|  |  |  |
| --- | --- | --- |
| ETF_logo_large | STATE OF WISCONSIN **Department of Employee Trust Funds**  **Robert J. Conlin**  SECRETARY | 801 W Badger Road  PO Box 7931  Madison WI 53707-7931  1-877-533-5020 (toll free)  Fax (608) 267-4549  http://etf.wi.gov |

Date: July 18, 2019

To: All Potential Proposers to RFP ETI0049

RE: **ADDENDUM No. 2**

**Request for Proposal (RFP) ETI0049**

**IT Audits and Consulting**

**Acknowledgement of receipt of this Addendum No. 2:**

**Proposers must acknowledge receipt of this Addendum No. 2 by providing the required information in the box below and including this Page 1 in Tab 1 of their Proposal.**

|  |  |
| --- | --- |
|  |  |
| Proposer’s Company Name: |  |
|  |  |
| Authorized Person (Printed Name and Title): |  |
|  |  |
| Authorized Person’s Signature: |  |
|  | Date |

**Please note the following updates to RFP ETI0049:**

1. **ADD** the following bullet to Page 12 of the RFP, Section 2.4, to the right of TAB 1, General Information and Forms, directly proceeding “Provide the following in the following order:”

* Page 1 of ADDENDUM No. 2: Completed and signed Page 1 of Addendum No. 2.

2. **ADD** the following questions regarding RFP ETI0049 from Proposers and answers from the Department to the RFP:

