessment
  - Perform an collection of software specifics for all devices connected to 'internet' County network
  - Provide recommendations of best practice based on review of software inventory collected
  - Verify that enterprise risk is minimized through application of patches and updates
  - Confirm that security best practices and procedures are implemented and followed
  - Verification of anti-virus protection and appropriate security update installation and provide recommendations on current trends in endpoint security
  - Verify password protection is appropriate to protect county systems from password hacking attempts via performing a brute force cracking attempt of the current Active Directory infrastructure
  - Review configuration of Intrusion Prevention System, and threat notification systems, and provide recommendations of adjustments to meet best practices
- Assessment of externally exposed network access points
  - Verify that public facing systems, servers, web pages, etc. are appropriately secure
- Assess and test the security of the County wireless networks
  - Inspect the wireless networks for common vulnerabilities

  - Provide recommendations to improve security with the wireless networks
  - Provide recommendations about existing wireless networks with respect to industry best practices
- Confirm that physical security to the MDF and IDF rooms is appropriate
- Analysis of IT staffing allocations, by FTE count and required skill levels, are sufficient to meet the required/recommended levels to maintain the existing network and mitigate any found deficiencies
  - Analysis to include training program recommendations to mitigate skill level deficiencies in order to implement any audit recommendations
  - Analysis shall take into consideration the security tools approved for purchase in the current fiscal year, to determine proper staffing allocations
- Discover any sensitive data that is leaving the County network, by installing and collecting data from a DLP (Data Loss Prevention) sensor during the assessment
- Perform analysis of log data of outbound Internet traffic (via firewall and Internet content filter) to identify risks associated with, but not limited to;
  - Use of County managed social media sites
  - Cloud based file sharing sites
- Assess the use of privileged accounts within the County network
  - Discover any accounts with non-expiring passwords
  - Create a matrix of account with administrative rights across two bodies
    - All County servers (inventory to be provided by County)
    - Detailed ampling of 50 end user workstations (inventory to be provided by Count)
  - Discover use of privileged accounts on the network, based on available logs
    - Identify privileged accounts most actively being used
    - Identify source network device privileged accounts are being used from
    - Identify destination target host privileged accounts are accessing
- Analysis of existing documented County policy, and technical procedures, that support the County's goal of addressing (where applicable) the Top 20 Critical Security controls
- Analysis to include recommendations of policy, and procedure edits, or introductions, needed to support this goal

The County anticipates that the assessment will be divided into three sections; the first section includes interviewing key personnel, the second section involves evaluating the networked resources via discovery tools and the final section involves using vulnerability analysis tools to probe networked resources and attempt to gain access to resources from both inside and outside the network.

During the interview phase the vendor will meet with key technology personnel and facilitate discussions to gain a better understanding of the technology infrastructure. Checklists need to be provided by the vendor technology staff before the on-site interviews so that staff members may be prepared to answer interview questions. During the personnel interviews the following items should be considered but the conversation should not be limited only to these topics:

- Network configurations, architecture and security
- Server configurations, architecture and security
- Storage systems configuration, architecture and security
- Security controls
- User access security
- Intrusion detection and remediation

During the final phase of the on-site security audit, the vendor will perform vulnerability assessments from within and without the organization using various monitoring, auditing and security cracking tools to assess the security of the county systems. Tests of the perimeter systems will also need to be performed against the public facing components of the county network. Open ports are to be discovered, probed for access and any information, along results of the probes, should be recorded and used as the basis for a suggested mitigation plan. The vendor should use a combination of invasive and non-invasive tools to detect any weaknesses in the network and servers. Invasive tests will require coordination with County technology management to provide an estimated time frame in which the tests may be conducted. The outcome of the final phase should be a log of any deficiencies along with recommended mitigation plans and strategies.

5.13.1.1 **PROJECT DELIVERABLES**

Upon completion of the interviews and assessment activities the vendor will compile and present a detailed report on the security findings. Preliminary discoveries of network and server weaknesses,

including architectural or configuration liabilities, and any policy or procedural deficiencies discovered as a result of the review in terms of risk will be included in the comprehensive report. An analysis of the effectiveness of internal network and server controls in preventing unauthorized access will also need to be provided. Analysis of vulnerabilities, along with recommendations on correcting the vulnerability, will also need to be detailed in the report.

