Enterprise Security and Application Examination
RFP#: 3000013048
Questions & Answers

Deloitte & Touche LLP

1. If a vendor completes this assessment, are they precluded from future design, development and implementation work?
    - No, the vendor is not precluded from all future design, development and implementation work by performing this audit.
2. Is LDI open to an option for certain resource(s) providing support to be delivered from remote locations?
    - Yes, at the discretion and approval of the designated State Project Manager as stated in the RFP.
3. Can you provide us with a listing of all in scope applications, databases and associated technologies that you reference in the RFP? Please also include mobile applications platform details such as iOS/Android, list of all COTS (Commercial off-the-shelf) products in use including identity and access management.
    - The in scope applications, to include mobile applications, are documented in section 1.48 Tasks and Services. The MFS Mobile Application's platform is currently iOS and the Producer/Adjuster Mobile is built for iOS and Android. The link to LDI Software Development Standards is http://ldi.la.gov/docs/default-source/documents/publicaffairs/softwaredevelopmentstandards.pdf and can be found in Section 1.50 Technical Requirements. For identity and access management, we currently utilize Azure and AWS Identity Management.
4. Does LDI have source code and web application scanning tools/infrastructure available or does vendor need to bring in the software/hardware for the code review?
    - Source code can be provided. Vendor will need to bring in scanning tools and/or recommend scanning tools, included licenses for software.
5. Can you provide more specifications around your expectations for the systems architecture review in the RFP? For example, number of IP addresses in scope, does this include network scanning, external/third-party hosted applications, etc.
    - LDI expects the systems review to cover only LDI internal systems.

IBM Global Technology Services

1. What technology platforms are leveraged by LDI to support the IAM (Identity & Access Management) functions currently? If possible, please highlight the IAM technologies that handle internal LDI state employee access vs. LDI consumer (Industry Access platform) access.
    - LDI utilizes multiple technologies to support IAM for both, including OAuth and ASP.Net.
2. Will the awarded examiner be precluded from assisting LDI with any remediation efforts as a result of delivering this project? If so, what would be the duration that would need

to pass before the awarded company can assist LDI with implementation and remediation projects?
    - No, the awarded examiner is not precluded from assisting LDI with any remediation efforts due to performing this audit.
3. As part of security review, is a security threat and risk assessment of the applications and associated infrastructure in scope?
    - Yes, a security threat and risk assessment of the applications and associated infrastructure are in scope.
4. Will LDI please provide a list of the following?
    a. # of data centers
        - Two (2)
    b. # of IT/App Dev teams, business units, etc.
        - One (1) LDI IT/App Dev Team, one (1) LDI Business Unit.
    c. # of applications
        - Four (4) main LDI Applications, two (2) Mobile Applications
    d. # of servers
        - Ranging from 100 – 200 virtual servers
    e. Technology, software and hardware products being used in the infrastructure
        - VMWare and Windows Stack. Please refer to LDI Software Development Standards for a more specific listing of LDI Software utilized.
5. Are there configuration benchmarks or best practices frameworks, such as CIS Benchmarks, NIST, etc, that examiner findings must be mapped to?
    - There is no specific framework that must be utilized. Please provide all best practices frameworks or configuration benchmarks that you plan to utilize, in your proposal. Prior to use, the benchmarks and frameworks must be approved by the State Project Manager.
6. Are any of the applications or data hosted off-prem with 3rd party providers or in the Cloud?
    - No
7. Does LDI seek Manual Penetration Testing with exploitation as part of the Assessment of the LDI applications/technologies/networks? If so, what would be the rough in scope size of these in terms of numbers of applications, IP addresses, etc?
    - No, an architectural applications audit is required for this contract.
8. Does LDI seek any type of application focused code review, or DAST or SAST or manual code evaluation as part of the assessment of the LDI applications/technologies/networks? If so, how many lines of code are there per-application and what languages are they written in?
    - Yes.
        - RMS is ~300,000 lines

        - Employee Portal is ~25,000 lines
9. Does LDI seek Manual Penetration testing focused on the externally exposed footprint of any of its applications/technologies/networks?
    - No.