**Request for Proposals (RFP) ETI0049 – IT Audits and Consulting**

**Vendor Q&A**

| **Q#** | RFP Document | **Page #** | **Question** |
| --- | --- | --- | --- |
| **Q1** | Appendix 2 A 2 | 2 | What are the number of systems and Applications that are in scope for vulnerability assessment? |
| **A1** |  |  | Appendix 2, A.2, covers Network Security Assessment, and application review is out of scope for this service. |
| **Q2** | Appendix 2 – 1.0.B.II | 2 | How many sites are to be physically socially engineered? How many users are to be electronically socially engineered? |
| **A2** |  |  | One, the Department headquarters. |
| **Q3** | Appendix 2 – 1.0.B.VII | 3 | How many interfaces are to be evaluated? |
| **A3** |  |  | For Appendix 2 – 1.0.B.VII: A sampling of 4 “interfaces” (data exchanges between systems) will be evaluated. |
| **Q4** | Appendix 2 - 2.1 | 5 | Is the timeframe flexible in terms of a start date to actually begin the work? |
| **A4** |  |  | Yes, however there are 3 audits and 3 consulting engagements targeted for completion by 6/30/2020 so the Department is anxious to begin work as soon as possible once a Contract is executed. |
| **Q5** | N/A | N/A | What does the Agency have budgeted for this project? |
| **A5** |  |  | The Department chooses not to answer this question. |
| **Q6** | 2.4.1 Format Requirements  Tab 3 |  | In accord with 2.4.1 Formal Requirements, Tab 3, would you please provide the RFP (RFP/Appendix/Form and Department Terms and Conditions) in Word format so that we may we make redline exceptions via Track Changes to the terms and conditions with the submittal of our proposal?  As stated in the requirements, “…the Proposer must make its specific required revision to the language of the provision by striking out words or inserting required language to the text of the provision.  Any new text and deletions of original text must be clearly color coded or highlighted, which requires the Proposer’s response be printed in color.”  This cannot be done to a pdf document format as is currently provided and any conversion process may cause unintended changes or typographical errors. |
| **A6** |  |  | The Word versions of the RFP document and Appendices 1-3 have been posted on the Department’s extranet site, which is referenced in the RFP. |
| **Q7** | 9 Contract Terms and Conditions |  | With our proposal submittal, may we disclaim to terms and conditions of an existing contract which the State of Wisconsin is eligible to use? |
| **A7** |  |  | No. |
| **Q8** | Appendix 2  Section 2.2.D |  | As our engagements are staffed on a first come first served basis, a specific resource may not be available. We have a policy of not naming our resources. Would it be acceptable to provide a list of titles and roles as well as a number of available resources? |
| **A8** |  |  | This approach is reasonable, although additional detail is appreciated, such as a brief explanation of what the titles and roles entail. |
| **Q9** | 1.9 Calendar of Events | 8 of 50 | Would the Department grant a two-week extension to allow Vendors sufficient time to prepare and submit proposal responses after release of Proposer Questions? |
| **A9** |  |  | No. The Department has granted an extension to July 29, 2019. |
| **Q10** | Q1 1.9 Page 8 |  | We respectfully request a one-week extension, with a due  date on July 31. We feel we can provide a detailed response  with this additional time. |
| **A10** |  |  | No. The Department has granted an extension to July 29, 2019. |
| **Q11** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | 1. What is the current imaging, endpoint management and patching solution? SCCM, Kace, etc..? |
| **A11** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q12** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | What OS platforms are in use? |
| **A12** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q13** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | Laptop/desktop models for which you want to create image? |
| **A13** |  |  | The Department uses devices from two vendors (7 models supported). |
| **Q14** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | Are all endpoints on corporate network or internet-based endpoints will be part of scope as well? |
| **A14** |  |  | Yes. |
| **Q15** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | Are you planning to evaluate new (Microsoft) methodologies around imaging as part of this initiative or this will be limited to evaluating the current processes? In other words, are you looking for recommendations for new better solutions? |
| **A15** |  |  | Yes. |
| **Q16** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | What applications are typically added as part of imaging? |
| **A16** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q17** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | Any large size application that you would be deploying? |
| **A17** |  |  | Yes, additional information will be provided to the selected vendor under a non-disclosure agreement. |
| **Q18** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | Are the machines using BIOS or UEFI? |
| **A18** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q19** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | Do you have PKI infrastructure? |
| **A19** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q20** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | Do the NICs support WOL (Wake On Lan)? |
| **A20** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q21** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | What is the AV solution you are using? |
| **A21** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q22** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | How many AD sites? what is the replication frequency between sites? |
