Request For Proposal (RFP)

Project: **Cybersecurity Assessment**

Issue Date: Thursday, January 4, 2024

Bids Due: Monday, January 22, 2024 - 12:00 PM

RFQ Contact: Bert Audette, baudette@famemaine.com, 207-620-3522

Introduction

FAME is accepting proposals from interested and qualified firms for cybersecurity assessment services to evaluate the information security controls, policies, and practices of the organization against objective controls in the NIST Cybersecurity Framework (CSF).

Background

The Finance Authority of Maine is an independent agency of the State of Maine located in Augusta, Maine. The Authority is the State's business and higher education finance agency, providing direct loans and financial services to businesses and students, and insuring loans from financial institutions to businesses and students attending institutions of higher education. The Authority is the administrator for the State's College Savings Plan, NextGen and is involved in administering funds from federal programs such as the State Small Business Credit Initiative.

Qualifications

Respondents should demonstrate and identify the qualifications of the company, staff, and sub-contractors that will perform the services offered. FAME prefers service providers that have a depth of expertise and experience in the following areas:

- Experience providing IT security controls and security assessment and auditing services for financial institutions and government agencies.
- Experience evaluating and mapping security controls against NIST Cybersecurity Framework (CSF) v1.1 and against the FTC GLBA Safeguards Rule.
- Experience with Windows Server, Active Directory, SQL Server, Microsoft 365, Entra ID (Azure AD), and similar solutions and their associated security risks.

- Experience with security risks associated with application development.
- Relevant industry recognized standard credentials such as CISSP, CISA, CISM, etc. for assessment personnel. Assessment lead is expected to hold a valid CISSP credential or its equivalent and have 10+ years of cybersecurity experience.
- Relevant industry recognized standard credentials such as GPEN, GWAPT, GXPN, CPT, OSCP, etc. for penetration testing personnel.

Scope of Work Requirements

1) Assess and evaluate FAME's security controls, policies, and practices against all the objective controls in the NIST Cybersecurity Framework (CSF) v1.1 (Identify, protect, detect, respond, and recover) as well as the FTC GLBA Safeguards Rule.
    a. The evaluation will determine FAME's CSF implementation tiers and target profiles and research similar organizations to determine target maturity and effectiveness.
    b. The evaluation will analyze any differential gaps between current and target states and prioritize suggested improvements by category and sub-category with both short and long-term recommendations to achieve these improvements.
    c. The evaluation will consider and document both associated threat level (high, medium, low) and estimated level of effort and resources required to mitigate (high, medium, low) each recommendation.
    d. The evaluation <u>may be</u> informed by the following assessment methods, as applicable:
        i. Through performing observations or testing of practices within the Cybersecurity Framework sub-categories as deemed necessary to identify the implementation maturity and effectiveness of FAME's security activities regarding compliance with the objective controls
        ii. Through requesting, collecting, reviewing, and evaluating evidence and documentation, etc.
        iii. Through conferences with key FAME personnel.
            1. This evaluation may include both scheduled group and targeted personnel interviews to be performed virtually or on-site at FAME's offices in Augusta, ME as necessary to inform the evaluation.
            2. Key FAME personnel may include:
                a. All IT personnel
                b. HR personnel
                c. Information security and risk management personnel
                d. Other personnel, as identified.
        iv. Through an inspection of FAME's custom applications that are accessible to external parties.
        v. Through demonstration or supervised inspection of hardware and software technical controls as authorized by FAME's CIO.
        vi. Through vulnerability analysis and non-destructive penetration testing, as authorized by FAME's CIO.

vii. Through other evaluation methods proposed by the Respondent, as authorized by FAME's CIO.

