|  |  |  |
| --- | --- | --- |
|   | **COUNTY OF DANE**DEPARTMENT OF ADMINISTRATION**PURCHASING DIVISION**Room 425 City-County Building210 Martin Luther King Jr. Blvd.Madison, WI 53703-3345608/266-4131FAX 608/266-4425 TDD 608/266-4941 |  |
| CARLOS PABELLONDirector of Administration |  | CHARLES HICKLINController |

DATE: June 22, 2017

TO: All Proposers RFP #117060: Information Technology Security Assessment

FROM: Carolyn Clow, Purchasing Agent

SUBJECT: ADDENDUM #4

**The following responses are provided to questions received:**

|  |  |
| --- | --- |
| *Question #1* | *Is it possible to recuse ourselves from the remediation projects as it relates to the following Bid phrase?  In other words just do the assessment even though we have product partnerships?* |
|  |  |
| Answer #1 | No; the County wants this audit to be independent of any security vendor so the County is assured that when working with the security auditor they are recommending best of breed products and not just trying to sell the County a specific vendor’s products.  |
|  |  |
| *Question #2* | *Is the County of Dane interested in additional information on deliverables around privacy, current policy and procedures and current staff training on privacy and security?* |
|  |  |
| Answer #2 | Dane County will consider the above depending on the results of the Security Audit.  |
|  |  |
| *Question #3* | *Please reaffirm if Dane County is seeking external and internal network penetration testing as part of this RFP, or if automated scanning will satisfy the RFP. Addendum #1 indicated penetration testing is required, however the County’s response to Question #1 of Addendum #2 seems to indicate that penetration testing is not required, since the vendor stated their understanding was that the assessment would be performed using automated tools, and Dane County did not respond to clarify. Or, is the County assuming that scans will be conducted as part of the penetration test? Penetration testing doesn’t simply involve automated tools and there is a significant cost difference between scanning/pen testing.**For reference:**In Addendum #1, Dane County provided the following:**•             Original question: Is Dane County looking for a) an automated external and/or internal vulnerability scan followed up with a vulnerability assessment report of findings or b) a manual external and/or internal penetration test performed by an ethical hacker?**•             Dane County answer: Yes, penetration testing is required.**In Addendum #2, Dane County provided the following:**•             Original question (different vendor): For the vulnerability risk assessment (\*\*\*which from Amendment 1 we understand is essentially an assessment using tools such as automated vulnerability assessment tools\*\*\* (e.g.: Nessus) to perform discovery and identify system vulnerabilities can the County provide the following information to assist in scoping the work and level of effort needed to meet the County’s needs:**Do you want credentialed or non-credentialed scans, or some of each? Credentialed scans would require us to obtain an administrative-level user account and password for each different type of operating system and device.**•             Dane County answer: It is the County’s opinion that credentialed scans produce better results than non-credentialed scans. For the purpose of this RFP, assume all scans will be credentialed scans.* |
|  |  |
| Answer #3 | Penetration testing is required as this is a full audit. All scans should be conducted as part of penetration testing.  |
|  |  |
| *Question #4* | *Out of 100 applications how many will fall under black box testing and how many under grey box testing?* |
|  |  |
| Answer #4 | Grey Box testing will be sufficient for all applications tested.  |
|  |  |
| *Question #5* | *For Grey box application testing can rough size be provided- ( no. of pages in the application along with privilege levels?)* |
|  |  |
| Answer #5 | Yes. |

