MULTI-STATE LOTTERY ASSOCIATION
Johnston, IA 50131
procurement@musl.com

MUSL wishes to thank bidders for submitting questions in regard *MUSL RFP 2021 Operational Security Assessment and Audit.* Thank you for your continued interest. We look forward to receiving your proposal by 19 July 2021.

The following is a consolidation of all questions and MUSL's response.

1. **Question:**
   Section 3.1. Do you want the assessment focused solely on the adequacy and effectiveness of the 2019 remediation efforts, or do you want an expanded assessment seeking new issues?

   Response:
   The primary focus of this project will be to assess the overall health of MUSL's operational security. This includes an evaluation on the adequacy and effectiveness of 2019 OSAA remediation efforts and a fresh review and analysis of our current state.

2. **Question:**
   Section 3.3.2. Do you wish the Draw control activities to include an on-site, visual assessment of the 'Draw' in addition to the analysis of this item?

   Response:
   On-site observations of draw activity are required for two locations: Johnston, IA and Tallahassee, FL.

3. **Question:**
   Section 3.3.3, Access management, internal and external. When you include active directory do you wish to determine the technical security (vulnerability-focus) of active directory or if the rules are being followed (compliance)? These require different activities.

   Response:
   Deliverables should include an assessment on the adequacy of our technical security, propose gap remediation and evaluate the effectiveness of existing procedures.

4. **Question:**
   How many findings were there identified on the 2019 review where the remediations will need to be reviewed?

   Response:
   In scope for this project are 31 recommendations from the 2019 review.

5. **Question:**
   MUSL lists several possible standards (e.g. CIS, WLA) that may be utilized but does not list either ISO or NIST. Is there a desire to be assessed against either of those security frameworks?

   Response:
   MUSL follows v7.1 of the CIS Control Framework and WLA-SCS section L.2.for draw activities. If there are important areas that those standards do not cover, we would like the vendor to bring those to our attention.

6. **Question:**
   How many personnel work at MUSL?

   Response:
   MUSL anticipates interaction with approximately 7 to 8 staff.

7. **Question:**
   Where do drawings occur?

   Response:
   Drawings occur in Johnston, IA and Tallahassee, FL.

8. **Question:**
   Will in-person observations be required at both locations?

   Response:
   Yes.

9. **Question:**
   The link provided in the RFP does not have an organization chart on the webpage or link to one. Please provide a copy of the most recent organization chart.

   Response:
   An organizational chart will be provided to the selected vendor.

10. **Question:**
    Section 1.12 (Standards Applicable to the Award): Please provide additional insight into how each of the individual evaluation criteria will be weighted. For example, what percentage of the overall score is allocated to cost?

Response (Question 10):
MUSL will select the best overall proposal taking into account vendor qualifications, methodology, operational security design, testing experience and fee proposal.

11. Question:
Is there a preferred version of the CIS Controls for the assessment? v7.1 or v8?

Response:
MUSL follows CIS Framework v7.1.

12. Question:
Does MUSL prefer and/or require field work to be completed on-site at MUSL locations, or is remote assessment permissible?
Response:
A combination of on-site and virtual fieldwork is acceptable. The vendor's project plan should reflect their proposed approach.

13. Question:
Will the presentation to the Audit Committee at the completion of the project be required to be in person?

Response:
The Audit committee prefers an in-person presentation, but video conferencing is potential option, as circumstances dictate.

14. Question:
Regarding RFP Section 3.3.8 (Data Security): Will MUSL permit the use of Computer Auditing Tools and scripts?

Response:
CAAT's are acceptable. Use of any tool or script requires prior review and written approval by MUSL.

15. Question:
Regarding RFP Section 3.3.14 (Other): Would MUSL like the proposing firm to include in our proposal other suggested areas for the assessment?

Response:
The RFP reflects the primary areas of focus.

MULTI-STATE LOTTERY ASSOCIATION
Johnston, IA 50131
procurement@musl.com

16. Question:

Regarding RFP Section 3.5.3 (Workspace Accommodations): Please provide a summary of current and/or expected COVID 19 protocols.

Response:

MUSL follows CDC and state/local guidelines.

17. Question:

Regarding Appendix C, Section 6.1, Item g: Does this pertain to any employee of our Firm? Or does this pertain only to employees who have worked on or may work on the engagement?

Response:

The selected vendor is expected to have policies and procedures in place to maintain strict confidentiality of client information. The prohibition of lottery game play is applicable to the engagement team and members of team members' immediate family member (parent, stepparent, child, stepchild, spouse, or sibling) that reside in the same household.

18. Question:

Regarding Section 7 of the RFP (Costs): Does MUSL have a budget estimate or not-to-exceed threshold for this project that you can share? If yes, please provide detail.

Response:

Proposals should reflect the bidders' fees for delivering the requirements of the RFP.

19. Question:

How many IT, security, and management personnel are expected to be included in scope for interviews and walkthroughs described under section 3.3?

Response:

We anticipant interaction with approximately 7 to 8 MUSL Staff.

20. Question:

How many policies and procedures need to be reviewed as part of 3.3.11 information security?

Response:

Approximately 30 policies and procedures.

MULTI-STATE LOTTERY ASSOCIATION
Johnston, IA 50131
procurement@musl.com

21. Question:

Provide an overview of MUSL infrastructure including workstations, servers, network/system configurations, active directories, databases, applications.

Response:

MUSL currently manages:

- Thirty-five workstations
- 90 servers, mostly virtual.
- Three firewalls
- Three managed switches
- Two wireless base station devices.
- Approximately 12 internal and external web applications,
- Azure, Office 365 and On-premises Active Directory
- Three databases are in scope.

Additional information will be provided to the selected vendor.

22. Question:

Describe your SDLC methodology, the number of systems developed in-house and do you use any third-party developers.

Response:

All development is done in-house following an Agile SDLC methodology. Two applications are in-scope.