| **A22** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q23** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | Do you already have SQL DB for solutions like SCCM? If so which version? |
| **A23** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q24** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | How many users connect remotely? |
| **A24** |  |  | All users have VPN access for remote connectivity. |
| **Q25** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | What is the bandwidth between sites? |
| **A25** |  |  | The Department has one office location (headquarters) and one data center, bandwidth between the two is 40GB. |
| **Q26** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | What are the overall expectations for the ultimate goal of consulting around imaging processes?   1. Keep existing and improve the process 2. Replace existing and improve the process 3. Other? |
| **A26** |  |  | The Department is open to option 1 or option 2 based on vendor recommendation following evaluation of current process. |
| **Q27** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | Please describe your mains goals and objectives with this engagement? |
| **A27** |  |  | The Department is looking for the selected vendor to evaluate all elements of the Department’s IT Disaster Recovery program, including: supporting planning documentation, governance, roles and responsibilities, testing, training, and evaluating how these elements support the overall objective of system resiliency in support of key business operations. |
| **Q28** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | How many data centers and locations are in scope for this engagement? |
| **A28** |  |  | The Department has one headquarters location, one data center location, and one location for DR**.** |
| **Q29** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | How are the sites connected? What type of connection? |
| **A29** |  |  | The Department has one headquarters location, one data center location, and one location for DR. There is a 40GB connection between the headquarters and data center locations. |
| **Q30** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | What type of DR solution do you have today? |
| **A30** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q31** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | What type of Backup solution do you have today? |
| **A31** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q32** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | What is your RTO and RPO requirements? Please describe. |
| **A32** |  |  | This information is documented, and RTOs vary by system. This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q33** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | Are you running HyperV or VMware in your environment? Which versions? |
| **A33** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q34** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | What type of security compliances do you need to meet? |
| **A34** |  |  | The Department is required to safeguard information in electronic form under the HIPAA Security Rule, 45 CFR Part 160, and Subparts A and C of Part 164.  At the state level there is a general requirement for information security. The Department is required by 40.07, Wisconsin Statutes, to prevent personal information from being disclosed except as provided under the statute. |
| **Q35** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | Do you require HIPS / IDS / Monitoring / Reporting on suspicious activity? |
| **A35** |  |  | Yes. |
| **Q36** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | What type of firewalls do you have today? |
| **A36** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q37** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | Are there any applications installed on your VMs that are home grown? |
| **A37** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q38** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | Do you have resources maintaining them, keep the code up-to-date and etc? |
| **A38** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q39** | B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):  IV. Business Continuity/Disaster Recovery Audit | 27 | How much storage is currently required for your VMs? |
| **A39** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q40** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  II. Data Loss Prevention Review  III. Data Privacy Review | 28 | What type of data repositories are in use today? |
| **A40** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q41** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  II. Data Loss Prevention Review  III. Data Privacy Review |  | Can the organization generally identify all locations where sensitive data is stored across the enterprise, including on internal servers or cloud storage, as well as those hosted by any third-party providers? |
| **A41** |  |  | Yes, the Department has this capability. |
| **Q42** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  II. Data Loss Prevention Review  III. Data Privacy Review |  | Can the organization categorize the types of data it uses? |
| **A42** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q43** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  II. Data Loss Prevention Review  III. Data Privacy Review |  | Do you have a data governance program? |
| **A43** |  |  | Yes. |
| **Q44** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  II. Data Loss Prevention Review  III. Data Privacy Review |  | Is the organization planning how to develop its technology, products, processes, and organizational structure with data protection and privacy as key components, and is it aware of the gaps for doing so? |
| **A44** |  |  | Yes. |