DELIVERABLES	DESCRIPTION
Hard Copy Documentation	
Executive Summary	• Summarized version of the detailed report
Initial External Assessment	• Assessment of externally exposed systems and found vulnerabilities
Detailed Report	• Internal and external risk analysis and recommendations • Physical security review of network and security policies • Server and storage operations analysis and recommendations • Comprehensive vulnerabilities assessment and mitigation plan
Electronic Documentation	
Executive Summary	• Electronic version of printed report
Detailed Report	• Electronic version of printed report • Presentation materials of detailed report
Vulnerability Report	• Electronic version of the vulnerabilities assessment and mitigation plan
Six Month Follow-up	
Follow-up	• Facilitate an on-site follow-up with county staff six months after the delivery of the reports • Document the follow-up meeting

6.0 PROPOSAL FORMAT

6.1 **PROPOSAL DOCUMENTS:** To achieve a uniform review process and to obtain a maximum degree of comparability, the proposal shall, at a minimum include a Table of Contents detailing sections and corresponding page numbers.

6.1.1 Proposals may be submitted online via http://collincountytx.ionwave.net or submitted via CD-ROM or Flash Drive. Electronic submissions are preferred.

6.1.2 If submitting manually, proposal shall be submitted in a sealed envelope or box with RFP name, number, and name of firm printed on the outside of the envelope or box. Manual submittals shall be sent/delivered to the following address and shall be received prior to the date/time for opening:

Collin County Purchasing
2300 Bloomdale, Suite 3160
McKinney, TX 75071

Paper copies shall be printed on letter size (8 ½ x 11) paper and assembled using spiral type bindings, staples, or binder clips. Do not use metal-ring hard cover binders. Manual submittals shall include an electronic copy in a searchable format.

It shall be the responsibility of the offeror to insure that their proposal reaches Collin County Purchasing prior to the date/time for the opening no matter which submission method is used.

Proposal shall include but not be limited to information on each of the following:

6.2 **FIRM OVERVIEW**

Offeror is requested to define the overall structure of the Firm to include the following:

6.2.1 A descriptive background of your company's history.
6.2.2 State your principal business location and any other service locations.
6.2.3 What is your primary line of business?
6.2.4 How long have you been selling product(s) and/or providing service(s)?
6.2.5 State the number and locations of where your products/services are in use.

6.3 **PROPOSED PROJECT TEAM/STAFF QUALIFICATIONS/EXPERIENCE/CREDENTIALS**

6.3.1 Offeror is requested to provide qualifications as well as experience information on Offeror's key personnel.

6.4 **PROPOSED PROJECT**

6.4.1 Offeror is requested to identify the proposed services to include but not limited to the following areas:

6.4.1.1 Describe Work Plan for the project based upon the scope of work in Section 5.13.1.

6.5 REFERENCES

6.5.1 Offeror is requested to include at least five (5) references with names, addresses, telephone numbers and e-mail addresses. Preferred references would be those where similar applications have been put in place.

6.6 TIME SCHEDULE

6.6.1 Provide a schedule on each phase of the proposed project beginning with program development and ending with the date of operation. The schedule shall include all tasks that will require time in the process, such as County review (identify amount of time assumed for each task). All work shall be performed during normal business hours (Monday – Friday, 8am – 5pm). Weekend and after hours work will not be permitted.

6.7 PRICING/FEES

6.7.1 Provide an explanation of the total cost of the service(s) showing a breakdown by item. Be sure to include all items necessary to render project complete and operational.
6.7.2 State Not to Exceed Travel Costs.
6.7.3 State Cost for 6 month follow up meeting.

6.8 OTHER PROJECTS INVOLVED WITH

6.8.1 Offeror is requested to provide a list of other projects that you are currently involved with or will be involved with.

6.9 SCOPE OF WORK

6.9.1 Offeror shall provide a response for each of the requirements in section 5.13.1.

IT Security Audit
RFP No. 2016-137

Questions & Answers:

1) In reference to the *"Confirm that physical security to the MDF and IDF rooms is appropriate"* requirement, will this only be a review of physical security of the MDF, or is a social engineering test expected?

