<Company Logo>

<Company Name>

<Project Name>

Prepared October 11, 2017

Proprietary and confidential

R E Q U E S T F O R P R O P O S A L

Table of Contents

USING THIS TEMPLATE

Foundstone has developed this Request For Proposal ("RFP") template to help organizations identify and select a quality security vendor to perform professional services work. It also lists questions organizations should consider asking potential vendors to ensure that a thorough and comprehensive approach to the project will be taken. This template should apply for a variety of information security projects including:

- External Network Vulnerability Assessment and Penetration Testing
- Internal Network Vulnerability Assessment and Penetration Testing
- Web Application Penetration Testing
- Dial-In / RAS Security Testing
- DMZ or Network Architecture Designs / Reviews
- Wireless Network Assessment and Penetration Testing
- Virtual Infrastructure Security Assessment
- Server Configuration Reviews
- Firewall and Router Configuration Reviews
- VPN Configuration Reviews
- Voice over IP Assessments
- Social Engineering Assessments
- Physical Security Reviews
- Software Source Code Reviews
- Application Threat Modeling and Design Reviews
- Information Security Policy and Procedure Development or Review
- Information Security Risk Assessment
- Security Awareness Program Development or Review
- Incident Response Program Development or Review
- Secure SDLC Program Development or Review
- PCI Quarterly Scans
- PCI Report on Compliance Assessment or Gap Analysis

TEMPLATE CONTENTS

The template contains a number of different sections that provide the vendor with a better understanding of the business and technical objectives of the effort. The major sections of the RFP template are:

- **Introduction and Background:** A description of the project's objectives plus any additional background about the organization or business objectives that may provide the vendor with additional useful perspective.

- **Administrative Information:** Contact information that the vendors will need to prepare and submit their proposal as well as major dates associated with the RFP submission, evaluation and award process.

- **Guidelines for Proposal Preparation:** Guidelines for vendor communication with the organization are provided in this section and a preferred proposal format is described for the vendor.

- **Evaluation Factors for Award:** Outlines the criteria that will be used to evaluate the various proposals.

- **Statement of Work and Deliverables:** This section provides sufficient technical details about the environment to allow a vendor to understand the scope of the effort and price it appropriately. In addition, the deliverables or work products required from the project are described.

INTRODUCTION AND BACKGROUND

PURPOSE OF THE REQUEST FOR PROPOSAL

ABC Company is a provider of specific products or services to types of customers in the industry. It has facilities in approximately number locations within the United States, as well as several other locations in Europe and Asia.

ABC Company is interested in conducting a security assessment that will allow it to:

- Provide line items that summarize the scope of the work required. Examples are:
- Gain a better understanding of potential corporate network vulnerabilities that may be visible from the Internet.
- Determine if the current wireless network is configured securely.
- Evaluate the security associated with public self service web applications that are used by ABC Company's customers.

These activities are part of ABC Company's ongoing risk management program and are focused on identifying the risk level ABC Company is currently exposed to so that an appropriate set of responses to those threats can be developed.

ABC Company is seeking to identify and select an outside independent organization to perform the activities listed above. The remainder of this document provides additional information that will allow a service provider to understand the scope of the effort and develop a proposal in the format desired by ABC Company.

ADMINISTRATIVE

TECHNICAL CONTACT

Any questions concerning technical specifications or Statement of Work (SOW) requirements must be directed to:

Name	
Address	
Phone	
FAX	
Email	

CONTRACTUAL CONTACT

Any questions regarding contractual terms and conditions or proposal format must be directed to:

Name	
Address	
Phone	
FAX	
Email	

DUE DATES

A written confirmation of the Vendor's intent to respond to this RFP is required by XX/XX/XX. All proposals are due by time am/pm on XX/XX/XX. Any proposal received at the designated location after the required time and date specified for receipt shall be considered late and non-responsive. Any late proposals will not be evaluated for award.