| **Q45** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  II. Data Loss Prevention Review  III. Data Privacy Review |  | Is the organization aware of technologies to encrypt personal data and has it encrypted some data, such as government identification numbers, birthdates, or banking numbers etc? |
| **A45** |  |  | Yes. |
| **Q46** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  II. Data Loss Prevention Review  III. Data Privacy Review |  | Is the organization aware of data loss prevention technologies to prevent data leakage and what DLP solution is currently in place? |
| **A46** |  |  | Yes, the Department is aware of DLP, how this is being used is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q47** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  II. Data Loss Prevention Review  III. Data Privacy Review |  | Does the organization have an ongoing effort to identify needed people, process, and technology controls to protect the confidentiality, integrity, and availability of data? |
| **A47** |  |  | Yes. |
| **Q48** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review | 28 | If AD is in place, please describe your AD configuration.  . |
| **A48** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q49** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | Account structure/office structure. How is AD structure mapped to HR? |
| **A49** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q50** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | How are admin rights assigned in AD? |
| **A50** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q51** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | Do any Application feed off AD data? |
| **A51** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q52** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | How are you DCs/DNS distributed? Are your DCs 2012? Can they handle replication traffic? |
| **A52** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q53** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | What is your network structure? |
| **A53** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q54** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | Do you have special rules for white glove users (Execs)? |
| **A54** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q55** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | How do you manage your Security Groups and Distribution Groups? |
| **A55** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q56** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | Do you have dynamic groups? |
| **A56** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q57** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | Is it self-service managed groups or via SD only? |
| **A57** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q58** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | Can you describe your identity lifecycle management? |
| **A58** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q59** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  IV. Identity Access Management (IAM) Review |  | What are the main IdM solutions: Oracle Identity, AD, MIM, Azure AD, Okta Identity etc. please provide as much information as possible. |
| **A59** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q60** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  V. eDiscovery Program Review | 28-29 | What solutions are currently being used for eDiscovery purposes?  Are you looking to keep existing solution or replace with another solution? |
| **A60** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q61** | D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:  VI. Records Management Review | 28-29 | What solutions are currently being used for Records Management?  Are you looking to keep existing solutions or replace with new solutions? |
| **A61** |  |  | The Department has invested in a knowledge base and follows state records management (Records Disposition Authorization/RDA) guidelines for records disposal. |
| **Q62** | C. Non-audit consulting, advisory and review services in FY20:  I. Systems Development Lifecycle (SDLC) Review | 28 | What SDLC methodology is currently being used? |
| **A62** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q63** | C. Non-audit consulting, advisory and review services in FY20:  I. Systems Development Lifecycle (SDLC) Review | 28 | What technology stack is the company currently on? |
| **A63** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q64** | C. Non-audit consulting, advisory and review services in FY20:  I. Systems Development Lifecycle (SDLC) Review | 28 | What are some of the current pain points of the process? |
| **A64** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q65** | C. Non-audit consulting, advisory and review services in FY20:  I. Systems Development Lifecycle (SDLC) Review | 28 | Is the their currently a role (or roles) in place to manage the SDLC?  Or is it process only? |
| **A65** |  |  | The Department has a SDLC process in place, details are confidential, and the Department will provide this information to the selected vendor under a non-disclosure agreement. |
| **Q66** | C. Non-audit consulting, advisory and review services in FY20:  I. Systems Development Lifecycle (SDLC) Review | 28 | What measures are currently in place to enforce the processes and rules?? |
| **A66** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q67** | C. Non-audit consulting, advisory and review services in FY20:  III. Data Management Review | 28 | Where/how is the data stored? |
| **A67** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q68** | C. Non-audit consulting, advisory and review services in FY20:  III. Data Management Review | 28 | How large is the data set? |
| **A68** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q69** | C. Non-audit consulting, advisory and review services in FY20:  III. Data Management Review | 28 | What is the backup/disaster recovery for the data storage? |