2) Provide a written report of the evaluation.
    a. Report will provide an executive summary as well as detailed observations, analyses, findings, results, and recommendations for improvement.
    b. Report will organize in alignment with the CSF control categories and sub-categories and identify each objective control as well as FAME's current implementation maturity and effectiveness of each control.
    c. Report will clearly identify CSF target profiles, target states, FAME's current maturity and effectiveness in each and analyze any differential gaps between current and target states.
    d. Report will perform a similar mapping and analysis against the FTC GLBA Safeguards Rule.
    e. Report will prioritize top areas of concern by category and sub-category and suggest improvements for each area of concern with both short and long-term recommendations for the implementation of these improvements.
    f. Report will identify findings of any non-destructive penetration testing with recommended remediations prioritized by severity, and associated common taxonomy (CVE, CWE, MITRE ATT&CK, TTPs.)
    g. A near final draft of the report will be provided to FAME's CIO for review at least two weeks prior to the agreed upon final report submission date. FAME's CIO will be provided with sufficient opportunity to offer comments and clarifications on the report contents prior to submission of a final report.
3) Present an executive summary review of the evaluation report and the highest priority recommendations for improvement to FAME's CIO and the risk management committee of the board. **This meeting is scheduled to occur on April 3rd, 2024.**
4) Provide FAME with follow-up services for a period no less than 90 days following delivery of the final report to the board, where FAME may ask questions or schedule follow-up calls and meetings to clarify information contained in the report. This follow-up support does not include support for vulnerability mitigation or remediation activities.

Engagement Requirements and Details

Respondents will be expected to sign a non-disclosure agreement with FAME to ensure that any sensitive details regarding FAME's technical environment and vulnerabilities identified during the assessment remain confidential and are not disclosed without FAME's prior consent.

Respondents are expected to meet the following expectations during the engagement:

- No testing or evaluation will begin until FAME and the successful Respondent formally agree on a final scope of work that includes the evaluation process and protocols, and a schedule of events that culminates in report submission and board presentation.
- If non-destructive penetration testing will be used during the assessment, FAME expects the service provider to perform the activities as outlined in the agreement, to scan,

enumerate, evaluate, and attempt to escalate privileges to FAME systems according to the scope of work and rules of engagement. Testers may use automated tools to perform scanning and other routine tasks helpful to the process, but a qualified individual must be engaged during the entirety of the tests. Fully automated penetration testing services will not be considered.

- The scope and duration of these tests will be mutually decided and agreed during pre-engagement activities.

The following details about FAME's technical environment are provided for Respondents to size their evaluation process appropriately to FAME's organizational and technical structure:

- Personnel: ~ 65 full time employees operating both on-site and remotely
- External IPs: 64 assigned with 10 to 15 reachable
- DNS Domains: 40 to 50 (1 primary, 10 host websites and limited mail, remaining are vacant or redirects)
- Physical servers: < 10
- Virtual machines: < 50
- Networks / VLAN segments: < 10
- Network devices: < 200
- IP Telephony devices: < 100
- Custom applications: < 25, Windows and web
- Development environments: VB6, C#, F#, .NET, SQL, IIS, PHP
- Databases: 25 to 30 in production + similar quantity in dev/test
- Server environments: VMware ESXi, Windows servers and clients, MS SQL, Citrix XenApp, Mac OS
- Authentication environment: MS Active Directory, Entra / Azure AD, Cisco Duo
- Mobile environment: Yes (Apple and Android)
- Custom mobile apps: No
- VPN: Yes
- Technical Documentation: Current network diagrams exist; protected data flow documentation does not. Previous security assessments documents are outdated and not available for review.

Value Added Services and Alternative Solutions (Optional)

FAME seeks creative and cost-effective solutions that increase efficiency and decrease expenditures. If the respondent's company offers unique or integrated service programs, or alternative solutions that add value to the products and services requested, please describe the details of the options available including cost, structure, and the benefits to FAME as an alternative option to the proposal for consideration.

Proposal Submission and Schedule

Proposals should be marked and submitted to FAME via electronic mail to Bert Audette, baudette@famemaine.com on or before Monday, January 22nd at 12:00PM.

The following table shows the anticipated schedule of events.

Event	Date
Request Published	Thursday, January 4, 2024
Deadline for Bid Submission	Monday, January 22, 2024 @ 12:00PM
Anticipated Decision Date	Friday, January 26, 2024
Anticipated Project Completion Date	Wednesday, April 3, 2024

Proposal Submission Guidelines:

This section contains instructions for Respondents to use in preparing their bids. FAME seeks detailed yet succinct responses that demonstrate the Bidder's qualifications, experience, and ability to perform the requirements specified throughout the Request.

The Respondent's proposal must follow the outline used below. Failure to use the outline specified here or failure to respond to all questions and instructions throughout the Request, may result in the proposal being disqualified or receiving a reduced score. FAME and its evaluation team, has sole discretion to determine whether a variance from the Request specifications will result in disqualification or reduction in scoring.