SCHEDULE OF EVENTS

Event	Date
1. RFP Distribution to Vendors	
2. Written Confirmation of Vendors with Bid Intention	
3. Questions from Vendors about scope or approach due	
4. Responses to Vendors about scope or approach due	
5. Proposal Due Date	
6. Target Date for Review of Proposals	
7. Final Vendor Selection Discussion(s)--Week of	
8. Anticipated decision and selection of Vendor(s)	
9. Anticipated commencement date of work	

GUIDELINES FOR PROPOSAL PREPARATION

PROPOSAL SUBMISSION

Award of the contract resulting from this RFP will be based upon the most responsive Vendor whose offer will be the most advantageous to ABC Company in terms of cost, functionality, and other factors as specified elsewhere in this RFP.

ABC Company reserves the right to:

- Reject any or all offers and discontinue this RFP process without obligation or liability to any potential Vendor,
- Accept other than the lowest priced offer,
- Award a contract on the basis of initial offers received, without discussions or requests for best and final offers, and
- Award more than one contract.

Vendor's proposal shall be submitted in several parts as set forth below. The Vendor will confine its submission to those matters sufficient to define its proposal and to provide an adequate basis for ABC Company's evaluation of the Vendor's proposal.

In order to address the needs of this procurement, ABC Company encourages Vendors to work cooperatively in presenting integrated solutions. Vendor team arrangements may be desirable to enable the companies involved to complement each other's unique capabilities, while offering the best combination of performance, cost, and delivery for the Penetration Test being provided under this RFP. ABC Company will recognize the integrity and validity of Vendor team arrangements provided that:

- The arrangements are identified and relationships are fully disclosed, **and**
- A prime Vendor is designated that will be fully responsible for all contract performance.

Vendor's proposal in response to this RFP will be incorporated into the final agreement between ABC Company and the selected Vendor(s). The submitted proposals are suggested to include each of the following sections:

1. Executive Summary
2. Approach and Methodology
3. Project Deliverables
4. Project Management Approach
5. Detailed and Itemized Pricing
6. Appendix: References
7. Appendix: Project Team Staffing
8. Appendix: Company Overview

The detailed requirements for each of the above-mentioned sections are outlined below.

DETAILED RESPONSE REQUIREMENTS

EXECUTIVE SUMMARY

This section will present a high-level synopsis of the Vendor's responses to the RFP. The Executive Summary should be a brief overview of the engagement, and should identify the main features and benefits of the proposed work.

SCOPE, APPROACH, AND METHODOLOGY

Include detailed testing procedures and technical expertise by phase. This section should include a description of each major type of work being requested of the vendor. All information that is provided will be held in strict confidence. The proposal should reflect each of the sections listed below (examples of the types of sections that could appear are listed below – select or modify them as appropriate):

- External Network Vulnerability Assessment and Penetration Testing
- Internal Network Vulnerability Assessment and Penetration Testing
- Web Application Penetration Testing
- Dial-In / RAS Security Testing
- DMZ or Network Architecture Designs / Reviews
- Wireless Network Assessment and Penetration Testing
- Virtual Infrastructure Security Assessment
- Server Configuration Reviews
- Firewall and Router Configuration Reviews
- VPN Configuration Reviews
- Voice over IP Assessments
- Social Engineering Assessments
- Physical Security Reviews
- Software Source Code Reviews
- Application Threat Modeling and Design Reviews
- Information Security Policy and Procedure Development or Review
- Information Security Risk Assessment
- Security Awareness Program Development or Review
- Incident Response Program Development or Review
- Secure SDLC Program Development or Review
- PCI Quarterly Scans
- PCI Report on Compliance Assessment or Gap Analysis

DELIVERABLES

Include descriptions of the types of reports used to summarize and provide detailed information on security risk, vulnerabilities, and the necessary countermeasures and recommended corrective actions. Include sample reports as attachments to the proposal to provide an example of the types of reports that will be provided for this engagement.