| **A69** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q70** | C. Non-audit consulting, advisory and review services in FY20:  III. Data Management Review | 28 | How is the data entered and accessed? Are there custom applications or interfaces? |
| **A70** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q71** | C. Non-audit consulting, advisory and review services in FY20:  III. Data Management Review | 28 | What is the current process for requesting access to data? |
| **A71** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q72** | Appendix 3, Department Terms and Conditions, 6.1 SOC 1/Type 2 Report | 34-35 | If our company is not SOC or SSAE certified, what type of reports can be provided in lieu of the SOC 1, SOC 2, and SSAE reports referenced in these sections? |
| **A72** |  |  | In absence of SOC or SSAE, provide your Information Security Plan, Business Continuity/Disaster Recovery Plan, etc. to help the Department assess. If these document are confidential, include them on Form G – Designation of Confidential and Proprietary Information |
| **Q73** | Appendix 3, Department Terms and Conditions, 12.0 LIQUIDATED DAMAGES: | 36 | Per company policy, we do not accept any contract that includes “liquidated damages,” but will rather provide a “performance bond” for up to 100% of the value of the engagement, at client expense.  Is this acceptable? |
| **A73** |  |  | The Department will not accept assumptions, exceptions, or changes to the items listed in ***RFP Table 4. No Assumptions or Exceptions Allowed.*** Per Section 2.4.2 Supplemental Information – IMPORTANT, no assumptions or exceptions to the Appendix 3 Sections listed in Table 4 are allowed. |
| **Q74** | Appendix 3, Department Terms and Conditions, 18.0 REMEDIES OF THE DEPARTMENT | 38 | Per company policy, we will not accept liability for any costs incurred by a client working with “other sources.”  Thus, the last sentence in that section would need to be deleted. Is this acceptable? |
| **A74** |  |  | The term “other sources” in that section refers to Contractor’s work with other sources to complete the services, not the Department using other sources. Contractor will be responsible for completing all services even if Contractor used other sources to complete the work. |
| **Q75** |  |  | Must the bidding company fulfill products and services in their entirety to be considered in the award? |
| **A75** |  |  | The Department is seeking a single firm to execute the entire body of work outlined in the RFP. |
| **Q76** |  |  | Will the NASPO or MHEC contracts be utilized for procurement? |
| **A76** |  |  | No. |
| **Q77** |  |  | Will ETF be open to financing options provided by the bidding vendor? |
| **A77** |  |  | No. |
| **Q78** | -- | -- | Will the selected vendor be allowed to provide other implementation services? |
| **A78** |  |  | The services are described in the RFP. No other services will be contracted. |
| **Q79** | 1.0 Services and Deliverables Required | 27 | Does the selected vendor need to provide assurance for the audit services? |
| **A79** |  |  | Yes, if an engagement is identified as an audit service, performance of the engagement is required to meet relevant auditing standards to provide assurance. |
| **Q80** | 1.0 Services and Deliverables Required | 27 | What is the sample size of application for “IT Controls” assessment? |
| **A80** |  |  | For IT General Controls: a sampling of 3-6 applications will be in scope. |
| **Q81** | 1.0 Services and Deliverables Required | 28 | What is an estimated number of interfaces to be included in the assessment? Is data sharing agreement review part of documentation that needs to be reviewed? |
| **A81** |  |  | For Appendix 2 – 1.0.B.VII: A sampling of 4 “interfaces” (data exchanges between systems) will be evaluated. The Department may request the Contractor to review one or two of the Department’s data sharing agreements. |
| **Q82** | 1.0 Services and Deliverables Required | 29-30 | Are they any regulatory requirement that ETF needs to comply with for data management and data privacy perspective? |
| **A82** |  |  | The Department is subject to the Privacy and Security Rules of the federal Health Insurance Portability and Accountability Act (HIPAA), as amended by the HITECH Act, due to the self-funded components of the State Group Health Insurance Plan that are administered by the Department. See 45 CFR Parts 160, 162 & 164.  At the State level, the Department is governed by the Department records confidentiality provisions in Chapter 40, Wisconsin Statutes. Chapter 40 specifically pertains to the Department. Section 40.07 states that Individual Personal Information in the records of the department is not a public record and shall not be disclosed except as provided in the section. In addition, the Department is subject to Wisconsin statute section 134.98, which requires certain notices for unauthorized acquisition of personal information.  As a public agency, the Department must comply with public records laws in Chapter 19, Wisconsin Statutes, which contain privacy provisions. |
| **Q83** | 1.0 Services and Deliverables Required | 28 | Are there multiple legacy application replacement activities? Is the scope of the review limited to project management or any technical review is required? |
| **A83** |  |  | The focus of this consultation is on the general project management principles and processes being used to carry forward our legacy application replacement activity. A technology review is not in scope. |
| **Q84** | 8.0 Cost Proposal | 20 | Does the cost proposal only cover for FY20 work? |
| **A84** |  |  | Yes. |
| **Q85** | 2.4.1 | 12 | Are actual index tabs required to be placed in hard copies (both original and those marked as copy) of our proposal? |
| **A85** |  |  | Yes, however, they don’t need to be labeled. |
