REQUEST FOR PROPOSALS
RFP No: CP 04/1617
FFA RISK ASSESSMENT OF THE NETWORK INFRASTRUCTURE AND INFORMATION SYSTEMS

BACKGROUND

FFA owns, operates and maintains an ICT infrastructure. The ICT infrastructure employs and houses a wide range of technologies including a suite of critical FFA information systems that streamlines the functions of the organisation. Noting the importance of the ICT infrastructure and information systems to all functions of FFA, maintaining a well-structured and secure infrastructure of information technology is essential to the daily function of the FFA. One very important factor that contributes to maintaining a well-structured, secure infrastructure of information technology is the ability to carry out more timely and thorough security risk assessment of the existing functions of the FFA ICT infrastructure and information systems.

FFA'S REQUIREMENTS

Objectives

FFA wishes to engage a security consultant firm/company having security expertise in network and information systems security to submit tender proposals to conduct a thorough security risk assessment of the **FFA Network Infrastructure and Information Systems**.

All security risk assessment activities should be conducted in a manner that includes:

- Simulating an attacker originating for the external perimeter (Internet).
- Simulating an attacker that has established access to the internal network. This could be from an already compromised system, malicious insider, or other avenue.
- An attacker that is attempting to compromise the environment through traditional wireless technologies.
- Identifying what exposures exist through using mobile devices and applications within the FFA network infrastructure and information systems.
- Performing simulated attacks against FFA web applications in order to identify what exposures exist.
- Performing zero-day research on applications used by FFA in an attempt to identify exposures prior to attackers finding them in the wild.

- Determining the impact of a security breach on:
  - Confidentiality, Integrity and Availability of FFA's data
  - External and Internal infrastructure and availability of FFA information systems
  - FFA critical infrastructure and information systems

Scope

Conduct a thorough security risk assessment of the FFA Network Infrastructure and Information Systems highlighting security gaps according to risk exposure by:

- Performing threat modelling analysis , vulnerability analysis, penetration test and vulnerable code review of the infrastructure and information systems
- Conducting both targeted and blind penetration tests on FFA external and internal infrastructure and information systems
- Providing specific recommendations for remedy for each finding/risk along with suggestion for improvements in terms of technology solution and risk treatment modality [Accept/Mitigate/Transfer/Avoid].
- Providing specific solution specification with recommendation for the identified vulnerabilities
- Providing a security risk assessment report including any test results based on findings covering both FFA external and internal infrastructure and information systems.

Methodology

The security consultant firm/company should include as part of their tender proposal submission of the following;

- Types of security risk assessment to be performed
- How security risk assessment will be performed
- What the security risk assessment will target
- The tools used for the security risk assessment and
- Whether the security risk assessment can be done remotely or on site

The security risk assessment should be carried out in accordance with NIST Information Security testing and Assessment NIST 800-115 procedures or an equivalent standard.

Deliverables

- Security Risk Assessment Report detailing security gaps prioritised by risk exposure and containing recommendations to address these. The report should include test details, test cases, test methods, findings, and specific controls.
- Knowledge transfer to the FFA ICT team on assessing and improving security
- Recommendation on security software/tools needed to enhance security

Special Note

Contractor will have to sign separate non-disclosure agreements with the FFA considering data/information sensitivity.

Tender Evaluation Criteria

All bids shall be evaluated using a two stage procedure with evaluation of the technical proposal being completed prior to any financial proposal being reviewed and compared.

Bidders are required to submit their financial proposal as a separate document.

Technical Proposal

The criteria against which proposals will be assessed include the following:

Selection Criteria	**Percentage**
Experience • Evidence of relevant qualifications (OSCP, CEH, CISSP, etc.) and experience of key personnel to be involved • Proven capability in undertaking similar type of assignment (reference or testimonial required).	40 %
Methodology • Coverage of scope and deliverables	40 %
Timeframes • Bidders should include details regarding expected visits, time required to produce draft and final reports	20 %

Financial Proposal

Price is to be submitted as a separate document and may be quoted in United States Dollars (USD) or Solomon Dollars (SBD)

References

All submissions are required to provide evidence of professional or technical capacity such as educational or professional qualifications, details of experience on similar projects.

All submissions are required to verify financial capacity, for example; evidence may include a banker's reference, audited financial statements or details of professional indemnity insurance.

CLOSING DATE OF PROPOSAL - EXTENDED

Tenders must be received by the 31St January 2017

Tenders should be addressed to:

FFA Tender Committee
Forum Fisheries Agency (FFA)
CP04/1617 Security Risk Assessment of FFA Network Infrastructure and Information Systems
PO Box 629
Honiara

OR

Emailed to: procurement@ffa.int please note in the subject line: CP04/1617 Security Risk Assessment of FFA Network Infrastructure and Information Systems.

Place of performance

The security risk assessment is expected to be done largely remotely but if there is a need to be on site then this will take place at the FFA Headquarter in Honiara, Solomon Islands.

Request for further information

For additional information regarding the tender or to arrange an on-site visit please contact Mr Kenneth Katafono on email: kenneth.katafono@ffa.int

Award of Contract

FFA reserves the right to accept any EOI, and to annul the solicitation process and reject all proposals at any time prior to award of any contract, without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected bidder(s) of the grounds for such action.

Notification

The names of winning bidders shall be advertised on the FFA website;
www.ffa.int/employment/tenders/tender_results