REQUEST FOR QUOTES (RFQ)

Best Value Analysis Process

Issue Date: March 31, 2020

Issuing Office: Oregon Department of Environmental Quality
("Authorized Purchaser" or "DEQ")

Authorized Contact:
(Authorized Representative)

Tempest Roberts, Procurement and Contract Specialist
700 NE Multnomah Street
Portland, Oregon 97232
(503) 229-6934
BIDSDEQ@deq.state.or.us

Service Category: IT Security Services – Incident Management

Issued to:

CGI Technologies & Solutions, Inc.	(# 8472)
CSG Government Solutions	(# 8470)
Deloitte	(# 8482)
Gartner Inc.	(# 8480)
The North Highland Company	(# 8477)
TEKsystems Global Services, LLC	(# 8478)
Point B Inc.	(# 8479)
CBIZ	(# 9415)

RESPONSE DUE DATE AND TIME : April 15, 2020 - 3:00 PM PT
(Offer Due Date and Time)

1. Introduction

The State of Oregon, Department of Environmental Quality (DEQ) as the Authorized Purchaser is issuing this RFQ for web application security testing. Web application security testing is a subcategory of IT security testing under State procurement. This RFQ solicits quotes, as binding price estimates, from the Consultants identified on page 1 for performing security testing services.

The web application security testing services under this RFQ are a critical part of the secure software development life cycle (SDLC) framework that will be used to strategically design and develop a customized, scalable cloud-based web application for the full implementation of the Oregon Clean Vehicle Rebate Program (OCVRP). The cloud-based rebate processing platform (online platform) will be designed, developed, and deployed by the Center for Sustainable Energy (CSE), DEQ's contractor for full implementation of the OCVRP.

Broadly, the security testing services described in this RFQ are to include (i) static evaluations of web application security; and (ii) dynamic evaluations of web application security. All contracted security testing services and examinations will be performed as third-party evaluations. The estimated term for the Work Order Contract (WOC) under this RFQ is May 1, 2020 through August 31, 2020.

2. Definitions

"ASVS" means the Application Security Verification Standard 4.0 (March 2019) published by the Open Web Application Security Project (OWASP)

"Cloud-based rebate processing platform" or **"online platform"** means a customized, scalable, and integrated web-based platform (web portal) for full implementation of the Program. The cloud-based rebate processing platform (or online platform) includes the complete and secure Rebate application processing system and its associated secure database, file storage and website. The platform will provide for secure (1) storage and retrieval of Program information assets; (2) generation of lists of Program participants approved for rebates, generation of lists of Program participants denied rebates, lists of rebate aware payment schedules and amounts, and lists of other financial data related to Rebate application processing; (3) DEQ access to the database and file storage with authorized permissions to allow data extraction for Program transparency, evaluation, and auditing purposes; (4) a Program statistics dashboard and (5) hosting of Program information, including (i) Program outreach and education content, (ii) Program FAQs, (iii) a list of the vehicles currently eligible for all types of rebates offered by the Program and the associated rebate amount per vehicle, and (iv) the Program Implementation Manual and the information contained therein.

"Dynamic evaluation" means the use of vulnerability signatures in manual or automated dynamic analysis tools to find security problems. Dynamic evaluation is designed to detect conditions indicative of a security vulnerability in a web application in its running state.

"Functional implementation" means (1) the definition, design, development, and successful testing of the temporary rebate application processing tool; (2) deployment of the temporary rebate application processing tool as a web application; (3) the evolution and maintenance of artifacts, products, and processes to ensure accurate, complete, and timely Rebate application processing of backlog using the temporary rebate application processing tool; and (4) the definition, design, development, and successful testing of the temporary rebate application processing tool.