   Physical controls only. Social Engineering is out of scope for this RFP.

2) In reference to the *"Discover any sensitive data that is leaving the County network, by installing and collecting data from a DLP (Data Loss Prevention) sensor during the assessment"* requirement… Does the County have an appliance in mind or in place for data loss prevention?

   No we do not a solution in place, nor a preference. Our desire is to understand where our risks for data loss are. Today, we expect email is our primary leak point, but we look forward to any additional loss vectors found during the audit, that we can apply to improving our posture for standards we are measured against (HIPAA, CJIS, PCI, etc…)

3) In reference to the *"Discover any sensitive data that is leaving the County network, by installing and collecting data from a DLP (Data Loss Prevention) sensor during the assessment"* requirement… Do you have a time period in mind for DLP?

   We expect the overall engagement will last longer than 30 days, and that County business cycle repeat on that timetable, so a 30 day snapshot of traffic for DLP analysis should suffice. If an offeror has proven results of a shorter time window, it should be explained in the submission. The County will take shorter windows into consideration.

4) Is the County expecting a full report of vulnerabilities of all 1800 entities on the network, or is a snapshot acceptable?

   Snapshots are acceptable. The County has point in time reports from previous assessments. We are most interested in understanding the quantity of devices on our network. Recommendations on courses of action for software issues that require remediation can be made based on a snapshot of findings.

   The County expects approximately 1800 entities will be found, with about 200 of those being servers.

5) In the RFP specifications you mention mapping top 20 critical security controls, is the top 20 more of a guideline or would you prefer an analysis that's more in depth?

   We would prefer an in depth analysis to map to the Top 20 Critical Controls. CIS Version 6.

6) What is something that the previous provider did really well that you don't want taken away?

   The previous provider provided solid insight into employee behaviors, based on their technical findings. Specifically the analysis of password findings of both our end users and service accounts.

7) Is there anything that the previous provider did that you would have wanted to occur differently?

   This assessment will have more clearly defined rules of engagement for our tests, especially the controlled pen test. Our biggest takeaway from the previous assessment is that at least one County employee, like the IT Security Officer, needs to be informed of all actions that will be taken as part of testing.

8) In regards to the *"Analysis of existing documented County policy, and technical procedures,"* requirement how many pages of reading can the offeror expect to have to perform as part of the assessment?

   Currently, approximate 20-30 pages of documentation for a 'security policy' will be available to be reviewed. Our expectation, is that a recommendation of gaps will be presented based on that documentation review, preferable prioritized for the County to plan implementation of new policy and procedure.

9) Commissioners Court committed to project?

   Yes, the Commissioners Court is sent updates on a regular basis. The IT Security Officer presents updates of Security posture. Additionally, the funds for a security assessment are now part of the yearly base budget, approved by The Court.

10) How long has SIEM been in place?

SIEM has been actively monitored for 1 year. We would like to know if we are collecting data and parsing as we should. We believe that environment is one of our better manicured toolsets, based on a vendor visit for 5 days in late 2015. To that point, an offeror with a partnership with whatever might be our weakest environment, that could offer follow up consulting services, would definitely be noted during proposal review.

11) Physical assessment-MDF and IDF only ones addressed in specifications. Anything else we are at risk for?

Yes. IT will work on putting something together and provide to the selected offeror, for other physically restricted areas that should be reviewed.

12) Where is the County at with SOC operations?

Our IT Security Administrator is operating as the SOC currently. The County is in the process of providing more security knowledge to our operations team. This is an excellent question, and part of the driver for the creation of the *'Analysis of IT staffing allocations…'* requirement.

13) In terms of Data exfiltration, is the County looking to determine what is leaving or technical enforcement of what leaves?

Both. However, more value will be placed on the findings of what is leaving.

14) In terms of the physical access control system, is the system The County is using managed by IT? If so, will we have access to this?

The system is centrally managed. It is not all managed by IT. However, we can gain access if needed. The County will provide a report, listing priority access points to be reviewed, along with those that can pass through those access points. It should be noted, that the County considers recommendation on attestation practices of the physical access system as very valuable information in the final report.

15) Is the IT Security Administrator-the firewall engineer, the manipulator, or the advisor?