|  |  |
| --- | --- |
| *Question #6* | *Page 1, Section 1.1 Introduction “The County intends to conduct follow-up assessments in years 2-3 of the contract resulting from this RFP.”*1. *What is meant by years 2-3 of the contract?*
2. *Does the County expect any form of response to this intention?*
3. *If so, please indicate what expectations should be met in the response.*
 |
|  |  |
| Answer #6 | The amount of testing that is to occur in Years 2 and 3 will be determined by the results of the full year 1 audit. No response to years 2 and 3 is required with this RFP. Years 2 and 3 will be contracted independently of the full year 1 audit.  |
|  |  |
| *Question #7* | *Page 2 Section 1.2.2* *“6.Work with County staff to improve its incident detection and incident prevention processes based upon the results of these assessments”**Besides identifying potential weaknesses in incident management and recommending remediation, please enumerate what other expectations the County may have of the vendor regarding the objective (i.e., what does “work with County staff” mean beyond recommendations)* |
|  |  |
| Answer #7 | “Work with the county staff” includes making recommendations, answering questions, and helping set priority for dealing with the findings of the audit. It also includes working with the Dane County security team as the audit is conducted.  |
|  |  |
| *Question #8* | *Page 2 Section 1.2.2* *“Recommend improvement to support the County’s regulatory compliance requirements”**Can the County explain what regulations are to be included in this requirement? Later HIPAA and CJIS are identified. Besides these, are there other regulations that need to be considered? If so, please enumerate.* |
|  |  |
| Answer #8 | CJIS and HIPAA are the only regulations Dane County is concerned with for this audit. These are the only ones the County is required to comply with at this time. Dane County does not store any PCI data, but instead use a clearing house for PCI data.  |
|  |  |
| *Question #9* | *Page 2 Section 1.2.3 - Deliverables* *“A Security Risk Assessment Report that identifies threats to the County’s IT environment along with the threat source and business impact for each threat.”*1. *Can the County describe the range of threats beyond basic operational and environmental threats they expect the bidder to include in the assessment (e.g., should bidders include terrorism, pandemics, geopolitical activism, etc.)?*
2. *Does the County have an existing threat profile they would like the bidder to incorporate into the assessment?*
 |
|  |  |
| Answer #9 | 1. Dane County is looking for the identification of threats that include potential loss of data or operational capacity. If that is what is meant by basic operation, then that is what is desired by the County.
2. No.
 |
|  |  |
| *Question #10* | *Page 3 Section 1.2.5**“Information that is more detailed will be supplied at time of contract.”**Can the County confirm the security environment included in the Security Assessment is limited to the 8 platforms identified, or if not, can the County identify any other platforms, services and assets to be included in the Security Assessment?* |
|  |  |
| Answer #10 | This assessment will be limited to the platform identified.  |
|  |  |
| *Question #11* | *Page 3 Section 1.2.5**“Information that is more detailed will be supplied at time of contract.”*1. *Does the County formally maintain procedure documentation that will enable a reviewer to determine what information security controls are in place?*
2. *If not, will these controls have to be extracted through interviews with County IT personnel?*
3. *Has the County formally documented the “desired levels of security” referenced in the definition statement?*
4. *To determine if controls are “correctly operating as intended”, does the county mean operating “effectiveness” (i.e. sampling) or simple validation that controls are “in place”? If sampling is required, what is the approximate number of controls to be tested?*
5. *Are past reports of the security assessment available for review?*
6. *Is the County IT security program aligned with any recognized security framework (e.g., ISO/IEC 27001/2, NIST CSF, COBIT, other)? If so, can you identify it?*
7. *Can the county clarify the intent of the security assessment by explaining the difference between Section 1.2.3 that describes a Security Risk Assessment Report that asks bidders to identify threats and treatments, and the definition in Section 1.3 that asks bidders to perform a controls assessment?*
 |
|  |  |
| Answer #11 | a. Partial documentation is available.b. Documentation is incomplete so interviews will be needed. c. No.d. The County wants to make sure that it’s controls are operating effectively.e. Yes (2009).f. Not at this time. g. Section 1.3 is asking that the vendor evaluate the County’s current security controls to see where they can be improved. A risk assessment will involve more than just security controls.  |
|  |  |
| *Question #12* | *Page 3 Section 1.3 Definitions “Vulnerability Assessment: A vulnerability assessment is conducted to determine the weaknesses inherent in the information systems that could be exploited leading to information system breaches or malicious activity.”*1. *Please list the number of externally facing web applications that are in scope of vulnerability testing.*