"Full implementation" means (1) the launch of the online platform plus any and all required post-launch activities needed to ensure the active operation and security of the online platform; (2) the evolution and maintenance of artifacts, products, and processes to ensure accurate and complete Rebate application processing, including the processing of all post-launch rebate applications plus the processing of any remaining backlog; (3) the evolution and maintenance of artifacts, products, and processes to ensure the accurate and traceable delivery of Program rebates to approved Program participants; (4) the evolution and maintenance of artifacts, products, and processes to ensure that both Rebate application processing and rebate delivery are done in a timely manner; (5) the evolution and maintenance of artifacts, products, and processes to provide participation guidance to all Program participants and to any potential Program participant; and (6) the evolution and maintenance of artifacts, products, and processes to provide an extensive outreach campaign to encourage participation among vehicle dealerships and the general public with a priority of reaching low-income and disadvantaged communities. Throughout full implementation the Contractor will strictly follow the Program rules and will incorporate legislative changes to the Program rules into full implementation operations when authorized to do so.

"Launch" means the deployment of the secure online platform as a fully functional and secure web application. Pre-launch is the Program management phase before launch and is characterized by those activities, tasks, artifacts, products, and processes that are developed and executed prior to the launch of the online platform. Post-launch is the Program management phase after launch and is characterized by those activities, tasks, artifacts, products, and processes that are developed and executed after the launch of the online platform.

"OWASP" means the Open Web Application Security Project (https://www.owasp.org/). OWASP has published the Application Security Verification Standard 4.0 (March 2019) and the OWASP Testing Guide 4.0 (Sept 2014).

"Secure" means that the entire ecosystem in which a web application is embedded (i.e., the web application itself, the websites hosting the web application, the web services called by the web application, and all linkages between the web application, the websites, and the web services) have been subjected to web application security testing that is necessary and sufficient to protect Program information assets.

"Static evaluation" means the analysis of security architectural design, and information flows and data assets through the manual inspection and review of Program documents. Static evaluation reviews design conditions that may be indicative of primary security vulnerabilities. Static evaluation is performed with the web application in a non-running state.

"Testing" means conducting the necessary and sufficient operations, evaluations, and reviews to ensure that a web application meets defined usability and security criteria. Testing includes those tests associated with standard, software development life cycle practices (e.g., unit tests, validation and verification tests, etc.) as well as tests associated with web application security (e.g., penetration and vulnerability tests).

"Temporary rebate processing tool" means a temporary online and secure web application for the accurate and complete Rebate application processing of backlog.

3. General Background

In 2017, Governor Kate Brown signed Executive Order No. 17-21 which created a program to provide rebates to Oregonians who must meet all program requirements and who purchase particular types of zero-emission vehicles, including plug-in hybrid zero-emission vehicles, and other zero-emissions vehicles meeting the standards listed in OAR 340-270. The 2017 Oregon Legislature authorized DEQ, through the Environmental Quality Commission, to develop and implement the new program, now called the Oregon Clean Vehicle Rebate Program (OCVRP or Program).

On December 12, 2018, the Department of Administrative Services, Procurement Office on behalf of DEQ released a Request For Proposal (RFP) #DASPS-2219-18 seeking firms to market, implement, administer, and represent DEQ with respect to the Program. On September 23, 2019 DEQ and the Center for Sustainable Energy (CSE) signed Contract #DASPS-1536-19/DEQ#041-20 that enables CSE to provide full implementation of the Program. Full implementation includes the design, development, and deployment of a cloud-based rebate processing platform (online platform). The online platform is a web application that, in addition to hosting Program information, will enable CSE to continuously process all new, Program applicants for Program rebates. With the online platform, Program applicants will be able to apply online and submit documents in an electronic format. Applicant information subsequently will be stored and processed in a cloud-based system. Program rebate processing will include the submission and storage of sensitive personally identifiable information (PII), including household income data. CSE is expected to use standard, SDLC protocols for the design and development of the online platform, including unit testing, validation and verification testing, and user acceptance testing.

4. Web Application Security Testing Background

The online platform will consist of:

(i) a front-end web publishing and content management system built in Drupal and hosted on a secure Pantheon environment;

(ii) a set of front-end web forms built with the Salesforce Visualforce framework coupled to a user management and user authentication system built with Salesforce Communities;

(iii) a back-end workflow system built with Salesforce objects and Salesforce databases; and

(iv) a back-end system for the secure storage of documents built in Box. The data collected through the public-facing web forms will be stored in Salesforce and in Box.