The advisor.

16) How large is The County's network team?

Helpdesk- 3 employees
Security team- 2 employees
Network primary- 2
Infrastructure team- 5-6 employees
Technicians-5 or 6 employees

17) For the Wireless Assessment. How many physical facilities will be in scope?

3 facilities, the Admin Building, Courthouse and Sheriff's Office.

18) Once an offeror has been selected, Will IT provide a list of inventories The County has or plans to use?

Yes, we will provide this information, as deemed applicable to this years assessment, to selected offeror during kickoff meeting.

19) Is the County currently using an anti-virus solution?

Yes. And as with all security toolsets, the County values findings on actual coverage of these tools against our asset base. The County would also value recommendations of toolsets based on industry trends.

20) Any major infrastructure upgrade plans?

Yes, we will provide this information to selected offeror during kickoff meeting. The County will also provide insight into security related tools that will be acquired during this fiscal year, for the offeror to reference in reporting.

21) What if the vendor provides pricing for an item that is not needed in the proposal?

If the vendor chooses to provide multiple solutions it shall be listed as an alternate. Refer to Section 6.7.1 Pricing in the specifications for more

information. NOTE: Pricing will only be evaluated for those who are elevated to level 3.

22) Is The County open to awarding this project to multiple vendors?

The County's preference is to award to one vendor.

23) For the controlled pent test, does the system in question have a dedicated IP space, or reside on a shared web front end?

Dedicated.

a) What is a part of the last assessment?

Yes. A vulnerability assessment was performed.

b) Should emphasis of testing be Internal or external, take into account any pivoting?

The County should be able to learn everything that needs to be known from testing, from an internally sourced test of this system. Pivoting is not a primary concern based on network architecture. The County is open to turning on/off perimeter controls to gauge their effectiveness in protecting the system in question.

24) For the controlled pent test, is the county interest in testing authenticated or unauthenticated connections?

Both.

25) Will the data from previous assessment be available to selected offeror?

The County is open to providing this information to the selected offeror during the recommendation phase, on an as needed basis.

26) Does the County place higher value on actual findings or closure of findings?

The actual findings themselves. We learned from our last assessment that purchases needed to be made to remediate some of the mass findings, and it is expected that the same will occur in this year's audit.

27) Wireless network penetration test? Also centrally managed?

Yes and we will test based upon 3 sites (1 Admin, 1 Courthouse, and 1 Sheriff)

28) Is the 911 operations tied into Sheriff Office building?

It is a separate system. Testing of that network is not necessary. We can provide IP space, for exclusion of testing tools.

29) In Section 5.13 and 5.13.1 of the specifications it states voice architecture and voice networks. These are the only statements throughout the specifications that discuss voice networks is this supposed to be a part of the RFP or is it a typo?

Please refer to Addendum No. 2, Specifications (Revised), eliminating voice architecture and voice networks.

30) What is the total number of locations in scope, and their geographic region(s)?

3. All in McKinney, Texas.

31) What is the total number of external (Internet routed) IP addresses in scope and use?

Approximately 40.

32) What is the total number of internal IP Addresses in scope and use?

An estimated 1800.

33) What is the total number of wireless access points in scope and their locations?

Approximately 250 across three physical locations.

34) Are all servers, appliances considered in scope for security testing? If no, enter only those in scope below. Note that any servers/appliances hosted by a third party will require approval.

All devices with the IP address are in scope for identification and vulnerability scanning. Any penetration testing will be performed in a controlled manner, of County owned assets only.

35) Total Number of End-Point Systems:

Approximately 1600

36) Total Number of Internal Servers in Scope:

Approximately 200

37) Total Number of Network Devices In Scope (Including FW's, Switches, Routers, and Include the Vendors for these devices, e.g. Cisco, Juniper, etc.):

Approximately 1800

38) Types of Operating Systems run on servers and end-points:

Primarily Microsoft Windows based, with an approximately 200 Apple iOS devices (tablets and phones) that could be detected in a network sweep for assets/endpoints.

39) Number and Type of Mobile Devices with Access to the internal network. (Any BYOD?)

BYOD is technically possible. The County does not currently have an estimate of mobile devices connecting to the internal wireless network.