2. *Does Dane County require proof of exploits or simply a report from scanning tools?*
 |
|  |  |
| Answer #12 | a. 100 b. A report from a scanning tool would be fine, to start with, additional proof may be required given the vulnerability uncovered.  |
|  |  |
| *Question #13* | *Page 3 Section 1.3 Definitions* *“A Physical Risk Assessment Report that identifies risk of physical harm or sabotage to the County’s IT environment, including but not limited to: Network Closets, Server Rooms, and Work Areas. The report should include the facility and location (room number) where the risk is located, information that will help evaluate whether the risk shall be accepted, avoided, transferred or mitigated, and recommendations on how to mitigate the risk identified..”*1. *Please indicate the approximate square footage of the facilities that are in scope.*
2. *Will the assessor be provided and escort within these facilities (for efficiency in finding the in scope “network closets, etc.)?*
3. *DO these facilities have “external entry” security measure (such as guards, security desks, key cards/pads) to gain physical access to the buildings? Is external access and egress in scope? If so, how many?*
 |
|  |  |
| Answer #13 | a. The square footage cannot be determined at this time. b. Yes.c. Yes; some of them require secured access and badging in some cases. External egress testing of the buildings themselves is not in the scope of this RFP; however, access to IT equipment within the facilities is.  |
|  |  |
| *Question #13* | *Page 10 Section 4.5.2**What form of proof or validation does the County require to demonstrate that the assessor is vendor agnostic?* |
|  |  |
| Answer #13 | Section 4.5 requires that the proposer provide narrative detailing how each section will be complied with. This narrative will demonstrate that the assessor is vendor agnostic.  |
|  |  |
| *Question #14* | ***OS****What version of Windows Server is in use?   (Is the State Using Group Policy)**What Version of Linux is used (RED HAT, SUSE etc.)?**Are there any devices using iOS?**How many Virtual Machines are in use?* |
|  |  |
| Answer #14 | 1. Windows Server 2012 and 2016. Group policy is used.
2. Linux Red Hat.
3. a small subset of IOS devices are in use.
4. Approximately 350 VM guests run under VMware.
 |
|  |  |
| *Question #15* | ***Desktop****Does the County used a standard build for Windows and Mac devices, if any?* |
|  |  |
| Answer #15 | Yes. |
|  |  |
| *Question #16* | ***Remote Access*** *Are employees permitted to bring their own devices?**Which MDM software is used to support BYOD?**Are County employees or vendors permitted to work remotely? Is WYSE used to facilitate this?**Does the County WYSE Terminals have a specific security/risk policy with the provider?*             |
|  |  |
| Answer #16 | 1. No
2. N/A
3. Yes; No
 |
|  |  |
| *Question #17* | ***Network Infrastructure****What type of firewalls, routers and switches are deployed?**Do all https sites, at a minimum, use SHA-2 encryption?**Does the County use any open source software?  Is there an inventory of every instance and version?* *Does the County employ a SIEM?**Does the County utilize any cloud IaaS?**What is the Dell Server Environment (Memory/HD/Size/Raid etc.)?**What version of Dell Switches (Are they managed)**What standard Antivirus software has the County deployed?**Which firewalls are used by the County?**How many Server Environments (Domains) does the County utilize?* |
|  |  |
| Answer #17 | a. This will be provided to the winning vendor, an RFP is not the appropriate form to reveal this information. b. Yesc. Yes; Dane County has a software inventory system d. SIEM is not fully implemented at this time. Depending on results of this assessment Dane County will proceed with a full implementation. e. Nof. Various Dell servers are utilized. g. This will be provided to the winning vendor, an RFP is not the appropriate form to reveal this information. h. This will be provided to the winning vendor, an RFP is not the appropriate form to reveal this information. i. This will be provided to the winning vendor, an RFP is not the appropriate form to reveal this information. j. One. |
|  |  |
| *Question #18* | ***Applications****Does the County develop applications in house? Which coding standard, if any, is followed?**Is the County using Web Applications or any cloud PaaS?* |
|  |  |
| Answer #18 | a. Yes; No coding standards are in use. b. Yes; very limited at this time.  |
|  |  |
| *Question #19* | ***Personal Data****Does the County collect, process, share personal data of non-US Citizens?  If so, from which countries?**Is there a privacy policy associated with the aforementioned data collection?**Other than health information, what other PII collected?* *Do any of the u businesses collect PCI data?  Can we get access to your report of compliance?* |
|  |  |
| Answer #19 | a. Yes.b. CJISc. no; Dane County uses a PCI clearing house. d. N/A |
|  |  |
| *Question #20* | ***Vendor Management****Is the winner of the bid expected to evaluate the security of any of the vendors?*  |
|  |  |
| Answer #20 | Yes. |
|  |  |
