



Proposal for Foundstone Technical Services

Presented

To

Statement of Work #



Statement of Work

INTRODUCTION

Objectives

_____ (“Customer”) has, subject to the Provisions of DIR Contract No. DIR_SDD_1855, contracted Foundstone Professional Services, a division of McAfee, Inc. (“Foundstone”), thru reseller MOMENTUMCOM, INC. dba Solid Border, to assess the security of specific applications within Customer's networks in order to determine if there are areas for improvement in either the application architecture or the actual programming of the applications.

Statement of Work

SCOPE OF WORK (“SOW”)

1. **Description of Services to be rendered.** Subject to the terms of DIR Contract No. DIR-SDD-1855, _____.

Application Testing

Foundstone will perform a series of steps to review the security of the following application(s):

Foundstone will test the application(s) for vulnerabilities that could lead to unauthorized access of those applications or their supporting environments. Foundstone will use a combination of tools, utilities and methodologies to review the various potential points of security failure. Those steps will include, but not be limited to, the following types of activities:

- Scan for and identify well-known Web server, code engine, and database vulnerabilities
- Identify and attempt to compromise any server and application administration flaws
- Analyze basic functionality of the user interface, normal application behavior, and the overall application architecture for potential security vulnerabilities
- If possible, analyze data communications between the application and databases or other back-end systems
- Manually analyze all input facilities for unexpected behavior such as SQL injection, arbitrary command execution, and unauthorized data access
- Analyze user and group account authentication and authorization controls to determine if they can be bypassed
- Identify information leakage across application boundaries, including the capability to enumerate other users’ data and “show code” weaknesses that reveal internal application logic
- Identify areas where error handling is insufficient or reveals too much sensitive information
- Identify opportunities to write to the host file system or execute uploaded files
- Identify product sample files, application debugging information, developer accounts or other legacy functionality that allows inappropriate access
- Attempt to determine if fraudulent transactions can be performed
- Attempt to view unauthorized data, especially data that should be confidential
- Examine client-side cached files, temporary files, and other information that can yield sensitive information or be altered and re-submitted
- Analyze encoded and encrypted tokens, such as cookies, for weakness or the ability to reverse engineer

2. **Deliverables** Subject to the terms of the DIR Contract No. DIR-SDD-1855.A report deliverable will be provided at the conclusion of the engagement. Foundstone produces two primary deliverables from its security assessment engagements - an executive summary document and a detailed technical report. Customer shall have the right to keep the deliverables after the engagement for its own internal purposes. The executive summary describes the project’s scope, approach, findings and recommendations in a non-technical fashion suitable for senior management. It describes the:

- Purpose of the engagement
- Major steps that were taken to perform the engagement
- Positive security aspects that were identified

Appendix F to DIR Contract No. DIR-SDD-1855



- Primary types of vulnerability issues encountered and their business impact
- Systemic causes of the vulnerability issues encountered
- General recommendations - both policy and technical
- An assessment of how this organization's security posture compares to other similar organizations

The detailed report contains a more technical description of the project's activities, findings and recommendations. Much of the content provided in the executive summary is repeated in the detailed technical report. However, much more detailed descriptions of the methodology, technical findings and technical recommendations are provided. The technical findings are categorized and structured to facilitate immediate remedial action by the technical administrators. The following information is provided for each vulnerability:

- A text description of the vulnerability
- Business or technical risk inherent in the vulnerability
- Vulnerability classification (High, Medium or Low) that describes the risk level as a function of vulnerability impact and ease of exploitation
- A step-by-step technical description of how to reduce the exposure inherent in the vulnerability

Schedule for provision of Services and Deliverables

Testing to begin on a mutually agreeable date on or after _____.

Appendix F to DIR Contract No. DIR-SDD-1855



PRICING

Fee Schedule (in accordance with Appendix C. Pricing Schedule. of DIR Contract No. DIR-SDD-1855):

Application Testing- _____

Unemployment Insurance System – 5 weeks total

- Up to 4 weeks of system testing
- Up to 1 week to generate report to be delivered by the end of September.