The online platform will leverage the security and privacy-related features, audits, and certifications of Salesforce and Box. The Salesforce system will use secure password hashing functions for password encryption and user authentication. Data in transit from Box to Salesforce will be secured using https. Data at rest in Salesforce will be encrypted and secured through access control and permissions. Data at rest in Box will be encrypted and secured through access control and permissions.

The intent of the web application security testing under this RFQ is to verify that DEQ's system security requirements have been met by using a variety of static and dynamic evaluations. The specific security requirements to be verified are listed as Application Security Verification Level 2 requirements, detailed in the Application Security Verification Standard (ASVS) 4.0 (March 2019) published by the Open Web Application Security Project (OWASP). The dynamic evaluations to be selected are to be driven by risk assessment and threat modeling. The static evaluations are to be performed using a variety of Program documents; the dynamic evaluations are to be performed on a secure staging site that is equivalent in functionality to the production site for the online platform.

Per DEQ's Contract with CSE, DEQ will use a third-party, independent firm to perform pre-launch, web application security testing of the online platform; also per this Contract, CSE will provide pre-launch support for independent, third-party, web application security testing of the online platform. Pre-launch support includes access to design and development documentation as well as access to a secure staging site for testing. The design and development documentation includes a variety of contract deliverables including,

1. Contract Deliverable_4.1.2_Platform Requirements
2. Contract Deliverable_4.1.4_ Platform Prototype
3. Contract Deliverable_4.1.5_Platform Design
4. Contract Deliverable_4.1.6_UAT Readiness Report
5. Contract Deliverable_4.2.1_Test Plan
6. Contract Deliverable_4.2.2_Requirements Traceability Matrix
7. Contract Deliverbale_4.2.4_Deployment Readiness Report
8. Contract Deliverable_10.1.1_Program System Security Plan

5. Scope of Services

The specific assessments and activities that will be done in support of the web application security testing are detailed in Exhibit 1, Scope of Work. The services will include the following:

1. Static evaluation of web application security, including:
   a) Architectural design review
   b) Identification and classification of information flows and data assets
   c) Identification and classification of web application vulnerabilities

d) Identification of web application security threats and an evaluation of the likelihood and potential impact of each threat if exploited

2. Dynamic evaluation of web application security, including:
   a) Security testing objectives
   b) Test methods and evaluation of testing outcomes
   c) Dynamic security testing

3. Final assessment of web application security, including:
   a) Summary of web application security evaluations

Prior to the start of any web application evaluations, the consultant awarded a WOC resulting from this RFQ shall be required to sign a nondisclosure agreement with CSE. All third-party security testing shall be completed before the launch of the online platform, which is scheduled for July 2020.

6. Questions and Requests for Clarification

All questions and requests for clarification regarding this RFQ must be submitted in writing by e-mail to **DEQBIDS@deq.state.or.us** and must be received no later than **April 8, 2020 at 3:00 pm pt.**

DEQ may issue revisions, substitutions or clarifications of the RFQ. DEQ will send revisions, substitutions or clarifications, if any, electronically to the consultants identified on page 1 of this RFQ.

7. Quotation Submittal

Quotes must be received on or before the Offer Due Date and Time to the email address identified in Section 6 to be considered. Offers will be accepted by e-mail only.

Quotes will not be accepted after the Offer Due Date and Time. DEQ, in its sole discretion, may extend the Offer Due Date if it is in the best interest of DEQ.

8. Quotation Submittal Requirements

a. Quotes must include a detailed description of Offeror's proposed approach and methodologies for providing the Services, as defined in Exhibit 1, Scope of Work.

b. Quotes must include a description of Offeror's Key Persons assigned to do work under the WOC, other staff, and their experience.

c. Quotes must include a description of past projects Offeror has completed that are similar in scope to what is being requested in this RFQ. Similar in scope means (i) performing architectural design review; (ii) identifying and classifying information flows and data assets; (iii) identifying and classifying web application vulnerabilities; (iv) developing web application threat scenarios; (v) developing security testing objectives; (vi) defining test methods and rubrics for the evaluation of testing outcomes; (vii) performing dynamic vulnerability and penetration testing; (viii) evaluating static and dynamic evaluation data for security standards verification; and (ix) providing practical recommendations in cases of nonconformance for high-level security systems in business, commercial, or government facilities.

d. Quotes must include submission of the Pricing Sheet (Exhibit 2). The Pricing Sheet must be signed by an authorized representative of the Offeror.

e. Quotes must include 3 references using the Reference Check Form (Exhibit 3). Forms must be completed by the reference, returned to the Offeror and submitted with the quote. References should be from customers for whom Offeror has performed similar projects within the past five (5) years.