| *Question #21* | ***Operations****Are the businesses risked ranked?**Does the County maintain data flow diagrams that show all data collection touchpoints (phone in, hard copy application, website, mobile devices) and connections with vendors or other third parties?**Does the County have an incident management process?  Does it include steps to determine if incidents rise to the level of a breach under state breach notification laws?* *Does the County currently perform table top exercises for large scale incidents?**Does the Country have a data classification schedule and access controls designed around it?* *Does the County have a DR Site?  Hot/warm/cold?**Is this site in scope for this RFP?* |
|  |  |
| Answer #21 | a. Nob. Some documentation exists but is not completec. Nod. Noe. Nof. Yesg. No; but could be included in years 2 and 3 under separate contract.  |
|  |  |
| *Question #22* | ***Other****What project deadlines do you have?* *Are there crucial milestones that the vendors should be aware of?* *Is the County comfortable with vendors providing a different timeline?**Which email systems/platform is used the County?* |
|  |  |
| Answer #22 | a. It is expected that the audit will be completed within one year of a signed contract. b. Noc. Yesd. Microsoft Outlook |
|  |  |
| *Question #23* | *Out of 100 applications, how many will fall under black box testing and how many under grey box testing?*  |
|  |  |
| Answer #23 | Grey Box testing will be sufficient for all applications tested. |
|  |  |
| *Question #24* | *For Grey box application testing can rough size be provided- ( no. of pages in the application along with privilege levels?)* |
|  |  |
| Answer #24 | Yes. |
|  |  |
| *Question #25* | *Is the County of Dane interested in additional information on deliverables around privacy, current policy and procedures and current staff training on privacy and security?* |
|  |  |
| Answer #25 | Maybe; depending on the results of the assessment.  |
|  |  |
| *Question #26* | *Are the 100 web applications to be tested with or without authentication?* |
|  |  |
| Answer #26 | Without authentication. |
|  |  |
| *Question #27* | *Are the 30 Work Stations to be tested part of the 500 internal IPs?* |
|  |  |
| Answer #27 | Yes. |
|  |  |
| *Question #28* | *Are the 50 wireless access points within the 6 locations that are to be tested?* |
|  |  |
| Answer #28 | Yes. |
|  |  |
| *Question #29* | *When was their last vulnerability assessment?* |
|  |  |
| Answer #29 | 2009. |
|  |  |
| *Question #30* | *When was their last pen test?* |
|  |  |
| Answer #30 | 2009.  |
|  |  |
| *Question #31* | *Is a phishing exercise part of the vulnerability assessment?* |
|  |  |
| Answer #31 | Yes.  |
|  |  |
| *Question #32* | *As part of the physical security assessment are we required to gain access to the facilities by using such technique as tail gating etc.* |
|  |  |
| Answer #32 | A specific technique is not required. Whatever you use to determine the security of our facilities is fine.  |
|  |  |
| *Question #33* | *Regarding the 100 web applications in scope for penetration testing, how many****user roles and how many dynamic pages****for each application must be covered?* |
|  |  |
| Answer #33 | Dane County has a small amount of dynamic pages and user role use is limited.  |
|  |  |
| Question #34 | *Regarding section 7.3, Local Purchasing Ordinance, can****vendors outside of the state****participate?* |
|  |  |
| Answer #34 | Yes, vendors outside of the state can participate. |
|  |  |
| *Question #35* | *Regarding regulations, can you confirm that****HIPAA and CJIS****are the only relevant regulations for this assessment?* |
|  |  |
| Answer #35 | CJIS and HIPAA are the only regulations Dane County is concerned with for this audit. These are the only ones the County is required to comply with at this time. Dane County does not store any PCI data, but instead use a clearing house for PCI data. |
|  |  |
| *Question #36* | *What is the ideal****start/end date****for the engagement to occur?* |
|  |  |
| Answer #36 | To be determined during contract negotiations. Must be completed within 1 year of a signed contract.  |
|  |  |
| *Question #37* | *Will Dane County pay for****travel expenses****or should the vendor include those costs in the estimate?* |
|  |  |
| Answer #37 | Include travel costs in the cost proposal. No additional travel costs will be paid. |
|  |  |
| *Question #38* | *300 is the total number of applications. Among these, approximately 100 of**them are web applications. For the purpose of this RFP assume that all 100 web**applications will be tested. –* *-          How many unique dynamic web pages are in each application?**-          Would you be looking for a vulnerability scan on the applications or an actual pen-test on each of the 100 applications?* |
|  |  |
| Answer #38 | 1. We have a small amount of dynamic pages
2. Pen-test may be limited to the website only
 |
|  |  |
| *Question #39* | *On Page 1, you say that the respondents shall not outsource any of the project work to a security vendor.    Do you mean specifically security products vendor?    Is it permitted to outsource any of the project work to a security consultant who is also security product agnostic?* |
|  |  |
| Answer #39 | Yes.  |
|  |  |