| **Q86** | 9.2, 1st Bullet | 21 | May we request progress payments? |
| **A86** |  |  | A payment schedule will be developed during negotiations between the Department and the selected vendor and included in the executed Contract. |
| **Q87** | Appendix 1, Item 1.3 | 2 | We are a privately held corporation and do not release detailed financial statements. In lieu of financial statements will you accept a Supplier Qualifier Report from Dun and Bradstreet? |
| **A87** |  |  | Proposer’s current audited financial statements are preferred. If the Proposer does not have audited financial statements, or absolutely cannot provide them, the Proposer should provide current financial information it provides to other entities that will enable the Department to assess the Proposer’s financial soundness, such as what is provided to creditors/investors when raising funds. A D&B Supplier Qualifier Report is acceptable. |
| **Q88** | 1.1 Introduction | 3 | The RFP includes distinct workstreams. Can Cost Proposals vary based on services listed within the RFP’s Introduction bullet points, or would alternative price points result in disqualification? |
| **A88** |  |  | The Department understands Proposals may vary based on services requested and anticipates a range of price points within each Proposal based on the skillset(s) needed to complete the work. In addition to the information and rates required to be entered in Tab 1 of the Cost Proposal Workbook, you may provide other information in Tab 2 of the Cost Proposal. All cost information must be included only in the Cost Proposal. |
| **Q89** | 1.2 ETF Overview | 3 | Will the OIA be responsible for final review of any deliverables, or will the Proposer be responsible for submission of final deliverables? |
| **A89** |  |  | The Proposer is responsible for submission of final deliverables, which will be formally reviewed for acceptance by the Department’s Office of Internal Audit. |
| **Q90** | 1.10 Contract Term, Statements of Work, Rate Increases | 8 | Are estimates at this point only intended to cover the initial term (FY20 and FY21) and not any additional one-year period? |
| **A90** |  |  | Yes. |
| **Q91** | N/A | N/A | What is the current state of intelligent automation / RPA within OIA? Has an opportunity assessment been conducted to evaluate the value of RPA implementation? If yes, can a summary of this assessment be provided? |
| **A91** |  |  | The OIA does not have RPA. |
| **Q92** | Form H – Cost proposal setup | p.5(RFP)  p.1(Form H) | Page 5 of the RFP shows that the initial term is FY20 and FY21 but the cost proposal shows only FY20. Can you provide clarification on what the cost proposal should cover? |
| **A92** |  |  | FY20. |
| **Q93** | Appendix 2 – Technical Questionnaire | 2 | IT Governance Audit:  The RFP states the evaluation will be performed by evaluating the five domains of IT governance as defined by COBIT 5. Is this these process be evaluated against the COBIT process capability model? If so has the organization defined desired target levels for maturity? |
| **A93** |  |  | The Department has not defined target maturity levels at this time. |
| **Q94** | Appendix 2 – Technical Questionnaire | 2 | IT General Controls:  How many applications will be in scope? |
| **A94** |  |  | For IT General Controls: a sampling of 3-6 applications will be in scope. |
| **Q95** | Appendix 2 – Technical Questionnaire | 2 | IT General Controls:  Does the organization have a specific ITGC framework the contractor will assess against or will the contractor evaluate against generally expected control baselines based on good industry practice? If the former how many controls are in the proscribed framework? |
| **A95** |  |  | The Department prefers an ITGC recommendation be based on industry best practices. |
| **Q96** | Appendix 2 – Technical Questionnaire | 2 | IT General Controls:  Does the organization have proscribed sampling guidance for sample sizes or can the contractor use internal guidelines aligned with Institute of Internal Auditors standard practice? |
| **A96** |  |  | The selected vendor can use IIA standard practice. |
| **Q97** | Appendix 2 – Technical Questionnaire | 3 | IT Vendor Management:  The RFP states “The Contractor shall evaluate the existing vendor management processes including due diligence, security, contract review, financial stability, and contract compliance. **Additionally, the Contractor shall provide an assessment of the quality of and the ability to rely upon the Contractor’s attestations regarding internal controls**.” Is the bolded sentence referring to an opinion on the ability to rely on vendor IT controls? |
| **A97** |  |  | The bolded sentence should read as follows: “***Additionally, the Contractor shall provide an assessment of the quality of, and the ability to rely upon, vendor attestations regarding their internal controls.”*** The Department expects the Contractor to provide professional judgement, not necessarily an audit opinion, on the ability to rely on vendor IT controls. |
| **Q98** | Appendix 2 – Technical Questionnaire | 3 | IT Interfaces:  Is this intended to over a sample of interfaces between systems or a complete assessment of all interfaces? |
| **A98** |  |  | The Department intends this to cover a sample of interfaces. |
| **Q99** | Appendix 2 – Technical Questionnaire | 3 | IT Interfaces:  Does the entity already have an inventory of interfaces or is there a discovery component to audit? |
| **A99** |  |  | The Department does not see this engagement including a discovery process. The Department has a list of interfaces. This information is confidential and Department will provide this information to the selected vendor under a non-disclosure agreement. |
