MUSL RFP 2024 Operational Security Assessment
Vendor Questions and MUSL Responses - Issued April 3, 2024

1. What is the ultimate business problem that MUSL is solving with scope execution of this RFP? Do you have any specific goals or concerns you would like the testing to address?

   Per the RFP – "MUSL is required to engage an independent third party to perform a risk-based assessment on the design and effectiveness of its operational security and provide a gap-analysis identifying areas for potential improvement."

   MUSL is looking to have a third party examine its operational security to see whether MUSL is in compliance with recognized security standards, and to make recommendations for improvement.

2. What has MUSL done to date related to the scope, how were expectations not met?

   MUSL has performed operational security reviews biennially since 2015, but this year's scope is focused on the two identified security standards (NIST-CSF and WLA) and against MUSL's internal Security Policies.

3. MUSL has stated this engagement will perform an operational security risk assessment against the NIST CSF framework and will include an evaluation on the adequacy and effectiveness of the 2021-22 assessment's remediation efforts. Since this is based on a standardized framework, would MUSL like for the review to include a maturity roadmap scoring each area against the standard to show not only compliance but also the level of maturity in each area? This would further provide a maturity road map for future improvements.

   That is not required, but could be beneficial.

4. Will the MUSL Project Lead help to schedule walk-through interviews with key process owners?

   Yes

5. Will the MUSL Project lead be available for weekly status meetings to ensure timely access to people and data requests?

   Yes

6. MUSL stated that Fieldwork will principally be performed at MUSL's headquarters in Johnston, IA, at its local backup facilities near Des Moines, and a co-located draw facility in Tallahassee, Florida as well as a backup draw facility in Lincoln, Nebraska. Is remote capabilities available at all or should the resources plan to be on sight during the scheduled times?

   On-Site reviews are required.

7. Would the contractor be able to utilize Survey tools initially that are mapped back to the NIST CSF to allow process owners to answer initial questions and capture data requests? We have found this approach to be highly successful in allowing the process owners time to collect the data requests and answer the questions while reducing the costs to the client. This may further provide a way to interview a larger number of participants without increasing the budget.

   That would be acceptable.

8. If we have significant referenceable NIST CSF assessment experience and are not registered as a WLA SCS auditor, can our firm still propose this assessment?

   WLA certification capabilities are required to meet the RFP requirements.

9. What are the primary drivers for the testing (compliance, security audit, M&A, etc.)?

   Compliance, Security and Audit.

10. Are there any specific compliance standards you are targeting, such as PCI DSS, HIPAA, or ISO 27001?

    Yes – NIST CSF and WLA Security Standards, as well as MUSL's internal Security Policies.

11. What type of testing do you want (can pick multiple): network penetration testing, application security pentesting, social engineering, wireless, physical penetration testing, custom engagement

    No pen or physical testing, or phishing exercises are required.

12. Can you provide an overview of your network architecture at a high level?

    To the extent required, that will be provided during the engagement.