40) How many Firewall Devices are in scope for this effort, and approximately how many rules in total?

Two sets of firewall pairs, total approximately 750 rules.

41) How many Security Policies are in scope as part of this effort for the documentation review?

The County currently enforces 3 polices that are intended to be enveloped into a larger Information Security Policy, and would like recommendations on current gaps, with advice on priority of addressing the identified documentation gaps.

42) How many facilities and what types of facilities are in scope for the physical security assessment, if beyond the MDF and IDF rooms?

The scope of this assessment will focus on three locations; Admin building, courthouse and Sheriff's office.

43) What security and privacy compliance requirements, outside of PCI and CJIS, is the County governed by?

HIPPA, as well.

44) Does the County have a data classification scheme in place today?

No.

45) Is the goal of the policy assessment to evaluate implementation of the policy or determine policy gaps against SANS Top 20 Critical Security Controls or both?

Determine gaps.

46) How many staff in IT?

62

47) How many staff support security?

3

48) Regarding the external penetration test, what is the total IP address space to be assessed (i.e.: 512 addresses, 1024 addresses, etc.) and how many anticipated live devices are on the external facing perimeter. Approximate percentage of total IP space is fine (i.e.: 1024 addresses, approximately 50% assigned).

Estimated 256 addresses, that have approx. 25% assigned.

49) How does main bullet point 3 of section 5.13.1 materially differ from the first main bullet point in section 5.13.1? A reader could interpret these as both being addressed with the penetration test. If that is not the customers intention, please explain your desired activities/deliverables for the third main bullet.

In review, the County has noted there is not a difference. Enumerating vulnerabilities in the first bullet point, will satisfy the third main bullet point of 5.13.1.

50) Regarding main bullet point 4 of section 5.13.1, is this task envisioned as a wireless penetration test or as more of a wireless network configuration review activity? Both?

Both.

51) How many locations have wireless access installed that would be in scope for testing?

Please refer to question 34.

a) Approximately how large are the sites?

The Courthouse is roughly 170,000 square feet. The other two locations are smaller.

b) Are all wireless access points controlled/configured from a central controller?

Yes.

c) What is the wireless platform deployed (Aruba, cisco, etc.)?

Cisco

52) Regarding main bullet point 8 of section 5.13.1, how much log data in Gigabytes is there to be reviewed?

Roughly 30GB

a) Is it all in one location/system currently (i.e.: Splunk instance) or what that data need to be collected as part of this task?

The log data currently resides in the web content filter.

b) How far back in time is the vendor requested to search and is there a desire for this to be an ongoing exercise throughout the duration of the engagement, or even beyond?

We expect 30 days will suffice, covering most business cycles for the County. However, if a vendor has proven success using a smaller time window, we are open to that recommendation.

53) Regarding main bullet point 9 of section 5.13.1, how many servers are is scope and what platforms / OS versions are included in that mix?

About 200. All Windows OS.

54) Regarding main bullet 1 of section 5.13.1, sub-bullet 3: Are you envisioning this task to be accomplished through a review of the firewall rulesets, or a configuration review of the servers providing the services?

Both, but primarily a review of server configuration.

a) If a review of the firewall rulesets is expected, what type of firewall(s) (make/model) is in scope and how many total rules?

Two pairs of firewall sets, with 750 rules total.

b) If you would prefer a configuration review of the servers, how many servers are in scope and what type / OS are the servers?

About 10 that are publicly facing. Windows based.

55) Regarding main bullet 2 of section 5.13.1: How many devices are connected to the 'internet' County network?

See question 59.

a) What are the types of devices connected to the 'internet' County network?

WAF, IPS, Threat management platform, internet facing web servers, etc…

56) Regarding main bullet 2 of section 5.13.1, sub-bullet 7: The Intrusion Prevention System stated here, is it a network-based IPS or a host-based IPS?

Network.

a) If network, what type of IPS is it (make/model)?

McAfee NSM

57) In reference to "Complete network and server security assessment" requirement, provide count of live IP's that are to be considered in-scope for this assessment.

See question 63.

58) In reference to "Perform an collection of software specifics for all devices connected to 'internet' County network" requirement, What does this mean for the vendor? Please elaborate.