| **Q100** | Appendix 2 – Technical Questionnaire | 3 | Data Privacy Review:  Are there specific privacy standards or statutes this audit is intended to evaluate against? If so what are they? |
| **A100** |  |  | Please note that the “Data Privacy Review” item in 1.0D is not listed amongst the RFP’s requested services for specific audits. Audit items are listed in 1.0A and 1.0B. Data privacy review services are requested in the RFP for non-audit consulting, advisory and review services.  The Department is subject to the Privacy and Security Rules of the federal Health Insurance Portability and Accountability Act (HIPAA), as amended by the HITECH Act, due to the self-funded components of the State Group Health Insurance Plan that are administered by the Department. See 45 CFR Parts 160, 162 & 164.  At the State level, the Department is governed by the Department records confidentiality provisions in Chapter 40, Wisconsin Statutes. Chapter 40 specifically pertains to the Department. Section 40.07 states that Individual Personal Information in the records of the department is not a public record and shall not be disclosed except as provided in the section. In addition, the Department is subject to Wisconsin statute section 134.98, which requires certain notices for unauthorized acquisition of personal information.  As a public agency, the Department must comply with public records laws in Chapter 19, Wisconsin Statutes, which contain privacy provisions. |
| **Q101** |  |  | General Questions:  a) How many employees does the entity have?  b) How many employees are dedicated to IT?  c) How many core IT systems does the entity use?  d) How many core IT systems are developed internally vs. purchased/customized?  e) How many and what types of external entities does the entity directly exchange electronic information with?  f) What operating systems are used by typical workstations and servers?  g) How many endpoints and servers does the entity have?  h) How many software development personnel does the entity have? |
| **A101** |  |  | a) Less than 500.  b) Less than 100.  c) Currently 17 systems support service delivery.  d) The Department has a mix of in-house developed and COTS systems.  e) The Department has several third-party administrators with whom the Department exchanges data regularly.  f) This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement.  g) Approximately 500 end points, the number of servers will be reviewed with the selected vendor under a non-disclosure agreement.  h) Less than 50. |
| **Q102** | Appendix 2 – Technical Questionnaire | 2 | Network Security Assessment:  Approximately how many servers and workstations are in scope for the internal scans? |
| **A102** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q103** | Appendix 2 – Technical Questionnaire | 2 | Network Security Assessment:  For the external scans, how many IPs are in scope, and how many live hosts are expected? |
| **A103** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q104** | Appendix 2 – Technical Questionnaire | 2 | Network Security Assessment:  Is the Network Security Assessment internal vulnerability scan expected to be a credentialed or uncredentialed scan? |
| **A104** |  |  | The Department anticipates a bifurcated approach that includes credentialed and uncredentialed scanning. |
| **Q105** | Appendix 2 – Technical Questionnaire | 2 | Social Engineering Assessment:  Email phishing and a physical walk-in test appear to be included. How many targets are expected for the email phishing? |
| **A105** |  |  | Less than 500 users will be included in the email phishing exercise. |
| **Q106** | Appendix 2 – Technical Questionnaire | 2 | Social Engineering Assessment:  Email phishing and a physical walk-in test appear to be included.  How many facilities for the physical test? If multiple facilities are in scope, how far apart from each other are they located? |
| **A106** |  |  | One facility. |
| **Q107** |  |  | How many employees are in the Department? |
| **A107** |  |  | Less than 500. |
| **Q108** | Section 1.2 | 3 | Was the Department’s biannual audit plan developed based on the results of an IT risk assessment? |
| **A108** |  |  | Yes. |
| **Q109** | Appendix 2, Section 1.0 | 2 | Does the Department have a full, documented set of IT policies and procedures? |
| **A109** |  |  | Yes, these will be provided to the selected vendor under a non-disclosure agreement. |
| **Q110** | Appendix 2, Section 1.0 | 2 | Are the Department’s IT policies, procedures, processes, and controls currently aligned with COBIT 5 or another framework? If another framework, which one? |
| **A110** |  |  | The Department’s IT policies, procedures, processes and controls are not currently aligned with a formal industry framework. |
| **Q111** | Appendix 2, Section 1.0 | 2 | Will the Network Security Assessment be limited to vulnerability scanning, or are penetration tests desired? |
| **A111** |  |  | The Department does not anticipate penetration testing occurring as part of this engagement. |
| **Q112** | Appendix 2, Section 1.0 | 2 | Does Audit III for FY20, IT General Controls, include testing of technical application controls (i.e., input and access, output, processing, and file and data transmission controls)? |
| **A112** |  |  | The selected vendor will confirm the operating effectiveness of IT general controls for a sample of applications related to security, change management / system development, batch scheduling, and backup and recovery. |
| **Q113** | Appendix 2, Section 1.0 | 2 | Regarding the three IT audits listed under A. Audits in FY20 — when was the last time each of these audits was performed?   1. IT Governance Assessment 2. Network Security Assessment 3. IT General Controls |
| **A113** |  |  | This is the first audit of this depth and breadth in these areas. For the network security assessment, the Department is in a shared service environment which will limit the scope of this portion to the aspects the Department controls. |