Bid proposals shall contain the information requested below and follow the format listed below.

1) Statement of Understanding
    a) The proposer should clearly state their understanding of FAME's goals for this project and describe how their proposed solution will facilitate the stated objectives.
2) Solution
    a) Provide a detailed summary and functional overview that identifies how you propose to meet each of the scope of work requirements as listed in this Request to inform a comprehensive evaluation of FAME's security policies and practices.
    b) Identify a proposed timeline and anticipated schedule of events necessary to meet the anticipated deadline, including all major milestones through final report and presentation delivery.
    c) Identify the resources, preparation tasks, and activities that FAME is responsible for or must perform to accomplish the scope of work.
3) Pricing
    a) FAME prefers contracts for this project to be issued on a fixed price. Detail the costs of major component elements and provide a total project cost to meet all stated objectives.
    b) Provide the costs of proposed alternative, optional, or value-added services.

c) Provide your firm's hourly rate for any additional consultation in support of recommendations and remediation activities as identified during the assessment.

4) Experience and Qualifications
   a) Provide a summary background of your organization identifying your experience and qualifications to perform this assessment.
   b) Identify the names and functions of the specific individuals (staff and sub-contractors) who would be assigned to lead the completion of this project for FAME and provide a summary of their experience and qualifications to provide the services offered.
   c) Demonstrate your experience with security assessment documentation by providing a sample representative report that is performed by your organization which meets similar requirements.
   d) Provide a summary of your experience serving similar clients and projects and a list of at least three (3) clients for whom the Respondent has provided similar products and/or services to those requested in this Request. Information provided should include the name, address, and telephone number of the client organization, and the name, title, and phone of a person who may be contacted for further information.

Proposals must be received by the date and time listed on the cover page of the Request. Emails messages containing original proposal submissions, or any additional or revised proposal files, received after this deadline may be rejected.

Only proposal submissions received by email will be considered. FAME assumes no liability for assuring accurate/complete e-mail transmission and receipt.

Emails messages containing links to file sharing sites or online file repositories will not be accepted as submissions. Only email proposal submissions that have the actual requested files attached will be accepted. Encrypted email messages received which require opening attachments and logging into a proprietary system will not be accepted as submissions.

Email message size limits are 25MB per message. Respondents may submit files separately across multiple emails, as necessary, due to file size concerns. All emails and files must be received by the due date and time listed above.

Respondents are to insert the following into the subject line of their proposal submission: "Bid Submission – [Bidder's Name]"

Following announcement of an award decision, all submissions in response to this Request will be public records, available for public inspection pursuant to the State of Maine Freedom of Access Act (FOAA) (1 M.R.S. § 401 et seq.)

Evaluation Criteria:

The goals of the evaluation process are to ensure fairness and objectivity in review of the proposals and to ensure that the contract is awarded to the Respondent whose proposal provides the best value to FAME.

FAME reserves the right to communicate and/or schedule interviews/presentations with respondents, if needed, to obtain clarification of information contained in the proposals received. FAME may revise the scores assigned in the initial evaluation to reflect those communications and/or interviews/presentations. Changes to proposals, including updating or adding information, will not be permitted during any interview/presentation process and, therefore, respondents must submit proposals that present their rates and other requested information as clearly and completely as possible.

The evaluation criteria in the following table are intended to be the basis under which each proposal will be evaluated, measured, and ranked. FAME hereby reserves the right to evaluate, at its sole discretion, the extent to which each proposal received compares to the stated criteria. The recommendation of the evaluation team shall be based on the evaluations using the criteria. Members of the evaluation team will not score those sections individually but, instead, will arrive at a consensus as to assignment of points for each of those sections.

Criteria	Description	Maximum Score
Functional & Technical Requirements	Clearly demonstrated understanding of the project scope, work to be performed, completeness and reasonableness of the solution proposal for accomplishing the requested services.	50 points
Vendor Qualifications & Experience	Considers the bidder's qualifications to provide the requested services as well as past performance and experience in providing the services solicited by this Request, and the results of any reference checks performed.	25 points
Total Cost	Calculated total cost of the proposed solution, based on initial and on-going costs, and reasonableness of the pricing proposal. The bid with the lowest calculated total cost will be awarded maximum points. Bids with higher costs will be awarded proportionately fewer points, in comparison with the lowest cost bid.	25 points

Subcontractors

The Respondent is responsible for the performance of any obligations that may result from this RFP and shall not be relieved by the non-performance of any subcontractor. Bid proposals must

identify all subcontractors and describe the contractual relationship between the bidder and each subcontractor.