The expectation of this bullet point, is a collection of software revision levels for all devices outside of the County firewall, roughly 20.

59) In reference to "Provide recommendations of best practice based on review of software inventory collected" requirement, what does this mean for the vendor? Please elaborate.

In our external environment, we're looking for recommendation on components missing, additions we should add to improve our posture, etc…

60) In reference to "Verify that enterprise risk is minimized through application of patches and updates" requirement, what does this mean for the vendor? Is the County asking for identification of missing patches, or application of missing patches?

Identification

61) In reference to "Confirm that security best practices and procedures are implemented and followed" requirement, what does this mean for the vendor? 'Best practices' as defined by who, the county or consultant?

Consultant

62) In reference to "Assessment of externally exposed network access points" requirement, please define 'exposed network access points' and provide a count of live IP's that are to be considered in-scope for this assessment.

256 public IP's. approx. 25% used.

63) In reference to "Assess and test the security of the County wireless networks" requirement, how many physical sites are to be considered in-scope for this portion of the assessment?

Please refer to question 17.

a) How many authorized county wireless networks are to be considered in-scope for this portion of the assessment?

Three.

64) In reference to "Confirm that physical security to the MDF and IDF rooms is appropriate" requirement, How many physical sites are to be considered in-scope for this portion of the assessment?

Three.

65) In reference to "Analysis of IT staffing allocations, by FTE count and required skill levels, are sufficient to meet the required/recommended levels to maintain the existing network and mitigate any found deficiencies" requirement, how many physical sites need to be visited and how many interviews need to be conducted?

Two physical sites. Roughly 15-20 employees.

66) In reference to “Discover any sensitive data that is leaving the County network, by installing and collecting data from a DLP (Data Loss Prevention) sensor during the assessment” requirement, The County is requesting a DLP solution to be deployed, network monitoring, and report findings, is this correct?

a) How does the County expect this to be done as part of this engagement?

The County will provide a network span port (or equivalent) at the edge of the network, for a vendor provide DLP sensor to utilize.

b) Who is going to select a DLP solution?

The vendor.

c) Who will deploy it?

This will be a joint effort. The County will provide network, and physical, support. The Vendor is expected to provide the sensor and manage it.

d) How will it be configured?

Per the recommendations of the vendor.

e) Does the County have a classification policy?

No.

f) How will DLP be ‘trained’?

The County would like a report on ‘standard’ types of data that might be leaking. Social security numbers, credit card numbers, etc…

67) In reference to “Perform analysis of log data of outbound Internet traffic (via firewall and Internet content filter) to identify risks associated with, but not limited to;” requirement, what type of log data will the consultants be reviewing? Is it currently centralized to a single location?

The log data is on not currently centralized. One thing the County is hoping to understand, is how to correlate existing data from those sources to identify data loss, in case a DLP solution cannot be budgeted in the near future.

68) In reference to “Discover use of privileged accounts on the network, based on available logs” requirement, what type of log data will the consultants be reviewing? Is it currently centralized to a single location?

Primarily Active Directory security logs. To note, most of the list data is collected in the County SIEM.

69) In reference to "Analysis of existing documented County policy, and technical procedures, that support the County's goal of addressing (where applicable) the Top 20 Critical Security controls and Analysis to include recommendations of policy, and procedure edits, or introductions, needed to support this goal" requirements, How many documents (policies, procedures, etc.) need to be reviewed?

Please refer to question number 8.

70) How many external hosts are in scope for the testing (IP count)

Estimated 256 addresses, that have approx. 25% assigned

71) How many websites / applications are in scope for the external review

Roughly 8 publicly facing web applications for vulnerability enumeration.

72) Vendor always performs unauthenticated testing of apps, but will this include Authenticated testing or not

a) If authenticated, how many user levels will we test for each application

The County's primary interest is in unauthenticated testing.

b) How many pages for each app (static / dynamic)

Approx. 10

c) Are there web services in use with each application

Yes.

73) What language are the applications coded in

Primarily .net and C#.

74) Any third party or commercial applications included in scope. If so does the entity have permission to audit the application.

Nothing that isn't owned by the County will be tested.

75) Please confirm the expectations for the DLP solution.

See answer 67-F.