| *Question #40* | *Please provide the number of IP addresses for internal vulnerability assessment and number of IP addresses for external vulnerability assessment.* |
|  |  |
| Answer #40 | 1. We support approximately 100 external facing IP addresses. For the proposes of this RFP assume all of these will be tested. Internally assume a minimum of 300 IP addresses will be tested.  |
|  |  |
| *Question #41* | *On Page 3, you mention a total number of business units (35) and number of facilities (26).     Does this mean that there are 26 different sites/ locations which would need to be visited for the purpose of doing this assessment?* |
|  |  |
| Answer #41 | No; a maximum of 8 facilities will need to be visited, all within the geographic boundaries of Dane County. |
|  |  |
| *Question #42* | *How many sites or locations are in scope for the physical security assessment?* |
|  |  |
| Answer #42 | A maximum of 8 facilities will need to be visited, all within the geographic boundaries of Dane County.  |
|  |  |
| *Question #43* | *How many sites/ business units/ locations are in scope for HIPAA and CJIS compliance?* |
|  |  |
| Answer #43 | (3) HIPAA (1 ) CJIS |
|  |  |
| *Question #44* | *Has Dane County undergone a security risk assessment, vulnerability risk assessment and physical risk assessment before?* |
|  |  |
| Answer #44 | Yes (2009) |
|  |  |
| *Question #45* | *Has Dane County performed any compliance efforts for HIPAA and CJIS before?* |
|  |  |
| Answer #45 | Yes |
|  |  |
| *Question #46* | *How many systems store electronic protected health information?   Please provide system names if possible.* |
|  |  |
| Answer #46 | Approximately 3.  |
|  |  |
| *Question #47* | *Is there any preference provided to certified businesses, e.g. Minority-owned, Woman-owned, etc.?* |
|  |  |
| Answer #47 | No. |
|  |  |
| *Question #48* | *On Page 5, it says that the contract start date is September 1, 2018.    Please confirm – is this is a typo – is this date meant to be September 1, 2017.* |
|  |  |
| Answer #48 | This is negotiable , depending on the winning vendors availability. |
|  |  |
| *Question #49* | *What is the county’s timeline to finish the entire assessment?* |
|  |  |
| Answer #49 | Within one year of a signed contract.  |
|  |  |
| *Question #50* | *Is HIPAA and CJIS the only “regulatory” compliance laws/mandates that the County is required to comply with?* |
|  |  |
| Answer #50 | CJIS and HIPAA are the only regulations Dane County is concerned with for this audit. These are the only ones the County is required to comply with at this time. Dane County does not store any PCI data, but instead use a clearing house for PCI data. |
|  |  |
| *Question #51* | *Is the County currently HIPAA Security Rule compliance?* |
|  |  |
| Answer #51 | Yes; with some exceptions |
|  |  |
| *Question #52* | *Is the County currently CJIS compliant?* |
|  |  |
| Answer #52 | Yes. |
|  |  |
| *Question #53* | *Is this security risk assessment acting as the annual HIPAA security risk assessment and annual CJIS security risk assessment?* |
|  |  |
| Answer #53 | No. |
|  |  |
| *Question #54* | *Is the scope of this RFP to include risks associated with non-Compliance (HIPAA, CJIS, PCI, State Privacy Laws, etc.)?* |
|  |  |
| Answer #54 | Yes. |
|  |  |
| *Question #55* | *Does the County have a preference for risk assessment methodology or approach?  NIST, ISO, OCTAVE, Hybrid?* |
|  |  |
| Answer #55 | No. |
|  |  |
| *Question #56* | *Can security testing (vulnerability assessment scanning) be conducted during normal business hours?  If not – please specify time windows.* |
|  |  |
| Answer #56 | Most penetration testing can be conducted during normal business hours |
|  |  |
| *Question #57* | *Can penetration testing be conducted during normal business hours or must this be done after-hours?  Please specify time windows.* |
|  |  |
| Answer #57 | Most security testing can be conducted during normal business hours |
|  |  |
| *Question #58* | *Can you provide a list of existing IT and IT security policies & procedures?  Just the list not the actual document.* |
|  |  |
| Answer #58 | No.  |
|  |  |
| *Question #59* | *Does the County have a pre-existing data classification policy or standard?*  |
|  |  |
| Answer #59 | No. |
|  |  |
| *Question #60* | *For the 6 chosen business units, will all facilities under those 6 business units, require onsite inspection and assessment? If so, how many out of the 26 facilities are under those business units, are included and what are the square feet?* |
|  |  |
| Answer #60 | 8 business units, Square feet is not available at this time.  |
|  |  |
| *Question #61* | *Do you have existing policies and procedures for management of the physical security, all systems including CCTV, Access Control, Key Entry, etc.?* |
|  |  |
| Answer #61 | Yes  |
|  |  |
| *Question #62* | *On the physical risk assessment report, do you wish it to include risk to generators, power systems and cooling serving the IT environment?* |
|  |  |
| Answer #62 | No.  |
|  |  |

Please acknowledge receipt of this addendum by noting “Addendum #4 Received” on the bottom of the Signature Affidavit when you submit your bid. If you have any questions regarding this addendum, please contact me at 608-266-4966.

Sincerely,

Carolyn A. Clow, CPPB

Purchasing Agent