ISSQUARED

1. Will the Scope of the Project include assessing security of network infrastructure components, network security components or end user devices?
    - No.
2. In section 1.3 (Goals and Objectives) reference is made to 'all associated technologies' in the context of application security, application architecture and databases. What would those associated technologies consist of?
    - The link for LDI Software Development Standards is http://ldi.la.gov/docs/default-source/documents/publicaffairs/softwaredevelopmentstandards.pdf and can be found in Section 1.50 Technical Requirements.
3. Would secure remote access to servers, applications and databases be offered?
    - Yes
4. Will remote web-based meetings be acceptable to LDI if requested by contractor?
    - Yes, only upon approval of the designated State Project Manager.
5. Will contractor be allowed to install their preferred monitoring and assessment tools onto the LDI network?
    - Yes, if the designated State Project Manager approves the tools.
6. Will the contractor be able to establish/schedule their days onsite?
    - The Contractor and the State Project will work together to establish/schedule the contractor's days onsite. The State Project Manager must approve the schedule.
7. Regarding Section 3.3 Project Management – Does LDI have any preferred Project Management tools they would prefer the Contractor to use?
    - No.
8. Regarding Section 3.5 Contractor Resources – Will it be acceptable for the Project Manager and the Person performing the assessment be the same individual?
    - This is not recommended. Approval from the designated State Project Manager will need to be given first for this to occur.
9. What state and federal regulations, if any, is LDI required to follow?
    - The main source of regulations for LDI fall underneath the Title 22 Louisiana Insurance Code.
10. Will the selected contractor of this bid need to be on-site for the full anticipated term of contract, approximately September 9th, 2019-June 30th, 2020?
    - No.

11. Can preparation of deliverables and assessment of information gathered be done remotely?
    - Yes, only upon approval of the designated State Project Manager.
12. Does LDI have or will provide a plan for future Cloud based applications? (p. 28)
    - Yes.
13. Must submittal of worksheets and bi-weekly status reports be done with LDI equipment on-site, or can the contractor create the worksheets and bi-weekly reports remotely and then send electronically to the designated recipients? (p. 34)
    - The worksheets and reports can be created remotely and then sent electronically at the discretion of the designated State Project Manager.
14. Under 5.0 Compensation and Maximum Amount of Contract, there are blank items. Are those supposed to contain information?
    - No.
15. Does bi-weekly indicate two times a week, or does it indicate every 2 weeks?
    - Every two weeks

Janus Associates

1. Section 1.48, Tasks and Services, page 28. For sizing purposes, how many LDI applications and APIs that integrate with non-LDI applications are in-scope?
    - Two (2)
2. Section 1.48, Tasks and Services, page 28, All LDI Mobile Application's Codebase and Technologies. Is this to be a code security examination or a security review of the application without examining the code itself?
    - A code security examination.
3. Section 1.48, Tasks and Services, page 28. Are the LDI Software Development Standards documented?
    - Yes.
4. Section 1.48, Tasks and Services, page 28. How many LDI Software Development Standards are to be reviewed and updated?
    - All standards located in the LDI Software Development Standards are to be reviewed and recommended for updating based on the review.
5. Section 1.48, Tasks and Services, page 28. How large is the entirety of LDI's codebase?
    - Over 400,000 – 600,000 lines to review.
6. Section 1.48, Tasks and Services, page 28, 3rd bullet at the bottom. What type of activities are you seeking for the task of integrating and enhancing systems and technologies where practical?
    - Providing a detailed and defined architectural path
7. Section 1.48, Tasks and Services, page 28, 3rd bullet at the bottom. For this item "integrating and enhancing systems and technologies where practical" will this be follow-on work at a time and materials price?
    - No.

8. Section 1.10, page 12. You ask for a certified copy of a board resolution – are we to submit this as a separate document or incorporate it into our proposal?
    - You can incorporate it into your proposal.
9. Section 1.31.6, page 22. Are we to submit a COI with our proposal or upon award of contract?
    - No, you do not need to send the certificates as part of your proposal. The Certificates are to be received and approved by the Agency before work commences and upon any contract renewal or insurance policy renewal thereafter.