PROJECT MANAGEMENT APPROACH

Include the method and approach used to manage the overall project and client correspondence. Briefly describe how the engagement proceeds from beginning to end.

DETAILED AND ITEMIZED PRICING

Include a fee breakdown by project phase and estimates of travel expenses.

APPENDIX: REFERENCES

Provide three current corporate references for which you have performed similar work.

APPENDIX: PROJECT TEAM STAFFING

Include biographies and relevant experience of key staff and management personnel. Describe the qualifications and relevant experience of the types of staff that would be assigned to this project by providing biographies for those staff members. Describe bonding process and coverage levels of employees. Affirm that no employees working on the engagement have ever been convicted of a felony.

APPENDIX: COMPANY OVERVIEW

Provide the following for your company:

- Official registered name (Corporate, D.B.A., Partnership, etc.), Dun & Bradstreet Number, Primary and secondary SIC numbers, address, main telephone number, toll-free numbers, and facsimile numbers.
- Key contact name, title, address (if different from above address), direct telephone and fax numbers.
- Person authorized to contractually bind the organization for any proposal against this RFP.
- Brief history, including year established and number of years your company has been offering Information Security Testing.

EVALUATION FACTORS FOR AWARD

CRITERIA

Any award to be made pursuant to this RFP will be based upon the proposal with appropriate consideration given to operational, technical, cost, and management requirements. Evaluation of offers will be based upon the Vendor's responsiveness to the RFP and the total price quoted for all items covered by the RFP.

The following elements will be the primary considerations in evaluating all submitted proposals and in the selection of a Vendor or Vendors:

1. Completion of all required responses in the correct format.
2. The extent to which Vendor's proposed solution fulfills ABC Company's stated requirements as set out in this RFP.
3. An assessment of the Vendor's ability to deliver the indicated service in accordance with the specifications set out in this RFP.
4. The Vendor's stability, experiences, and record of past performance in delivering such services.
5. Availability of sufficient high quality Vendor personnel with the required skills and experience for the specific approach proposed.
6. Overall cost of Vendor's proposal.

ABC Company may, at their discretion and without explanation to the prospective Vendors, at any time choose to discontinue this RFP without obligation to such prospective Vendors.

SCOPE OF WORK

REQUIREMENTS

The following information should be used to determine the scope of this project and provide pricing for this engagement: *(Fill in the appropriate information for the scope of this project, providing as many details as possible about the targets of the assessment. The rows in the table below provide a few examples for various types of assessments.)*

External Network Vulnerability Assessment • Number of IP addresses in target space: XX • Number of live hosts: XX
Internal Network Vulnerability Assessment • Number of servers in target space: XX • Number of network devices in target space: XX • Number of workstations in target space: XX
Server Configuration Reviews • Number and type (operating system and function) of servers to be reviewed: XX
Firewall Reviews • Number of type of firewalls to be reviewed: XX • Number of rules in each firewall rule set: XX
Web Application Assessment • Name and description of each application to be assessed: XX • Number of user input pages for each application: XX • Number of user roles / privilege levels for each application: XX
Application Code Review • Name and description of each application to be assessed: XX • Number of lines of code in the application: XX • Language(s) the application is written in: XX

DELIVERABLES

At the conclusion of the assessment, ABC Company requires written documentation of the approach, findings, and recommendations associated with this project. A formal presentation of the findings and recommendations to senior management may also be required. The documentation should consist of the following:

DETAILED TECHNICAL REPORT
A document developed for the use of ABC Company's technical staff which discusses: the methodology employed, positive security aspects identified, detailed technical vulnerability findings, an assignment of a risk rating for each vulnerability, supporting detailed exhibits for vulnerabilities when appropriate, and detailed technical remediation steps.

EXECUTIVE SUMMARY REPORT
A document developed to summarize the scope, approach, findings and recommendations, in a manner suitable for senior management.