9. Evaluation and Award

Quote submissions will be reviewed to determine if all Submittal Requirements have been met. Those meeting the Submittal Requirements will be evaluated to determine the "Best Value" for the State. "Best Value" is based solely on the evaluator's determination of what best meets the needs of DEQ taking into account price as well as the following considerations:

- Experience
- Expertise, especially with Salesforce
- References
- Availability
- Resource capacity
- Cost

The Offeror with the most advantageous Offer will be awarded a contract in a form substantially similar to the Work Order Contract (WOC) attached as Exhibit C to consultants Master Price Service Agreement. DEQ may negotiate contract terms and conditions with the successful Offeror. DEQ may award all or a portion of the Services requested, in its sole discretion.

DEQ's determination is final. DEQ, in its sole discretion, may reject all Quotes or cancel this RFQ if it is in the best interest of DEQ.

10. Responsibilities of DEQ

DEQ's obligations, as set forth in Exhibit 1, Scope of Work shall be performed by DEQ in a timely and proper fashion in accordance with the requirements in Exhibit 1, Scope of Work, or as otherwise agreed upon between the Parties, to allow consultant to perform its obligations in a timely fashion.

11. Travel and Other Expenses

Unless otherwise agreed, DEQ will not reimburse consultant travel or other expenses, unless DEQ has preapproved expenses and only pursuant to the Oregon Accounting Manual: http://www.oregon.gov/das/Financial/Acctng/Documents/40.10.00.pdf

EXHIBIT 1
Scope of Work (SOW)

PART I: OVERVIEW

General Background

The Center for Sustainable Energy (CSE) is in Contract with DEQ for full implementation of the Oregon Clean Vehicle Rebate Program (Program). Full implementation includes the design, development, and deployment of a cloud-based rebate processing platform (online platform). The online platform is a web application that, in addition to hosting Program information, will enable CSE to continuously process Program applicants for Program rebates. With the online platform, Program applicants will be able to apply online and submit documents in an electronic format. Program rebate processing will include the submission and storage of sensitive personally identifiable information (PII), including household income data. CSE is expected to use standard, software development lifecycle (SDLC) protocols for the design and development of the online platform, including unit testing, validation and verification testing, and user acceptance testing.

The online platform will consist of:

(i) a front-end web publishing and content management system built in Drupal and hosted on a secure Pantheon environment;
(ii) a set of front-end web forms built with the Salesforce Visualforce framework coupled to a user management and user authentication system built with Salesforce Communities;
(iii) a back-end workflow system built with Salesforce objects and Salesforce databases; and
(iv) a back-end system for the secure storage of documents built in Box. The data collected through the public-facing web forms will be stored in Salesforce and in Box.

The online platform will leverage the security and privacy-related features, audits, and certifications of Drupal, Pantheon, Salesforce and Box. The Salesforce system will use secure password hashing functions for password encryption and user authentication. Data in transit from Box to Salesforce will be secured using https. Data at rest in Salesforce will be encrypted and secured through access control and permissions. Data at rest in Box will be encrypted and secured through access control and permissions.

Although CSE is responsible for the design, development, and deployment of the online platform, DEQ is charged with ensuring that the online platform adequately protects PII from losses of confidentiality. The online platform must preserve authorized restrictions on information access and disclosure, and include the means for protecting personal privacy as well as proprietary information data assets.

The consultant awarded a WOC resulting from this RFQ will define and perform a suite of security testing evaluations and methods that ensure that the online platform complies with contractually-stipulated security requirements. The contractually-stipulated security requirements are defined as (i) the Technical, System Security, and Financial Requirements detailed in Exhibit A-1; and (ii) the Application Security Verification Level 2 requirements, detailed in the Application Security Verification Standard (ASVS) 4.0 (March 2019) published by the Open Web Application Security Project (OWASP).