76) What additional details can the County provide about the single CTF system so the vendor can scope the effort of attacking that system?

It is a web facing application, which gives it the priority it has. The County will accept testing from the internal network, if that is more convenient for the vendor.

a) Will the vendor have to search for this system or will the County just point us at a black box and say go?

The County will point the vendor to the black box and say 'go'.

b) Are there any restrictions?

Restrictions will be primarily based on any actions that might affect availability of the black box system.

77) When will the testing be performed (business hours, afterhours, overnights, weekends)

Afterhours for technical testing of the Internet facing environment.

78) Please clarify the County's expectations on the physical security review of the MDF /IDF rooms being there is no social engineering, and confirm that the County is not expecting the vendor to gain access to the room.

There is not an expectation of the vendor gaining access to any IDF rooms. The physical security review is intended to produce recommendations such as; upgrades to the system to 'modernize' that infrastructure; process improvement for provisioning, and maintaining, physical access; etc…

79) How many internet (publicly) routable IPs are in scope for the external network/host penetration test?

Estimated 256 addresses, that have approx. 25% assigned

80) Do you have IDS/IPS in place? If so, does it actively deny/block suspected attacks?

Yes. And yes. This is one technology the County has prioritized to learn of any configuration gaps against industry best practices.

81) Do you have a Web Application Firewall in place?

Yes.

82) Do you have any other perimeter security controls in place that we should be aware of (i.e. white-listing, etc.)?

All information related to this question is covered throughout the document. Please review all questions and answers.

83) Please provide the list of external IPs that are in scope for testing.

The County has two full class C's of public addressing space to be tested, that will be provided during project kickoff.

84) What facilities in scope for wireless testing? (Sites by address)

See question 86.

85) Please provide address(es) for all facilities that are in scope for wireless testing.

Admin Building – 2300 Bloomdale Road, McKinney, TX 75070
Courthouse – 2100 Bloomdale Road, McKinney, TX 75070
Sheriff's Office - 4300 Community Ave. McKinney, TX 75071

86) How many Custom Web Applications are in the external network? *(Custom, bespoke, or highly modified code only – Commercial off the shelf, e.g., JD Edwards/ Business Objects or System Administration Interfaces, are not considered custom code.)*

8.

87) Do these applications require credentials or some type of personally identifying data to access application functionality?

No.

88) If yes above, how many different roles are supported by the application? Please identify the role and type of access achieved by an authenticated user of that role.

N/A

89) Will application testing be done in the production environment or in a test/staging environment? Application testing can be done in test/staging if the code instance in this environment is a duplicate of the code in production.

Primary testing will be done in the production environment.

90) Do you have an active Web Application Firewall (WAF) in place? If yes, you likely meet requirement 6.6. If no, we may be required to perform a credentialed application vulnerability scan of each application in scope.

As part of our layered security approach, yes we do have a WAF in place. **Exclusion rules can be put in place, to allow testing traffic through during the assessment**.

91) Please provide application information using the table in Appendix A below. Feel free to duplicate the table for each application in scope for testing.

There are an estimate 8 applications externally facing to tested.

92) Can all testing be performed during "normal" business hours (6am Eastern - 6pm Pacific Monday – Friday)?

No.

93) Number of Servers in scope:

Estimate 200.

94) Number of Network devices in scope:

Approximately 150 network devices.

95) Number of physical buildings in scope:

3 facilities, the Admin Building, Courthouse and Sheriff's Office.

a) List building site addresses:

See question 86.

96) Is the 6 months penetration testing required to validate vulnerabilities have been remediated?

No.

97) How many IT staff need to be interviewed?

15-20

98) Which server operating systems are within the scope of inventoried devices?

Windows for client/server OS's. Cisco network devices.

99) Number of applications in scope? (estimated)

Roughly 8 web applications.

100) Vendor assumes that remediation activities will be provided by the County and or others? Vendor can provide a remediation quote as part of the deliverables.

That is a correct assumption on remediation responsibility. The County would value, and consider, any quotes submitted for remediation.

101) Site address for the county data center?

See question 86.

102) Types of Network Firewalls by manufacture?

Cisco ASA.

103) How many (and or estimated) wireless access points are in scope as a part of the audit?

See question 34.