| **Q114** | Appendix 2, Section 1.0 | 2 | Regarding the three non-audit consulting engagements listed under C. Non-Audit Consulting, Advisory, and Review Services in FY20 — when was the last time each of these reviews was performed?   1. SDLC Review 2. Endpoint Imaging Review 3. Data Management Review |
| **A114** |  |  | Non-audit consulting, advisory and review services have not been conducted previously in these areas to the depth and breadth of this scope. |
| **Q115** |  |  | Please share who the current incumbent is? |
| **A115** |  |  | There is no incumbent. |
| **Q116** | Appendix 1  Sec 1.2 & 1.5  Appendix 2  Sec 2.3 | 2  6 | The Department asks that the proposer confirm 10 years of experience and provide relevant engagements. This is also stated in the technical questionnaire on section 2.3 page 6 of 7. Would it be acceptable for the proposer to provide the information that the technical questionnaire asks for under the general questionnaire section and refer back to it in the technical questionnaire? |
| **A116** |  |  | No. The questionnaires are independent and scored separately. Proposals should be easy to read and review by evaluation committee members; flipping back and forth within a proposal does not aid in the review process. When responding to questions/requirements within the RFP do not simply refer back to other answers given. Provide the pertinent answer for each requirement. Do not provide duplicate supporting materials/attachments. |
| **Q117** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | What is the encryption solution in use? |
| **A117** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q118** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | What is the End Point detection & response (EDR) in place? |
| **A118** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q119** | C. Non-audit consulting, advisory and review services in FY20: Endpoint Imaging Review | 28 | What are the 3rd party products that need to be patched? |
| **A119** |  |  | This information is confidential, and the Department will provide this detail to the selected vendor under a non-disclosure agreement. |
| **Q120** | 2.3.1 Hard and Electronic Copies, Redacting | 10 | Please clarify the process by which it is possible to sign Forms A, B, C, D, and G, and still provide an OCR capability for those five documents. Per review of each of these documents it seems that the only way to apply the required signature is to them is to print them and sign paper copies, and once this is done, scanning the signed paper copies will not provide a document with OCR capability, but only a scanned image. |
| **A120** |  |  | The Forms do not need to be in OCR format, print them and sign them, or drop a signature into the document. |
| **Q121** | Appendix 1 General Questionnaire |  | The numbering in the General Questionnaire goes from 1.5 to 1.8. Please advise if questions are missing or provide correct numbering. |
| **A121** |  |  | This was an oversight. There is no section 1.6 or 1.7. Retain the RFP numbering in your Proposal. |
| **Q122** | Appendix 1  Appendix 2 |  | Would ETF prefer that proposers respond to the General and Technical Questionnaires directly on the Word document provided with Addendum 1, and include within our response submission? |
| **A122** |  |  | No preference. |
| **Q123** | Form H – Cost proposal setup | N/A | Is there any flexibility with how we show professional fees and expenses? The cost sheet states to combine expenses in the rate but in addition we would like to provide a detailed breakdown of hours, fees and expenses so we can be more transparent. |
| **A123** |  |  | In addition to the information and rates required to be entered in Tab 1 of the Cost Proposal Workbook, you may provide other information in Tab 2 of the Cost Proposal. All cost information must be included only in the Cost Proposal. |
| **Q124** | Section 2.4.2 Table 4:  Ref #1 App 3, section 3 (Legal Relations)  Ref #2 App 3, Section 6 (Audit Provisions)  Ref #3 App 3, Section 12.0 (Liquidated Damages)  Ref #7 App 3, Section 17 (Termination for Cause)  Ref #8 App 3, Section 18 (Remedies of the Department)  Ref #9 App 3, Section 22.0 (Confidential Information and HIPAA Business Associate Agreement)  Ref #10 App 3, Section 23.0 (Indemnification)  Ref #11 App 3, Section 25.0 (Right to Publish or Disclose)  Ref #12 App 3, Section 28.0, (Data Security and Privacy Agreement) |  | We request that the referenced sections be removed from Table 4 of Section 2.4.2 of the RFP and that exceptions be permitted for these sections, following the process outlined in Section 2.4.1 of the RFP.  A potential barrier to participating in the procurement are contract terms that create undue risk on the contractor. Given the nature of the referenced provisions, for contractors that operate under commercial terms and practices, these provisions may be overly burdensome.  We believe it is important to maximizing competition to allow offerors the opportunity to take exception to these sections and to allow the Department, in its discretion, to accept or reject any proposed exceptions, as provided in Section 2.4.1 of the RFP. |
| **A124** |  |  | The Department will not accept assumptions, exceptions, or changes to the items listed in ***RFP Table 4. No Assumptions or Exceptions Allowed.*** Per Section 2.4.2 Supplemental Information – IMPORTANT, no assumptions or exceptions to the Appendix 3 Sections listed in Table 4 are allowed. |
| **Q125** | Appendix 2 Audits in FY20 (July 1, 2019 – June 30, 2020): | 27 | Will ETF provide the tools to conduct the internal and external vulnerability assessment? |
| **A125** |  |  | No |

END

This Addendum is available on ETF’s Extranet at https://etfonline.wi.gov/etf/internet/RFP/InfoTechAudits-Consulting/index.html