Deliverable Transmittal, Review, and Acceptance

The consultant shall transmit Deliverables in both hard-copy and electronic (.pdf) format to the DEQ Program Coordinator at the address below,

Bruce Marron, Program Coordinator
Dept. of Environmental Quality, Air Quality Division
700 NE Multnomah St., Ste 600
Portland, OR 97232-4100
E: Marron.Bruce@deq.state.or.us

P: 503-229-6610

Delivery dates for each Deliverable are set forth in this SOW and are subject to DEQ performing its responsibilities in a timely manner. The selected Consultant shall provide written notice to DEQ upon delivery of a completed Deliverable to DEQ. By no later than ten (10) business days after receipt of such notice DEQ will determine whether the Deliverable meets acceptance criteria. Acceptance criteria includes all requirements and specifications for Deliverables as described and defined in this SOW.

If DEQ determines that a Deliverable does not meet the acceptance criteria in any respect, DEQ will notify the consultant in writing and describe in reasonable detail DEQ's basis for rejection of the Deliverable. Upon receipt of DEQ's notice of non-acceptance consultant shall within ten (10) business days, modify or improve the Deliverable at consultant's sole expense so that the Deliverable meets the acceptance criteria in all respects, and then must notify DEQ in writing that it has completed such modifications or improvements and re-submit the Deliverable to DEQ. DEQ will then review the modified or improved Deliverable within five (5) business days of receipt of the consultant's delivery of the Deliverable. Failure of the Deliverable to meet the acceptance criteria in all respects after the second submission will constitute a default by consultant. In the event of such default, DEQ may either (i) notify consultant of such default and instruct consultant to modify or improve the Deliverable, or (ii) notify consultant of such default and pursue its remedies for default of the Contract.

PART II: TASKS AND DELIVERABLES

Task 1: Static Evaluation of Web Application Security

The objective of static evaluation is to produce a threat model for the online platform. A threat model is a web application risk assessment and can be used to identify potential vulnerabilities and to direct the specifics of dynamic security testing.

Building a threat model for the online platform requires the manual inspection and review of documents in four key areas. First, the online platform's architectural design must be evaluated. Second, the information flows and data assets to be handled by the online platform must be identified and classified. Third, the primary vulnerabilities that would be expected for the online platform must be compiled. And lastly, a set of web application threat scenarios must be developed based on the primary vulnerabilities.

The primary Program documents to be inspected and reviewed include,

1. Contract Deliverable_4.1.2_Platform Requirements
2. Contract Deliverable_4.1.4_ Platform Prototype
3. Contract Deliverable_4.1.5_Platform Design
4. Contract Deliverable_4.1.6_UAT Readiness Report
5. Contract Deliverable_4.2.1_Test Plan
6. Contract Deliverable_4.2.2_Requirements Traceability Matrix
7. Contract Deliverbale_4.2.4_Deployment Readiness Report
8. Contract Deliverable_10.1.1_Program System Security Plan

The contractually-stipulated security requirement documents include,

1. Technical, System Security, and Financial Requirements detailed in Exhibit A-1
2. ASVS 4.0 (March 2019) Level 2 requirements published by OWASP

Additional documents to be inspected and reviewed may include various DEQ records, including authorized decision documents and standard operating procedures.

Task 1.1 Architectural Design Review

The consultant shall review the primary Program documents and any additional materials requested by DEQ to determine if the architectural design of the online platform is consistent with the contractually-stipulated security requirements.

Task 1.1 Deliverables

Architectural Design Review Report. The consultant shall produce a document labeled, *Architectural Design Review Report*, which will document the review and evaluation of the architecture of the online platform as being consistent with the contractually-stipulated security requirements.

Task 1.2 Identification and Classification of Information Flows and Data Assets

The consultant shall review the primary Program documents and any additional materials requested by DEQ to identify the information flows and the data assets expected to pass through or to be maintained by the online platform. Once identified, the chosen MPSA Holder will classify the information flows and the data assets as to their PPI confidentiality impact level and security risk.