Total Technical Services Fees: \$ _____

- **SKU to be used on the Purchase Order:** ES-FS-QUOTE

3. Terms of this Scope of Work:

The terms and conditions set forth in DIR Contract No. DIR-SDD-1855 shall govern all transactions by Customers under this Agreement. Customer shall not have the authority to modify the terms of this Agreement, except as to receive better terms or pricing for a particular procurement than those set forth herein. In such event, Manufacturer shall furnish a copy of such better offering to the DIR upon request. No additional term or condition of a purchase order issued by a Customer can weaken a term or condition of this Agreement. In the event of a conflict between a Customer's purchase order and this Agreement, the Agreement shall control. In the event of a conflict between this Agreement and DIR Contract No. DIR-SDD-1855, the DIR Contract shall control.

Appendix F to DIR Contract No. DIR-SDD-1855

Page 5 of 8



Statement of Work

Purchase Orders

Subject to the terms of DIR Contract No. DIR-SDD-1855, all Customer purchase orders associated to this SOW shall be made out to:

- MOMENTUMCOM, INC. dba Solid Border 1806 Turnmill, San Antonio, TX 78248
- Please fax purchase orders to 800-887-9974.
- Include DIR Contract number DIR-SDD-1855 **Contact Information**

Customer Points of Contact:

Foundstone Scope Contact:

Foundstone Resource Coordinator:

Sarah Ezell
(972) 987-2634 Office

Appendix F to DIR Contract No. DIR-SDD-1855



TECHNICAL SERVICES AGREEMENT TERMS

4. Scope of Work. Subject to the terms of the DIR Contract No. DIR-SDD-1855, Foundstone Professional Services, a division of McAfee, Inc. ("Foundstone"), agrees to provide to Customer the services, including any Deliverables, as are described in the Scope portion of this Agreement (the "Services"). Additional Services may be added to this Agreement and the Scope may be modified by the mutual written agreement of the parties. The Services will be performed by qualified personnel in a professional and workmanlike manner consistent with industry standards.
5. Customer Responsibilities. Subject to the terms of the DIR Contract No. DIR-SDD-1855,
Customer shall provide Foundstone with appropriate information concerning, and reasonable access to, Customer's computer systems and provide all information, access and full, good faith cooperation reasonably necessary to facilitate the Services, including one or more employees of Customer who have substantial computer systems and network and project management experience to act as a liaison between Customer and Foundstone. If Customer fails or delays in its performance of any of the foregoing, Foundstone shall be relieved of its obligations hereunder to the extent such obligations are dependent on such performance. Customer represents and warrants that (a) it owns and controls, directly or indirectly, all of the Customer Facilities that will be accessed to provide the Services, or that all such Facilities are provided for Customer's use by a third party, (ii) it has authorized Foundstone to access such Facilities to perform the Services, (iii) it has full power and authority to engage and direct Foundstone to access Customer Facilities and to conduct the Services, and, (iv) except as has been obtained previously, no consent, approval, authorization or other notice to a third party (including but not limited to employees, contractors, sub-contractors, and other entities with access to Customer's Facilities) are required in connection with Foundstone's performance of the Services.
6. Proprietary Rights. Shall be in accordance with Section 8 of DIR Contract No. DIR-SDD-1855.
7. Non-Disclosure. Shall be in accordance with Section 9.H. of Appendix A to DIR Contract No. DIR-SDD-1855.
8. Warranty and Disclaimer shall be in accordance with Section 6.C. of Appendix A to DIR Contract No. DIR-SDD-1855. 9. Infringement Indemnity shall be in accordance with Section 9.A. of DIR Contract No. DIR-SDD-1855..
10. Limitation of Liability shall be in accordance with Section 9.K. of Appendix A to DIR Contract No. DIR-SDD-1855. 11. Terminations shall be in accordance with Section 10.B. of Appendix A to DIR Contract No. DIR-SDD-1855.



Statement of Work

14.

Customer:

SIGNED: _____ DATE: _____

NAME / TITLE: _____ / _____

Customer to initial one of the following:

_____ Customer will issue a purchase order in conjunction with the execution of this SOW and the services contemplated hereunder.

_____ Customer will **NOT** issue a purchase order in conjunction with the execution of this SOW and the services contemplated hereunder.

MOMENTUMCOM, INC. dba Solid Border on behalf of McAfee, Inc.:

SIGNED: _____ DATE: _____

NAME / TITLE: _____ / _____

Please sign and fax to Brad Miller, 800-887-9974 FAX