For each portion of the proposed products or services to be provided by a subcontractor, the technical proposal must include the identification of the functions to be provided by the subcontractor and the subcontractor's related qualifications and experience.

The combined qualifications and experience of the bidder and any or all subcontractors will be considered in the RFP evaluation. All subcontracts held by the bidder must be made available upon request for inspection and examination by appropriate FAME officials, and such relationships must meet with the approval of FAME.

For all sub-contractors that are proposed to be used in providing the required products or services, Respondents must provide the following information: Name, Address, State in which the business is established, the subcontractor's responsibilities under the proposal, and the subcontractor's form of organization.

Questions and Inquiries:

It is the responsibility of all Respondents and other interested parties to examine the entire Request and to seek clarification, in writing, if they do not understand any information or instructions. All such questions and inquiries related to this Request are to be submitted in writing via email and directed to Bert Audette, baudette@famemaine.com prior to January 15th, 2024. No additional summary of questions and answers will be produced.

Selection and Award

The contract award will be based upon the best combination of vendor qualifications, capabilities, quality, delivery time, bid history, references, and experience performing similar projects in Maine, in addition to the evaluation criteria previously identified.

FAME reserves the right to reject any or all bids in whole or in part and is not necessarily bound to accept the lowest bid if that bid is contrary to the best interests of FAME. FAME also reserves the right to negotiate with any Respondent if that bidder is deemed to be most suited to the FAME's needs.

No Best and Final Offers

FAME will not seek or accept a best and final offer (BAFO) from any Respondent in this procurement process. All Respondents are expected to provide their best value pricing with the submission of their proposal. Price quotes must be firm through installation and adoption. All prices in the bid must be firm for six months.

Negotiations

FAME reserves the right to negotiate with the awarded Respondent to finalize a contract. Such negotiations may not significantly vary the content, nature or requirements of the proposal or the FAME's Request for Proposal to an extent that may affect the price of goods or services requested. FAME reserves the right to terminate contract negotiations with an awarded Respondent who submits a proposed contract significantly different from the proposal they submitted in response to the advertised Request. In the event that an acceptable contract cannot be negotiated with the highest ranked Respondent, FAME may withdraw its award and negotiate with the next-highest ranked Respondent, and so on, until an acceptable contract has been finalized. Alternatively, FAME may cancel the Request, at its sole discretion.

The final decision regarding the award of the contract will be made by the Chief Executive Officer of the Authority.

Notification of conditional award selection or non-selection will be made in writing by FAME.

Issuance of the Request in no way constitutes a commitment by FAME to award a contract, to pay costs incurred in the preparation of a response to the Request, or to pay costs incurred in procuring or contracting for services, supplies, physical space, personnel or any other costs incurred by the Respondent.

FAME reserves the right to reject any and all proposals or to make multiple awards.

Contract Administration and Conditions

The awarded Respondent will be required to execute a contract in form and content acceptable to FAME. Respondents should include any proposed contracts with their Response, but FAME reserves the right to require its own form contract.

Allocation of funds is final upon successful negotiation and execution of the contract, subject to the review and approval of FAME's Chief Executive Officer. The Authority recognizes that the actual contract effective date depends upon completion of the Request evaluation process, date of formal award notification, length of contract negotiation, and preparation and approval by FAME's Chief Executive Officer. Any appeals to FAME award decision(s) may further postpone the actual contract effective date, depending upon the outcome. The contract effective dates listed in this Request may need to be adjusted, if necessary, to comply with FAME requirements.

In providing services and performing under the contract, the awarded Respondent must act as an independent contractor and not as an agent of FAME.

Taxation and Compliance

FAME's purchase of goods and services is exempt from state, federal, and local sales and use taxes. The successful Respondent agrees to comply with all applicable federal, state, and local statutes, laws, and regulations in the performance of the Contract.