Task 1.2 Deliverables:

Information Flow and Data Asset Report. The consultant shall produce a document labeled, *Information Flow and Data Asset Classification Report*, that provides (i) the identification of information flows and data assets expected to pass through or to be maintained by the online platform during the post-launch period; and (ii) the classification of the identified information flows and data assets with respect to their PPI confidentiality impact level and security risk.

Task 1.3 Identification and Classification of Web Application Vulnerabilities

The consultantwill identify and classify potential vulnerabilities to the online platform, whether technical, operational, or managerial. Vulnerabilities are defined as security breaches that permit unauthorized access to data assets and enable the release or unauthorized use of PII or proprietary information data assets.

Task 1.3 Deliverables:

Security Risk Assessment Report. The consultant shall produce a document labeled, *Security Risk Assessment Report*, that details the identity, classification, type, and risk of potential vulnerabilities to the online platform.

Task 1.4 Web Application Security Threat Scenarios

The consultant shall adopt a realistic view of potential attack vectors from the perspective of an individual(s) intent on breaching, disrupting, or destroying the online platform. Using this perspective, the consultant shall develop a set of realistic threat scenarios or attack trees that shall be used to guide the selection of the methodologies, protocols, and evaluation rubrics used for subsequent dynamic evaluation of web application security.

Task 1.4 Deliverables:

Security Threat Scenarios Report. The consultant shall produce a document labeled*, Security Threat Scenarios Report*, that provides a set of realistic threat scenarios or attack trees that can be applied to the online platform. For each threat scenario or attack tree, the consultant shall provide (i) the rationale for selecting the threat scenario or attack tree; (ii) an explanation of the vulnerability exploited by the threat scenario or attack tree; and (iii) an assessment of the likelihood and potential impact to the agency if the threat be exploited.

Task 2: Dynamic Evaluation of Web Application Security

In the broadest sense, security testing has two objectives; first, to validate that security systems and controls operate as expected with few or no vulnerabilities; and second, to verify that security systems and controls meet the requirements as established for the web application. Detailed security testing objectives are used to define a security testing program.

Task 2.1: Security Testing Objectives

The consultant shall design and develop a set of security testing objectives given that (i) the online platform is expected to leverage the security systems and controls of third-party providers (Drupal, Pantheon, Salesforce, and Box); and (ii) must meet the contractually-stipulated security requirements.

Task 2.1: Deliverables

Security Testing Objectives Report. The consultant shall produce a document labeled, *Security Testing Objectives Report*, that defines the set of security testing objectives to be used for dynamic security evaluation of the online platform. Each objective shall be cross-referenced to one or more of the contractually-stipulated security requirements.

Task 2.2: Test Methods and Evaluation of Testing Outcomes

The consultant shall define and list the specific dynamic test methods (verification tests, validation tests, vulnerability test, penetration tests, automated tests, manual tests, etc.) that are necessary and sufficient to meet the security testing objectives defined by Task 2.1 above. Additionally, the consultant shall explain (i) the rationale for the use of any test method that is selected; (ii) the protocols for its deployment; and (iii) the rubrics used to determine whether the test outcome is a pass or fail event (i.e., a Bernoulli trial).

Task 2.2: Deliverables

Test Methods and Outcomes Report. The consultant shall produce a document labeled, *Test Methods and Outcomes Report*, that defines and lists the specific dynamic test methods that are necessary and sufficient to meet the security testing objectives defined by Task 2.1 above. Additionally, the document shall explain the rationale for the use of any test method that is selected, the protocols for its deployment, and the rubrics used to determine whether the test outcome is a pass or fail event (i.e., a Bernoulli trial).

Task 2.3: Dynamic Security Testing

The consultant shall perform all of the dynamic security tests that are listed in Task 2.2 above. For each dynamic security test performed the consultant shall document (i) the date and time of the test; (ii) all initial conditions and parameters in effect at the time of the test; (iii) the overview of the testing process; (iv) the exact details of the testing procedure; (v) the direct output(s) and results obtained from the test; and (vi) a professional evaluation (pass/fail) of the test.

Task 2.3: Deliverables

Security Testing Report. The consultant shall produce a document labeled, *Security Testing Report* that documents the results of all dynamic security tests applied to the online platform. For each dynamic security test performed, the *Security Testing Report* shall state (i) the date and time of the test; (ii) all initial conditions and parameters in effect at the time of the test; (iii) the overview of the testing process; (iv) the exact details of the testing procedure; (v) the direct output(s) and results obtained from the test; and (vi) a professional evaluation (pass/fail) of the test.

Task 2.4: Additional Dynamic Security Testing (Optional)

The consultant may, at DEQ's request, perform a second round of dynamic security testing. The second round of dynamic security testing would be limited to a subset of the dynamic security tests listed in Task 2.2 above. For each dynamic security test performed in the second round of dynamic security testing, the consultant shall document (i) the date and time of the test; (ii) all initial conditions and parameters in effect at the time of the test; (iii) the overview of the testing process; (iv) the exact details of the testing procedure; (v) the direct output(s) and results obtained from the test; and (vi) a professional evaluation (pass/fail) of the test.

Task 2.4: Deliverables

Supplemental Security Testing Report. If requested to do so, the consultant will produce a document labeled, *Supplemental Security Testing Report* that documents the results of a second round of dynamic security tests applied to the online platform. For each dynamic security test performed in the second round of testing, the *Supplemental Security Testing Report* shall state (i) the date and time of the test; (ii) all initial conditions and parameters in effect at the time of the test; (iii) the overview of the testing process; (iv) the exact details of the testing procedure; (v) the direct output(s) and results obtained from the test; and (vi) a professional evaluation (pass/fail) of the test.

Task 3: Final Assessment of Web Application Security

Ultimately, the outcomes of all evaluations of web application security, both static and dynamic, must be summarized and synthesized in order to answer the question: Does the current configuration of the online platform comply with contractually-stipulated security requirements or not?

Task 3.1: Summary of Web Application Security Evaluations

The consultant shall summarize and synthesize the results from the *Architectural Design Review Report,* the *Security Risk Assessment Report,* the *Security Testing Report*, and, if produced, the *Supplemental Security Testing Report.* The consultant shall compare the summarized and synthesized results to the contractually-stipulated security requirements. The consultant shall provide a professional assessment of whether or not the current configuration of the online platform does or does not meet each of the contractually-stipulated security requirements.

Task 3.1 Deliverable

Final Security Assessment Report. The consultant shall shall produce a document labeled, *Final Security Assessment Report*, that summarizes and synthesizes the results from the *Architectural Design Review Report,* the *Security Risk Assessment Report,* the *Security Testing Report*, and, if available, the *Supplemental Security Testing Report.* The *Final Security Assessment Report* shall provide a professional assessment of whether or not the current configuration of the online platform does or does not meet each of the contractually-stipulated security requirements. In the event that a contractually-stipulated requirement is not met, the *Final Security Assessment Report* shall provide recommendations and possible solutions for resolution of the nonconformance.

EXHIBIT 2
Pricing Sheet

Deliverable Number	Description	Proposed Completion Date	Proposed Hours for Completion	Proposed Cost
1.1	Architectural Design Review Report			
1.2	Information Flow and Data Asset Report			
1.3	Security Risk Assessment Report			
1.4	Security Threat Scenarios Report			
2.1	Security Testing Objectives Report			
2.2	Test Methods and Outcomes Report			
2.3	Security Testing Report			
2.4	Supplemental Security Testing Report (optional)			
3.1	Final Security Assessment Report			
TOTAL MAXIMUM NOT-TO-EXCEED COST				

EXHIBIT 3
Reference Check Form

Offeror Name: ______________________________

Reference Entity: ______________________________

Reference Contact Name: ______________________________

Contact Telephone Number: ______________________________

Please respond to the following questions.

Score: 1-5 for each response.

1. Detailed description of Qualifying Engagement.

   Score:

   Comments:

2. Offeror’s role and functional area of Qualifying Engagement.

   Score:

   Comments:

3. Description of technical environment and complexity.

   Score:

   Comments:

4. Description comparing Qualifying Engagement to RFQ Scope of Work.

   Score:

   Comments:

5. If given the opportunity, how likely would you use Offeror’s services again?

   Score:

   Comments: