



**CONSULTING AND TECHNICAL SERVICES II (CATS II)**

**TASK ORDER REQUEST FOR PROPOSALS (TORFP)**

**WEB APPLICATION SECURITY ASSESSMENT**

**CATS II TORFP # E00P2400385**

**COMPTROLLER OF MARYLAND**

**ISSUE DATE: MAY 24, 2012**

## TABLE OF CONTENTS

<b>SECTION 1 - ADMINISTRATIVE INFORMATION .....</b>	<b>5</b>
1.1 RESPONSIBILITY FOR TORFP AND TO AGREEMENT .....	5
1.2 TO AGREEMENT .....	5
1.3 TO PROPOSAL SUBMISSIONS .....	5
1.4 MINORITY BUSINESS ENTERPRISE (MBE) .....	5
1.5 CONFLICT OF INTEREST .....	5
1.6 NON-DISCLOSURE AGREEMENT .....	6
1.7 LIMITATION OF LIABILITY CEILING.....	6
1.8 CONTRACT MANAGEMENT OVERSIGHT ACTIVITIES .....	6
<b>SECTION 2 - SCOPE OF WORK .....</b>	<b>7</b>
2.1 PURPOSE.....	7
2.2 REQUESTING AGENCY BACKGROUND .....	7
2.3 ROLES AND RESPONSIBILITIES .....	7
2.4 PROJECT BACKGROUND AND DESCRIPTION .....	8
2.5 REQUIREMENTS.....	8
2.5.1 GENERAL REQUIREMENTS .....	8
2.5.2 REQUIREMENTS.....	8
2.6 DELIVERABLES.....	10
2.6.1 DELIVERABLE SUBMISSION PROCESS .....	10
2.6.2 DELIVERABLE DESCRIPTIONS / ACCEPTANCE CRITERIA .....	11
2.7 REQUIRED PROJECT POLICIES, GUIDELINES AND METHODOLOGIES .....	13
2.8 TO CONTRACTOR PERSONNEL MINIMUM QUALIFICATIONS .....	16
2.9 TO CONTRACTOR MINIMUM QUALIFICATIONS .....	16
2.10 TO CONTRACTOR REQUIRED EXPERTISE .....	16
2.11 INVOICING .....	17
2.11.1 INVOICE SUBMISSION PROCEDURE .....	17
2.12 MBE PARTICIPATION REPORTS .....	18
<b>SECTION 3 - TASK ORDER PROPOSAL FORMAT AND SUBMISSION REQUIREMENTS .....</b>	<b>19</b>
3.1 REQUIRED RESPONSE .....	19
3.2 FORMAT .....	19
3.2.1 TECHNICAL PROPOSAL.....	19
3.2.2 FINANCIAL RESPONSE .....	21
<b>SECTION 4 – TASK ORDER AWARD PROCESS .....</b>	<b>22</b>
4.1 OVERVIEW .....	22
4.2 TECHNICAL PROPOSAL EVALUATION CRITERIA.....	22
4.3 SELECTION PROCEDURES .....	22
4.4 COMMENCEMENT OF WORK UNDER A TOA .....	22
<b>ATTACHMENT 2 – MINORITY BUSINESS ENTERPRISE FORMS .....</b>	<b>24</b>
<b>ATTACHMENT 4 – CONFLICT OF INTEREST AFFIDAVIT AND DISCLOSURE .....</b>	<b>36</b>
<b>ATTACHMENT 5 – LABOR CLASSIFICATION PERSONNEL RESUME SUMMARY .....</b>	<b>37</b>
<b>ATTACHMENT 6 – DIRECTIONS .....</b>	<b>39</b>
<b>ATTACHMENT 7 – NOTICE TO PROCEED .....</b>	<b>40</b>
<b>ATTACHMENT 8 – AGENCY RECEIPT OF DELIVERABLE FORM.....</b>	<b>41</b>
<b>ATTACHMENT 9 – AGENCY ACCEPTANCE OF DELIVERABLE FORM.....</b>	<b>42</b>

**ATTACHMENT 10 – NON-DISCLOSURE AGREEMENT (OFFEROR) .....43**  
**ATTACHMENT 11 – NON-DISCLOSURE AGREEMENT (TO CONTRACTOR).....44**  
**ATTACHMENT 12 – TO CONTRACTOR SELF-REPORTING CHECKLIST .....46**  
**ATTACHMENT 13 – LIVING WAGE AFFIDAVIT OF AGREEMENT .....49**  
**ATTACHMENT 14 – ADDITIONAL MANDATORY CONTRACT PROVISIONS .....50**  
**EXHIBIT A .....52**

## KEY INFORMATION SUMMARY SHEET

This Consulting and Technical Services II (CATS II) Task Order Request for Proposals (TORFP) is issued to obtain the services necessary to satisfy the requirements defined in Section 2 - Scope of Work. All CATS II Master Contractors approved to perform work in the functional area under which this TORFP is released are invited to submit a Task Order (TO) Proposal to this TORFP. Master Contractors choosing not to submit a proposal must submit a Master Contractor Feedback form. The form is accessible via, your CATS II Master Contractor login screen and clicking on TORFP Feedback Response Form from the menu. In addition to the requirements of this TORFP, the Master Contractors are subject to all terms and conditions contained in the CATS II RFP issued by the Maryland Department of Information Technology and subsequent Master Contract Project Number 060B9800035, including any amendments.

<b>TORFP Title:</b>	Web Application Security Assessment
<b>Functional Area:</b>	<b>Functional Area 2 - Web and Internet Systems</b>
<b>TORFP Issue Date:</b>	05/24/2012
<b>Closing Date and Time for Proposals:</b>	06/18/2012 at 3:00 PM
<b>TORFP Issuing Agency:</b>	Comptroller of Maryland, Information Technology Division
<b>Closing Date for Questions:</b>	06/06/2012 at 3:00 PM
<b>Send Questions and Proposals to:</b>	Lavinia Lee <a href="mailto:TORFPWEB-P2400385@comp.state.md.us">TORFPWEB-P2400385@comp.state.md.us</a>
<b>TO Procurement Officer:</b>	Lavinia Lee Office Phone Number: 410-260-7503 Office FAX Number: 410-974-2762
<b>TO Manager:</b>	David Hildebrand Office Phone Number: 410-260-7768 Office FAX Number: 410-974-2762
<b>TO Project Number:</b>	E00P2400385
<b>TO Type:</b>	Fixed Price
<b>Period of Performance:</b>	Not-to-exceed 9 months from Notice to Proceed
<b>MBE Goal:</b>	10 Percent
<b>Small Business Reserve (SBR):</b>	No
<b>Primary Place of Performance:</b>	Comptroller of Maryland Annapolis Data Center 108 Carroll St Annapolis, MD 21404
<b>TO Pre-proposal Conference:</b>	Comptroller of Maryland Annapolis Data Center 108 Carroll St, Room 407A Annapolis, MD 21404 05/31/2012 at 10:00 AM See Attachment 6 for directions.

## SECTION 1 - ADMINISTRATIVE INFORMATION

### 1.1 RESPONSIBILITY FOR TORFP AND TO AGREEMENT

The TO Procurement Officer has the primary responsibility for the management of the TORFP process, for the resolution of TO Agreement (TOA) scope issues, and for authorizing any changes to the TOA.

The TO Manager has the primary responsibility for the management of the work performed under the TOA; administration functions, including issuing written directions; ensuring compliance with the terms and conditions of the CATS II Master Contract; and, in conjunction with the selected Master Contractor, achieving on budget/on time/on target (e.g., within scope) completion of the Scope of Work.

### 1.2 TO AGREEMENT

Based upon an evaluation of TO Proposal responses, a Master Contractor will be selected to conduct the work defined in Section 2 - Scope of Work. A specific TOA, Attachment 3, will then be entered into between the State and the selected Master Contractor, which will bind the selected Master Contractor (TO Contractor) to the contents of its TO Proposal, including the price proposal.

### 1.3 TO PROPOSAL SUBMISSIONS

The TO Procurement Officer will not accept submissions after the date and exact time stated in the Key Information Summary Sheet above. The date and time of submission is determined by the date and time of arrival in the TO Procurement Officer's e-mail box. The TO Proposal is to be submitted via e-mail as two attachments in MS Word format. The "subject" line in the e-mail submission shall state the TORFP #E00P2400385. The first file will be the TO Proposal technical response to this TORFP and titled, "CATS II TORFP #E00P2400385 Technical". The second file will be the financial response to this CATS II TORFP and titled, "CATS II TORFP #E00P2400385 Financial". The following proposal documents must be submitted with required signatures as .PDF files with signatures clearly visible:

- Attachment 1 – Price Proposal
- Attachment 2 - MBE Forms D-1 and D-2
- Attachment 4 - Conflict of Interest and Disclosure Affidavit
- Attachment 13 – Living Wage Affidavit of Agreement

### 1.4 MINORITY BUSINESS ENTERPRISE (MBE)

A Master Contractor that responds to this TORFP shall complete, sign, and submit all required MBE documentation (Attachment 2 - Forms D-1 and D-2) at the time it submits its TO Proposal. **Failure of the Master Contractor to complete, sign, and submit all required MBE documentation at the time it submits its TO Proposal will result in the State's rejection of the Master Contractor's TO Proposal.**

### 1.5 CONFLICT OF INTEREST

The TO Contractor awarded the TO Agreement shall provide IT technical and/or consulting services for State agencies or component programs with those agencies, and must do so impartially and without any conflicts of interest. Each Master Contractor shall complete and include a Conflict of Interest Affidavit and Disclosure in the form included as Attachment 4 this TORFP with its TO Proposal. If the TO Procurement Officer makes a determination that facts or circumstances exist that give rise to or could in the future give rise to a conflict of interest within the meaning of COMAR 21.05.08.08A, the TO Procurement Officer may reject a Master Contractor's TO Proposal under COMAR 21.06.02.03B.

Master Contractors should be aware that the State Ethics Law, State Government Article, §15-508, might limit the selected Master Contractor's ability to participate in future related procurements, depending upon specific circumstances.

## **1.6 NON-DISCLOSURE AGREEMENT**

Certain system documentation is available for potential Offerors to review at a reading room at Comptroller of Maryland, 108 Carroll St, Annapolis, MD 21404. Offerors who review such documentation shall be required to sign a Non-Disclosure Agreement (Offeror) in the form of Attachment 10. The documentation is available by appointment for review from **May 31, 2012** (date of pre-proposal conference) until **June 6, 2012** (close date for questions). Please contact the TO Procurement Officer of this TORFP to schedule an appointment.

In addition, certain documentation may be required by the TO Contractor awarded the TOA in order to fulfill the requirements of the TOA. The TO Contractor, employees and agents who review such documents shall be required to sign, including but not limited to, a Non-Disclosure Agreement (TO Contractor) in the form of Attachment 11.

## **1.7 LIMITATION OF LIABILITY CEILING**

Pursuant to Section 27 (C) of the CATS II Master Contract, the limitation of liability per claim under this TORFP shall not exceed the total TOA amount.

## **1.8 CONTRACT MANAGEMENT OVERSIGHT ACTIVITIES**

Department of Information Technology (DoIT) is responsible for contract management oversight on the CATS II Master Contract. As part of that oversight, DoIT has implemented a process for self-reporting contract management activities of CATS II TOs. This process shall typically apply to active TOs for operations and maintenance services valued at \$1 million or greater, but all CATS II TOs are subject to review.

Attachment 12 is a sample of the TO Contractor Self-Reporting Checklist. DoIT will send initial checklists out to applicable TO Contractors approximately three (3) months after the award date for a TO. The TO Contractor shall complete and return the checklist as instructed on the checklist. Subsequently, at six (6) month intervals from the due date on the initial checklist, the TO Contractor shall update and resend the checklist to DoIT.

## SECTION 2 - SCOPE OF WORK

### 2.1 PURPOSE

The Comptroller of Maryland (COM) is issuing this CATS II TORFP to obtain a web application security assessment by analyzing the code and testing the resiliency of three (3) specific Internet-facing online services, as described in this solicitation, against threats, penetration and potential data loss or exposure. Two (2) services are in production and one (1) is under development and testing.

A comprehensive written report shall be provided that indicates the assessment methodology used, analysis details, and findings that support each conclusion and recommended action. The report shall include a management summary of findings and recommendations.

An oral presentation of findings to management shall also be provided. Both the written and oral reports, supporting information, output of any tools utilized, draft documents, and the contents thereof, shall remain confidential and shall not be disclosed to any third party without the express written consent of the TO Manager.

The Agency is seeking one TO Contractor to perform all services and produce all deliverables requested in this TORFP.

### 2.2 REQUESTING AGENCY BACKGROUND

The principal duty of the COM is to collect taxes. The major revenue sources are individual income taxes, business income taxes, and sales and use taxes. The Agency also collects taxes on motor fuel, estates, admissions and amusement, alcohol, and tobacco. The Agency tests motor fuel to ensure the quality of the product for the consumer. Acting as Maryland's chief accountant, the Comptroller pays the State's bills, maintains its books, prepares financial reports, and pays State employees. The COM's Annapolis Data Center also provides information technology services for many State agencies. The Agency also provides information technology support for the 24 Register of Wills offices and the Board of Public Works. The Agency's main headquarters are located in Annapolis, Maryland with 11 branch offices throughout the State.

### 2.3 ROLES AND RESPONSIBILITIES

**TO Procurement Officer** - The Agency TO Procurement Officer shall serve as the sole point of contact for any questions arising out of the issuance of this TORFP; make the final recommendation for award of a TO resulting from this TORFP; identify and appoint all State points of contact associated with the resulting TO; negotiate and approve any Change Orders to the TO resulting from this TORFP; and render any final decision on the part of the State regarding any conflicts with respect to deliverables and payments.

**TO Manager** - The TO Manager shall serve as the initial and primary contact on issues relating to the TO and shall serve as the primary contact on issues relating to deliverables and payments.

Pursuant to this TORFP and in the event a TO Agreement is reached, the parties agree to the following:

- A. The Agency will provide the TO Contractor with all applicable application code and documentation, access privileges, contact information, and any additional information necessary for testing to proceed as described in this TORFP.
- B. The TO Contractor shall perform all services and produce all deliverables described in this TORFP.

**TO Contractor** - The parties to any TO Agreement issued pursuant to this TORFP are required to carefully safeguard any and all confidential information produced, provided and/or exchanged, which includes all communications – in any form. In order to successfully accomplish this requirement, any and all written communications produced by the TO Contractor as a result of the TO Agreement shall be deemed confidential and shall be so labeled on every page of every document.

Unless specifically authorized in writing by the TO Procurement Officer and the TO Manager, the TO Contractor shall not reference, discuss, or disclose information related to this TORFP with a limited exception for information that has been directly and intentionally released to the general public by the Agency (e.g., this TORFP or published Notice of Award). In addition, the TO Contractor shall not reference or disclose work performed or conducted pursuant to this TORFP in any communication that is not specifically and directly related to the services and deliverables required by this TORFP, which shall preclude the disclosure of any such information or materials to other State agencies or departments.

The TO Contractor shall designate a single individual to serve as its primary contact on contract-related and delivery-related matters.

## 2.4 PROJECT BACKGROUND AND DESCRIPTION

The COM is continuously striving to meet the needs of taxpayers by providing Internet applications that not only provide convenience, but improve the quality and accuracy of the information collected, while reducing processing costs. It is critical that these applications are secure and that the taxpayers can trust that their sensitive data is kept confidential. In order to accomplish this, we are seeking a highly qualified third-party to assess the applications risks.

## 2.5 REQUIREMENTS

### 2.5.1 GENERAL REQUIREMENTS

The focus of this TO is the following:

- TO Contractor shall provide a detailed assessment of the application code, coding techniques, and database methodology;
- TO Contractor shall conduct testing of the applications and database by using various test scenarios;
- TO Contractor shall perform penetration testing from both internal and external to the network;
- TO Contractor shall provide both a detailed report and management summary of the findings;
- TO Contractor shall provide detailed recommendations to help mitigate potential risks; and
- TO Contractor shall provide training of COM employees in secure coding best practices.

### 2.5.2 REQUIREMENTS

1	<p>TO Contractor shall conduct a web application security assessment on the following applications by analyzing the code and testing each application’s ability to (1) withstand an internal or external attack and (2) tolerate application failures and exception processing that could create a security breach situation.</p> <ul style="list-style-type: none"><li>▪ <b>iFile</b><ul style="list-style-type: none"><li>○ Registration</li><li>○ 2011 Resident Maryland Tax Return</li><li>○ 2011 Nonresident Maryland Tax Return</li></ul></li></ul>
---	---



	<ul style="list-style-type: none"> <li>○ 2012 Personal Estimated Payment - Form 502D</li> <li>○ 2011 Automatic Extension Payment - Form 502E</li> <li>○ Bill Payment (Individual taxes)</li> <li>○ 1099G Previous Year Refund Inquiry</li> <li>○ Estimated Payment Inquiry</li> <li>▪ <b>bFile</b> <ul style="list-style-type: none"> <li>○ Registration (New and Old)</li> <li>○ File Sales And Use Tax Returns</li> <li>○ File Withholding Returns (MW506)</li> <li>○ File Withholding Reconciliation (data-entry application and bulk upload application)</li> <li>○ Bill Payment (Business taxes)</li> </ul> </li> <li>▪ <b>pServices</b> <ul style="list-style-type: none"> <li>○ Registration</li> <li>○ 1099G</li> </ul> </li> </ul>
2	TO Contractor shall conduct full internal and external penetration (PEN) tests for the 3 Internet-facing online services to identify potential security vulnerabilities and provide steps for remediation of the identified security vulnerabilities. The methodologies, tools and equipment that are planned for use for the penetration test shall be provided and approved by COM.
3	TO Contractor shall conduct a manual review of source code for the 3 Internet-facing online services to identify issues in the source code (including insecure coding practices) that may allow an attacker to compromise the application or business functionality. Any tools used by TO Contractor to assist with the review shall be provided and approved by COM.
4	<p>TO Contractor shall identify any potential security vulnerabilities or data exposures for the 3 Internet-facing online services during normal application run-time and during an application failure. The application-level security assessments shall address at a minimum the Open Web Application Security Project (OWASP) Application Security Verifications which includes:</p> <ol style="list-style-type: none"> <li>1. Security Architecture</li> <li>2. Authentication</li> <li>3. Session Management</li> <li>4. Access Control</li> <li>5. Input Validation</li> <li>6. Output Encoding/Escaping</li> <li>7. Cryptography</li> <li>8. Error Handling and Logging</li> <li>9. Data Protection</li> <li>10. Communication Security</li> <li>11. HTTP Security</li> <li>12. Security Configuration</li> <li>13. Malicious Code Search</li> </ol>

	14. Internal Security
5	TO Contractor shall identify any potential risks to taxpayer confidential data for the 3 Internet-facing online services, which may include federal tax information (FTI), within the applications, business logic, database and batch processes.
6	TO Contractor shall conduct a review of the databases for the 3 Internet-facing online services to identify any security exposures or possibilities of data loss or leakage.
7	TO Contractor shall provide detailed steps for remediation of all identified security vulnerabilities.
8	TO Contractor shall provide COM technical training on the current best methodologies to incorporate security during the Software Development Life Cycle, and the industry-accepted best practices for secure coding and building secure databases.
9	At COM's sole discretion and after the remediation process has been completed by COM, the TO Contractor may be requested to validate the remediated code and certify the application at an OWASP Level 4. (See Deliverable ID 2.6.2.7 on Price Proposal Form)
10	TO Contractor shall conduct weekly status report meetings.

## 2.6 DELIVERABLES

### 2.6.1 DELIVERABLE SUBMISSION PROCESS

For each deliverable, the TO Contractor shall submit to the TO Manager the appropriate document(s).

Drafts of all final deliverables are required at least two (2) weeks in advance of when all final deliverables are due. Written deliverables defined as draft documents must demonstrate due diligence in meeting the scope and requirements of the associated final written deliverable. A written draft must:

- A) Be presented in a format appropriate for the subject matter and depth of discussion.
- B) Be organized in a manner that presents a logical flow of the deliverable's content.
- C) Represent factual information reasonably expected to have been known at the time of submittal.
- D) Present information that is relevant to the Section of the deliverable being discussed.
- E) Represent a significant level of completeness towards the associated final written deliverable that supports a concise final deliverable acceptance process.

Upon completion of a deliverable, the TO Contractor shall document each deliverable in final form to the TO Manager for acceptance. The TO Contractor shall document such delivery in an Agency Receipt of Deliverable Form (Attachment 8). The TO Manager shall countersign the Agency Receipt of Deliverable Form indicating receipt of the contents described therein.

Upon receipt of a final deliverable, the TO Manager shall commence a review of the deliverable as required to validate the completeness and quality in meeting requirements. Upon completion of validation, the TO Manager shall issue to the TO Contractor notice of acceptance or rejection of the deliverables in an Agency Acceptance of Deliverable Form (Attachment 9). In the event of rejection, the TO Contractor shall correct the identified deficiencies or non-conformities. Subsequent project tasks may not continue until deficiencies with a deliverable are rectified and accepted by the TO Manager or the TO Manager has specifically issued, in writing, a waiver for conditional continuance of project tasks. Once the State's issues have been addressed and resolutions are accepted by the TO Manager, the TO Contractor will incorporate the resolutions into the deliverable and resubmit the deliverable for acceptance. Accepted deliverables shall be invoiced within 30 calendar days in the applicable invoice format (Reference 2.10 Invoicing).

A written deliverable defined as a final document must satisfy the scope and requirements of this TORFP for that deliverable. Final written deliverables must:

- A) Be presented in a format appropriate for the subject matter and depth of discussion.

- B) Be organized in a manner that presents a logical flow of the deliverable’s content.
- C) Represent factual information reasonably expected to have been known at the time of submittal.
- D) Present information that is relevant to the Section of the deliverable being discussed.

The State required deliverables are defined below. Within each task, the TO Contractor may suggest other subtasks or deliverables to improve the quality and success of the project.

### 2.6.2 DELIVERABLE DESCRIPTIONS / ACCEPTANCE CRITERIA

ID #	Deliverable Description	Acceptance Criteria	Due Date / Timeframe
2.6.2.1	Detailed Project Management Plan	<p>The Project Management Plan shall outline the approach, and methodology the TO Contractor will use to conduct the required web applications security assessment and formulate the comprehensive security recommendations. The project plan shall also include the following sub-plans:</p> <ul style="list-style-type: none"> <li>• Schedule Management Plan</li> <li>• Scope Management Plan</li> <li>• Quality Control Management Plan</li> <li>• Staffing Management Plan</li> <li>• Communication Management Plan</li> <li>• Risk Management Plan</li> <li>• Change Management Plan</li> </ul> <p>The project management plan shall also include a detailed description of the tools/equipment, methodology employed. The methodology has to be agreed on by the Comptroller’s technical staff. If the TO Contractor anticipates that it will require any Agency resources to complete the services and produce the deliverables, this information shall be stated in the project plan. The Detailed Project Management Plan has to be approved by Comptroller’s Project Manager before proceeding with the risk assessment.</p>	NTP1 + 15 Calendar days
2.6.2.2	Project Schedule and Work Breakdown Structure	<p>The project schedule shall provide timelines and milestones; detail event sequencing that explains work details and the date/time and duration estimates, and resources for both the TO Contractor and COM. The project schedule shall track target and actual date/time for tasks. The WBS should reflect the chronology of tasks without assigning specific time frames or start / completion dates. The WBS may include tasks to be performed by the State or third parties as appropriate, for example, independent quality assurance tasks. The project schedule and WBS shall be reviewed weekly during the Weekly Status Meetings (see deliverable 2.6.2.7) and used to monitor project performance. The project schedule shall be updated weekly to monitor target to actual for date/time and tasks.</p>	NTP1 + 15 Calendar days
2.6.2.3	Project Risk Assessment	<p>The Project Risk Assessment shall identify and prioritize the risks inherent in meeting the requirements in Section 2 - Scope of Work. The Assessment shall include a description of strategies to mitigate risks. The Risk Assessment shall be reviewed, updated and managed by the process defined in the</p>	NTP1 + 30 Calendar days

		Risk Management Plan (see deliverable 2.6.2.1).	
2.6.2.4	Penetration Test Reports	<p>At the conclusion of the penetration tests, TO Contractor shall produce reports that describe the tools, methodologies, findings, and recommendations for remediation. An oral presentation providing an overview of the reports is also required. The documentation shall include:</p> <p><b>DETAILED TECHNICAL REPORT</b>  A document developed for the use of COM technical staff which discusses: the tools and 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.</p> <p><b>EXECUTIVE SUMMARY REPORT</b>  A document developed to summarize the scope, approach, findings and recommendations, in a manner suitable for senior management.</p>	NTP1 + 60 Calendar days
2.6.2.4	Web Applications Security Assessment Reports	<p>At the conclusion of the web applications security assessment, the TO Contractor shall produce reports that describe the approach, findings, and recommendations for remediation for each application. Oral presentations of the report are also required. The documentation should include:</p> <p><b>DETAILED TECHNICAL REPORTS</b>  A document developed for each application 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. Each document shall be sufficiently detailed so it may be used by the COM technical staff to remediate the vulnerabilities.</p> <p><b>EXECUTIVE SUMMARY REPORT</b>  A document developed to summarize the scope, approach, findings and recommendations, in a manner suitable for senior management.</p>	NTP1 + 120 Calendar days
2.6.2.5	Training	<p>TO Contractor shall provide on-site formal software development and coding security training of at least one week for ten employees. Examples of training topics from Software Assurance Forum for Excellence in Code (SAFECode) include techniques such as using threat modeling, least privilege, and sandboxing techniques, minimizing the use of unsafe string and buffer functions; validating input/output; using robust integer operations for dynamic memory allocations and array offsets; using anti-cross site scripting (XSS) libraries; using canonical data formats; avoiding string concatenation for dynamic SQL statements; using strong cryptography; using logging and tracing; testing recommendations to determine attack surfaces; using appropriate testing tools; fuzzing and robustness testing; penetration testing; and using a current compiler toolset, and static analysis tools. Successful completion of training shall be demonstrated by a report that indicates who was trained, training topics, duration of training,</p>	NTP1 + 130 Calendar days

		and date trained.	
2.6.2.6	Weekly Status Reports and Meetings	The TO Contractor shall conduct weekly status meetings. A weekly project status report shall be submitted after the end of each weekly period and prior to the weekly status meeting and shall contain at a minimum the work accomplished during the weekly period, progress made on the deliverables, problems/issues, and planned activities for next week. Weekly status reports and meetings shall provide a forum to discuss issues, identify action items and track project progress.	NTP1 + 15 Calendar days, and weekly thereafter until project end date
<b>OPTIONAL SERVICES</b>			
2.6.2.7	Validation and Certification (Optional)	After remediation has been completed by the COM and at COM's sole discretion, COM may request the TO Contractor to validate and certify the applications. If COM elects to exercise this optional deliverable, COM will issue a notice-to-proceed for this optional deliverable to the TO Contractor. The applications shall be certified to Level 4 of the Application Security Verification Standard (ASVS) OWASP.	NTP2 for Optional Deliverable + 30 Calendar days

## 2.7 REQUIRED PROJECT POLICIES, GUIDELINES AND METHODOLOGIES

In providing services and producing deliverables pursuant to this TORFP, the TO Contractor shall be familiar with and will be held accountable to the standards set forth in the following resources. Failure to comply with and perform pursuant to such standards may be deemed a breach of the TO Agreement by the TO Contractor. The TO Contractor shall be required to comply with all applicable laws, regulations, policies, standards, and guidelines affecting information technology projects, which may be created or changed periodically. The TO Contractor shall adhere to and remain abreast of current, new, and revised laws, regulations, policies, standards, and guidelines affecting project execution. The following policies, guidelines and methodologies can be found at <http://doit.maryland.gov/policies/Pages/ContractPolicies.aspx> under "Policies and Guidance." These may include, but are not limited to:

- The State's System Development Life Cycle (SDLC) methodology
- The State Information Technology Security Policy and Standards
- The State Information Technology Project Oversight
- The State of Maryland Enterprise Architecture
- The TO Contractor shall follow the project management methodologies that are consistent with the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK) Guide. TO Contractor's staff and sub Contractors are to follow a consistent methodology for all TO activities.
- Maryland Department of Information Technology – System Development Life Cycle <http://doit.maryland.gov/SDLC/Pages/SDLCHome.aspx>
- Technical Guide to Information Security Testing and Assessment NIST SP800-15 <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>
- IRS Publication 1075 – Tax Information Security Guidelines For Federal, State and Local Agencies <http://www.irs.gov/pub/irs-pdf/p1075.pdf>
- Maryland Department of Information Technology – Information Security Policy v\_2.3 Sept. 2010 [http://doit.maryland.gov/support/Documents/security\\_guidelines/DoITSecurityPolicy.pdf](http://doit.maryland.gov/support/Documents/security_guidelines/DoITSecurityPolicy.pdf)
- Open Web Application Security Project - A Guide to Building Secure Web Applications and Web Services (v. 2.0.1) <http://sourceforge.net/projects/owasp/files/Guide/2.0.1/OWASPGuide2.0.1.pdf/download>

PMBOK shall be used by Master Contractors in the development of their project management methodologies. The TO Contractor, including its staff and any subcontractors assigned to this TO Agreement, shall follow a consistent methodology for all TO activities as described in the TO Proposal.

All TO Contractor personnel, while on-site at either COM location or when representing the COM pursuant to this TORFP, shall adhere to all COM policies, guidelines, dress codes, and other standards placed on COM personnel. These standards will be provided to the TO Contractor prior to the start of work under the TO Agreement. Please note that COM reserves the right to modify, add to, or delete any of such standards at any time during the course of the TO Agreement.

COM is the custodian of private taxpayer data, or non-public personal information (NPPI), some of which is Federal Taxpayer Information (FTI), which is tightly controlled by the IRS with audits and safeguard reviews. NPPI is defined as any personally-identifiable information the COM collects and stores, including information submitted from taxpayers, which is not available to the general public.

The nature of the proposed TO Agreement may expose the TO Contractor to considerable COM-confidential information, including NPPI and FTI (together, "Confidential Information"). Confidential Information means any and all information provided by or made available by the State and/or COM, to the TO Contractor, or discovered in the conduct of testing activities, in connection with the TO Agreement, regardless of the form, format, or media on or in which the Confidential Information is provided and regardless of whether any such Confidential Information is marked as such. Confidential Information includes, by way of example only, information that the TO Contractor views, takes notes from, copies (if the State agrees in writing to permit copying), possesses or is otherwise provided access to and use of by the State in relation to the TO Agreement, or any and all information produced as a result of executing this Scope of Work..

The TO Contractor shall at a minimum follow any and all industry standards in addition to those specifically set forth in this TORFP, to protect the confidentiality of all such information.

The TO Contractor, and its employees, agents, and subcontractors, shall be required to attest that they understand that the COM retains Confidential Information and that all such Confidential Information will be protected by the TO Contractor, and individually protected by its employees, agents, and subcontractors, at all times. At no time shall any Confidential Information be removed, in any format, including but not limited to remote electronic access, from COM's premises except as specifically approved in writing by the COM TO Manager on a case-by-case basis. In addition, Confidential Information must be protected at all times when on-site at the Agency. This requirement is further set forth in Attachments 10 and 11 of this TORFP. If there are any inconsistencies between this Section 2.7 of this TORFP and the attached Non-disclosure Agreements, Attachments 10 and 11, the terms of this Section 2.7 shall control.

Notwithstanding any other terms or conditions set forth in this TORFP, the following provisions shall apply:

- A. At the discretion of the Agency, any breach of confidentiality is cause for immediate termination of the TO Agreement with the TO Contractor.
- B. COM shall determine what Agency-related information falls within the definition of Confidential Information. Absent specific guidance from the Agency to the contrary, any and all information that the TO Contractor is exposed to or discovers during the course of the TO Agreement must be treated by the TO Contractor as Confidential Information.
- C. The TO Contractor, at their expense, shall perform a criminal background check on all of its employees, personnel, and subcontractors who have any access to Confidential Information. All persons assigned to this TO Agreement by the TO Contractor must not have been convicted of a felony. The TO Contractor shall have policies and procedures in place to ensure the confidentiality of such information.

- D. The TO Contractor shall provide for the physical and electronic security of Confidential Information at all times that such information is under the TO Contractor's control, and the TO Contractor shall be able to determine any breach of Confidential Information.
1. The TO Contractor shall, in its TO Proposal, disclose to the Agency what safeguards it has in place to secure Confidential Information. COM does not intend to compromise the TO Contractor's own confidential or proprietary information with this requirement; however, the TO Agreement will not be awarded to a Master Contractor that does not have sufficient safeguards, or whose safeguards are not apparent to the Agency after reading the TO Proposal, to satisfy the Agency's security concerns and requirements.
  2. The Agency shall have the right to confirm that the TO Contractor has satisfied its obligations under the terms of the TO Agreement, which includes the right to review TO Contractor audits, summaries of test results, or other equivalent evaluations.
  3. The TO Contractor shall not make copies of any Agency supplied or Confidential Information, or any Confidential Information created as a result of work conducted under this TO Agreement, except as required for back-up or redundancy, and shall destroy or return to the Agency any such information that is no longer necessary for the TO Contractor to fulfill its obligations pursuant to the TO Agreement. In no event shall any data in the possession of the TO Contractor (as a result of this TORFP) survive the end of the TO Agreement, and the TO Contractor shall certify any destruction (including back-up copies) to the Agency.
- E. Where prior written consent to subcontract is granted by the Agency, the TO Contractor shall remain responsible for ensuring that each subcontractor agrees to provide at least equivalent safeguards of Confidential Information to those of the TO Contractor. The TO Contractor shall obtain Agency approval of these subcontractor safeguards prior to commencement of work by any subcontractor in relation to this TORFP. Notwithstanding any subcontract, it remains the TO Contractor's responsibility to the Agency to safeguard all Confidential Information.
- F. The TO Contractor shall immediately notify the Agency TO Manager, and provide available details by email, in the event of a breach or potential breach of Confidential Information.
1. The TO Contractor shall promptly and continually assess the extent and breadth of any possible or confirmed breach of the Agency's Confidential Information and shall remain in frequent, regular contact with the Agency regarding the incident.
  2. The TO Contractor shall take prompt action to remedy conditions that may have caused a breach, or, in the event of a potential breach, to address conditions that have been identified as having the potential to cause a breach.
- G. TO Contractor personnel shall not connect non-Agency hardware to the Agency's computing resources without prior written approval by the Agency's TO Manager. If approved, the TO Contractor is required to provide protections equivalent to the Agency's protection of its own hardware.
- H. Terms related to confidentiality provisions shall survive the termination of the TO Agreement issued pursuant to this TORFP.
- I. All persons who will be assigned to work under the TO Agreement shall be required to complete any and all paperwork deemed necessary by the Agency for security access to both the Agency's physical facility and computing resources. Refusal by any person assigned to the TO Agreement shall constitute immediate grounds for default by the TO Contractor. All TO Contractor personnel

shall be required to wear a badge, within plain sight identifying them by their name and the TO Contractor's name, at all times while on Agency premises.

## **2.8 TO CONTRACTOR PERSONNEL MINIMUM QUALIFICATIONS**

The Master Contractor's proposed staff shall document using Attachment 5 the professional and technical level of expertise for each proposed project team member. The Master Contractor's TO Proposal shall demonstrate that the proposed project team has the ability to perform penetration testing and security vulnerability assessments on Internet-facing systems, network perimeter security devices and equipment, as described in this TORFP, on hardware devices to include (but not limited to) firewalls, routers, Windows-based servers, and comparable network infrastructure devices. The TO Contractor shall propose applicable staff based on the requirements of the scope of work and document the project team's ability to satisfy the following requirements:

1. At least one team member shall –
  - a. Possess either an ISC2 Certified Information Systems Security Professional (CISSP) or a GIAC Security Expert (GSE) certification.
  - b. Have experience in conducting web application security assessments, with at least two (2) security risk assessments performed within the past three (3) years, specifically involving custom, .NET framework designed applications. Additionally, at least two (2) assessments shall have involved applications similar to those employed at the Agency where users authenticate securely through the Internet to transmit and receive sensitive data (i.e., Non-Public Personal Information-NPPI). If the TO Contractor proposes more than one individual with such credentials, the Agency may deem that technical proposal superior to others that are otherwise equal.
  - c. Have experience in conducting PEN testing as described in the Scope of Work.
  - d. Have successfully completed at least two (2) PEN tests within the last three (3) years.
2. Project Team Member's qualifications shall be documented on Attachment 5 and supported through the submission of references, at least two (2) references that demonstrate the successful completion of a comparable project within the last three (3) years.

## **2.9 TO CONTRACTOR MINIMUM QUALIFICATIONS**

The following minimum qualifications are mandatory. The TO Contractor shall demonstrate in its technical proposal that it meets all minimum qualifications stated in this TORFP and is capable of furnishing all services and producing high quality deliverables required to successfully complete/accomplish the purpose of the TO Agreement.

**A. References.** Provide a minimum of two examples of projects or contracts the Master Contractor has completed that were similar to Section 2 (see Section 3 – Master Contractor and Subcontractor Experience and Capabilities) in the last 3 years.

## **2.10 TO CONTRACTOR REQUIRED EXPERTISE**

The TO Contractor shall demonstrate, in its proposal, that it possesses such expertise in-house or has fostered strategic alliances with other firms in order to perform as required. The Master Contractor shall also include the following in their TO Proposal:

**A. Detailed Staffing Plan.** For the dual purposes of project efficiency and limitation of risk exposure, the TO Contractor shall propose the minimum number of persons necessary to satisfactorily perform the services requested in this TORFP including all requirements set forth in the Scope of Work. All persons who will be assigned to work under the TO Agreement (the "project team") shall be identified by name, and their individual credentials shall be submitted to the Agency in the Master Contractor's Technical



Proposal (see instructions for Attachment 5). At a minimum, the Master Contractor shall provide a resume and any additional documentation, including, if applicable, proper certification as described herein, for each proposed individual. During the evaluation of the technical proposal, the Agency will review the credentials of the proposed personnel. In the event that any individual proposed is not acceptable to the Agency, which will occur if the Agency determines that such individual does not meet the minimum qualifications required and set forth in Section 2.8 above, notice will be provided to the Master Contractor and the Master Contractor will be deemed not susceptible of award. After award of the TO Agreement, if it becomes necessary to replace an individual assigned to work on the TO Agreement, the TO Contractor shall provide at least 10 business days' notice of any proposed substitution of personnel to the TO Manager. The credentials of the proposed substitute shall be equivalent or superior to the incumbent and the TO Manager must approve the substitution prior to the individual commencing work under the TO Agreement.

**B. Designation of the Project Team.** A Master Contractor shall designate individuals as the "Project Team" in its TO Proposal. After award of the TO Agreement, a TO Contractor that seeks to remove and substitute an individual previously designated as a member of the Project Team shall provide the TO Manager at least 10 business days advance written notice of the proposed substitution.

**C. Commitment to Training of TO Contractor Personnel Assigned to the TO Agreement.** The TO Contractor shall provide training for substitute personnel in both the technical and business requirements of this TORFP, at the TO Contractor's own time and expense. This training shall result in a substitute that is immediately capable of functioning as a productive member of the TO Contractor's project team. By signing the TO Agreement, the TO Contractor shall be bound by this provision.

## 2.11 INVOICING

Payment will only be made upon completion and acceptance of the deliverables defined in Section 2.6.

Invoice payments to the TO Contractor shall be governed by the terms and conditions defined in the CATS II Master Contract. A proper invoice for payment shall contain the TO Contractor's Federal Tax Identification Number, as well as the information described below, and must be submitted to the TO Manager for payment approval. Payment of invoices will be withheld if a signed Acceptance of Deliverable form – Attachment 9, is not submitted.

The TO Contractor shall submit invoices for payment upon acceptance of separately priced deliverables, on or before the 15<sup>th</sup> day of the month following receipt of the approved notice(s) of acceptance from the TO Manager. A copy of the notice(s) of acceptance shall accompany all invoices submitted for payment.

### 2.11.1 INVOICE SUBMISSION PROCEDURE

This procedure consists of the following requirements and steps:

- A) The invoice shall identify the Comptroller of Maryland as the TO Requesting Agency, deliverable description, associated TOA number, date of invoice, period of performance covered by the invoice, and a TO Contractor point of contact with telephone number.
- B) The TO Contractor shall send the original of each invoice and supporting documentation (itemized billing reference for employees and any subcontractor and signed Acceptance of Deliverable form – Attachment 9, for each deliverable being invoiced) submitted for payment to the Comptroller of Maryland at the following address:

Comptroller of Maryland  
Information Technology Division  
P. O. Box 2367  
Annapolis, MD 21404 – 2367

Comptroller of Maryland TORFP Web Application Security Assessment E00P2400385

Attn: Fiscal Services

- C) Invoices for final payment shall be clearly marked as “FINAL” and submitted when all work requirements have been completed and no further charges are to be incurred under the TOA. In no event shall any invoice be submitted later than 60 calendar days from the TOA termination date.

## **2.12 MBE PARTICIPATION REPORTS**

Monthly reporting of MBE participation is required in accordance with the terms and conditions of the CATS II Master Contract by the 15<sup>th</sup> day of each month. The TO Contractor shall provide a completed MBE Participation form (Attachment 2, Form D-5) to Comptroller of Maryland at the same time the invoice copy is sent. The TO Contractor shall ensure that each MBE Subcontractor provides a completed MBE Participation Form (Attachment 2, Form D-6). Subcontractor reporting shall be sent directly from the subcontractor to Comptroller of Maryland. Comptroller of Maryland will monitor both the TO Contractor’s efforts to achieve the MBE participation goal and compliance with reporting requirements. The TO Contractor shall email all completed forms, copies of invoices and checks paid to the MBE directly to the TO Procurement Officer and TO Manager.

## **SECTION 3 - TASK ORDER PROPOSAL FORMAT AND SUBMISSION REQUIREMENTS**

### **3.1 REQUIRED RESPONSE**

Each Master Contractor receiving this CATS II TORFP must respond within the submission time designated in the Key Information Summary Sheet. Each Master Contractor is required to submit one (1) of two (2) possible responses: 1) a proposal; or 2) a completed Master Contractor Feedback Form. The feedback form helps the State understand for future contract development why Master Contractors did not submit proposals. The form is accessible via the CATS II Master Contractor login screen and clicking on TORFP Feedback Response Form from the menu.

### **3.2 FORMAT**

If a Master Contractor elects to submit a TO Proposal, the Master Contractor shall do so in conformance with the requirements of this CATS II TORFP. A TO Proposal shall contain the following sections in order:

#### **3.2.1 TECHNICAL PROPOSAL**

##### **A) Proposed Services**

- 1) **Executive Summary:** A high-level overview of the Master Contractor's understanding of the background, purpose, and objectives of the TORFP. The Executive Summary shall summarize the Master Contractor's capabilities and experience, and summarize the proposed methodology and solution for achieving the objectives of the TORFP.
- 2) **Proposed Solution:** A detailed narrative of the Master Contractor's proposed methodology and solution for completing the requirements and deliverables in Section 2 - Scope of Work. The Master Contractor must address each requirement and deliverable describing in detail how they intend to satisfy each requirement..
- 3) **Draft Project Schedule and Work Breakdown Structure (WBS):** The project schedule should include a comprehensive schedule of tasks and estimated times frames for completing all requirements and deliverables, including any tasks to be performed by State or third party personnel. The WBS should reflect the chronology of tasks without assigning specific time frames or start / completion dates. The final schedule and WBS should come later as a deliverable under the TO after the TO Contractor has had opportunity to develop realistic estimates. The Project Schedule and WBS may include tasks to be performed by the State or third parties as appropriate.
- 4) **Draft Project Risk Assessment:** Identification and prioritization of risks inherent in meeting the requirements in Section 2 - Scope of Work. Includes a description of strategies to mitigate risks. The final version of the Project Risk Assessment is a deliverable in Section 2 – Scope of Work. The Risk Assessment shall be reviewed, updated and managed by the process defined in the Risk Management Plan.
- 5) **Assumptions:** A description of any assumptions formed by the Master Contractor in developing the Technical Proposal. Master Contractors should avoid assumptions that counter or constitute exceptions to TORFP terms and conditions.
- 6) **Proposed Tools:** A description of any tools, for example hardware and/or software applications that will be used to facilitate the work.

##### **B) Proposed Personnel**

- 1) **Identify and provide resumes for all proposed personnel.** The resumes should prominently feature the proposed personnel's skills and experience as they relate to the Master Contractor's proposed

solution and Section 2 – Scope of Work. Resumes of the personnel who will be assigned to the project team and perform the assessments shall indicate past experience as related to the requirements defined in Section 2 – Scope of Work.

- 2) Certification that all proposed personnel meet the minimum required qualifications and possess the required certifications in accordance to Section 2.8.
- 3) Provide the names and titles of the Master Contractor’s management staff who will supervise the personnel and quality of services rendered under this TOA.
- 4) For each project team member, complete and provide Attachment 5 – Labor Classification Personnel Resume Summary.

C) MBE Participation

- 1) Submit completed MBE documents Attachment 2 - Forms D-1 and D-2.

D) Subcontractors

Identify all proposed subcontractors, including MBEs, and their roles in the performance of Section 2 - Scope of Work.

E) Master Contractor and Subcontractor Experience and Capabilities

- 1) Provide the draft Staffing Plan.
- 2) Provide up to two examples of projects or contracts the Master Contractor has completed that were similar to Section 2 - Scope of Work. Each example must include contact information for the client organization complete with the following:
  - a) Name of organization.
  - b) Point of contact name, title, and telephone number
  - c) Services provided as they relate to Section 2 - Scope of Work.
  - d) Start and end dates for each example project or contract. If the Master Contractor is no longer providing the services, explain why not.
- 3) State of Maryland Experience: If applicable, the Master Contractor shall submit a list of all contracts it currently holds or has held within the past five years with any entity of the State of Maryland. For each identified contract, the Master Contractor shall provide:
  - a) Name of organization.
  - b) Point of contact name, title, and telephone number
  - c) Services provided as they relate to Section 2 - Scope of Work.
  - d) Start and end dates for each example project or contract. If the Master Contractor is no longer providing the services, explain why not.
  - e) Dollar value of the contract.
  - f) Whether the contract was terminated before the original expiration date.
  - g) Whether any renewal options were not exercised.

Note - State of Maryland experience can be included as part of Section E2 above as project or contract experience. State of Maryland experience is neither required nor given more weight in proposal evaluations.

F) Master Contractor’s Facility

- 1) Identify Master Contractor’s including subcontractor’s facilities, including address, from which any work will be performed.

G) State Assistance

- 1) Provide an estimate of expectation concerning participation by State personnel.

H) Confidentiality

- 1) A Master Contractor should give specific attention to the identification of those portions of its proposal that it considers confidential, proprietary commercial information or trade secrets, and provide justification why such materials, upon request, should not be disclosed by the State under the Public Information Act, Title 10, Subtitle 6, of the State Government Article of the Annotated Code of Maryland. Contractors are advised that, upon request for this information from a third party, the TO Procurement Officer will be required to make an independent determination regarding whether the information may be disclosed.

**3.2.2 FINANCIAL RESPONSE**

- A) A description of any assumptions on which the Master Contractor's Financial Proposal is based (Assumptions shall not constitute conditions, contingencies, or exceptions to the price proposal);
- B) Attachment 1 Completed Financial Proposal with all rates fully loaded.

## **SECTION 4 – TASK ORDER AWARD PROCESS**

### **4.1 OVERVIEW**

The TO Contractor shall be selected from among all eligible Master Contractors within the appropriate functional area responding to the CATS II TORFP. In making the TOA award determination, the TO Requesting Agency will consider all information submitted in accordance with Section 3.

### **4.2 TECHNICAL PROPOSAL EVALUATION CRITERIA**

The following are technical criteria for evaluating a TO Proposal in descending order of importance.

1. The Master Contractor's overall understanding of the TORFP Scope of Work and technologies based on the required responses to Section 2.
2. The Master Contractor's documented, and confirmed by Contractor's references, successful experiences performing work similar to the web application security requirements of this TORFP.
3. The expertise, experience and credentials of proposed project team members meets or exceeds the minimum qualifications set forth in this TORFP.
4. The expertise of the Master Contractor meets or exceeds the minimum qualifications set forth in the Master Contract and meets or exceeds the mandatory skills defined in this TORFP.
5. The Master Contractor's draft Staffing Plan.
6. The Master Contractor's draft Project Management Plan.
7. The Master Contractor's draft Project Risk Assessment.

### **4.3 SELECTION PROCEDURES**

- A. Proposals will be assessed throughout the evaluation process for compliance with the requirements as defined in Section 2 and the quality of responses in the Technical portion of the TO Proposal. Proposals deemed technically qualified will have their financial proposal considered. All others will be deemed not reasonably susceptible of award and will receive e-mail notice from the TO Procurement Officer of not being selected to perform the work.
- B. Qualified TO Proposal financial responses will be reviewed and ranked from lowest to highest price proposed.
- C. The TO Proposal, considering both technical and financial submissions, that is deemed most advantageous to the Agency shall be selected for award of the TO Agreement. In light of the highly technical and sensitive work to be performed as a result of this TORFP, technical credentials will be given greater weight than pricing in the Agency's award decision.

### **4.4 COMMENCEMENT OF WORK UNDER A TOA**

Commencement of work in response to a TOA shall be initiated only upon issuance of a fully executed TOA, a Non-Disclosure Agreement (To Contractor), a Purchase Order, and by the first Notice to Proceed (NTP1) authorized by the TO Procurement Officer. See Attachment 7 - Notice to Proceed (sample). If the Agency, at its sole discretion, decides to proceed with the option services, the TO Procurement Officer shall issue the second Notice to Proceed (NTP2).

**ATTACHMENT 1**  
**PRICE PROPOSAL FORM**

**PRICE PROPOSAL FOR CATS II TORFP # E00P2400385**

Identification	Deliverable	Proposed Price
2.6.2.1	Detailed Project Management Plan and Sub-plans	
2.6.2.2	Detailed Project Schedule Updated Weekly	
2.6.2.3	Project Risk Assessment	
2.6.2.3	Penetration Test Reports	
2.6.2.4	Web Applications Security Assessment Reports	
2.6.2.5	Training	
2.6.2.6	Weekly Status Reports and Meetings	
2.6.2.7	Validation and Certification (Optional)	
<b>Total Not-to-Exceed Fixed Price</b>		

\_\_\_\_\_  
Authorized Individual Name

\_\_\_\_\_  
Company Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Company Tax ID #

SUBMIT AS A .PDF FILE WITH THE FINANCIAL RESPONSE

**ATTACHMENT 2 – MINORITY BUSINESS ENTERPRISE FORMS**  
**TO CONTRACTOR MINORITY BUSINESS ENTERPRISE REPORTING**  
**REQUIREMENTS**

**CATS II TORFP # E00P2400385**

These instructions are meant to accompany the customized reporting forms sent to you by the TO Manager. If, after reading these instructions, you have additional questions or need further clarification, please contact the TO Manager immediately.

1. As the TO Contractor, you have entered into a TO Agreement with the State of Maryland. As such, your company/firm is responsible for successful completion of all deliverables under the contract, including your commitment to making a good faith effort to meet the MBE participation goal(s) established for TORFP. Part of that effort, as outlined in the TORFP, includes submission of monthly reports to the State regarding the previous month's MBE payment activity. Reporting forms D-5 (TO Contractor Paid/Unpaid MBE Invoice Report) and D-6 (Subcontractor Paid/Unpaid MBE Invoice Report) are attached for your use and convenience.
2. The TO Contractor must complete a separate Form D-5 for each MBE subcontractor for each month of the contract and submit one copy to each of the locations indicated at the bottom of the form. The report is due no later than the 15<sup>th</sup> of the month following the month that is being reported. For example, the report for January's activity is due no later than the 15<sup>th</sup> of February. With the approval of the TO Manager, the report may be submitted electronically. Note: Reports are required to be submitted each month, regardless of whether there was any MBE payment activity for the reporting month.
3. The TO Contractor is responsible for ensuring that each subcontractor receives a copy (e-copy of and/or hard copy) of Form D-6. The TO Contractor should make sure that the subcontractor receives all the information necessary to complete the form properly, i.e., all of the information located in the upper right corner of the form. It may be wise to customize Form D-6 (upper right corner of the form) for the subcontractor the same as the Form D-5 was customized by the TO Manager for the benefit of the TO Contractor. This will help to minimize any confusion for those who receive and review the reports.
4. It is the responsibility of the TO Contractor to make sure that all subcontractors submit reports no later than the 15<sup>th</sup> of each month, regardless of whether there was any MBE payment activity for the reporting month. Actual payment data is verified and entered into the State's financial management tracking system from the subcontractor's D-6 report only. Therefore, if the subcontractor(s) do not submit their D-6 payment reports, the TO Contractor cannot and will not be given credit for subcontractor payments, regardless of the TO Contractor's proper submission of Form D-5. The TO Manager will contact the TO Contractor if reports are not received each month from either the prime contractor or any of the identified subcontractors. The TO Contractor must promptly notify the TO Manager if, during the course of the contract, a new MBE subcontractor is utilized. Failure to comply with the MBE contract provisions and reporting requirements may result in sanctions, as provided by COMAR 21.11.03.13.



# ATTACHMENT 2 – MINORITY BUSINESS ENTERPRISE FORMS

## FORM D – 1

### CERTIFIED MBE UTILIZATION AND FAIR SOLICITATION AFFIDAVIT

**This document shall be included with the submittal of the Offeror's TO Proposal. If the Offeror fails to submit this form with the TO Proposal, the TO Procurement Officer shall determine that the Offeror's TO Proposal is not reasonably susceptible of being selected for award.**

In conjunction with the offer submitted in response to TORFP No. E00P2400385, I affirm the following:

1. I acknowledge the overall certified Minority Business Enterprise (MBE) participation goal of [redacted] percent and, if specified in the TORFP, sub-goals of [redacted] percent for MBEs classified as African American-owned and [redacted] percent for MBEs classified as women-owned. I have made a good faith effort to achieve this goal.

OR

After having made a good faith effort to achieve the MBE participation goal, I conclude that I am unable to achieve it. Instead, I intend to achieve an MBE goal of [redacted] percent and request a waiver of the remainder of the goal. If I am selected as the apparent TO Agreement awardee, I will submit written waiver documentation that complies with COMAR 21.11.03.11 within 10 business days of receiving notification that our firm is the apparent low bidder or the apparent awardee.

2. I have identified the specific commitment of certified Minority Business Enterprises by completing and submitting an MBE Participation Schedule (Attachment 2 - Form D-2) with the proposal.
3. I acknowledge that the MBE subcontractors/suppliers listed in the MBE Participation Schedule will be used to accomplish the percentage of MBE participation that I intend to achieve.
4. I understand that if I am notified that I am the apparent TO Agreement awardee, I must submit the following documentation within 10 business days of receiving notice of the potential award or from the date of conditional award (per COMAR 21.11.03.10), whichever is earlier.
  - (a) Outreach Efforts Compliance Statement (Attachment D-3)
  - (b) Subcontractor Project Participation Statement (Attachment D-4)
  - (c) MBE Waiver Documentation per COMAR 21.11.03.11 (if applicable)
  - (d) Any other documentation required by the TO Procurement Officer to ascertain offeror's responsibility in connection with the certified MBE participation goal.

If I am the apparent TO Agreement awardee, I acknowledge that if I fail to return each completed document within the required time, the TO Procurement Officer may determine that I am not responsible and therefore not eligible for TO Agreement award. If the TO Agreement has already been awarded, the award is voidable.

5. In the solicitation of subcontract quotations or offers, MBE subcontractors were provided not less than the same information and amount of time to respond as were non-MBE subcontractors.

I solemnly affirm under the penalties of perjury that the contents of this paper are true to the best of my knowledge, information, and belief.

\_\_\_\_\_  
Offeror Name

\_\_\_\_\_  
Signature of Affiant

\_\_\_\_\_  
Address

\_\_\_\_\_  
Printed Name, Title

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
Date

**SUBMIT AS A .PDF FILE WITH TO RESPONSE**

# ATTACHMENT 2 – MINORITY BUSINESS ENTERPRISE FORMS

## FORM D – 2

### MINORITY BUSINESS ENTERPRISE PARTICIPATION SCHEDULE

**This document shall be included with the submittal of the TO Proposal. If the Offeror fails to submit this form with the TO Proposal, the TO Procurement Officer shall determine that the TO Proposal is not reasonably susceptible of being selected for award.**

TO Prime Contractor (Firm Name, Address, Phone)	Task Order Description
Task Order Agreement Number E00P2400385	
<b>List Information For Each Certified MBE Subcontractor On This Project</b>	
Minority Firm Name	MBE Certification Number
Work To Be Performed/SIC	
Percentage of Total Contract	
Minority Firm Name	MBE Certification Number
Work To Be Performed/SIC	
Percentage of Total Contract	
Minority Firm Name	MBE Certification Number
Work To Be Performed/SIC	
Percentage of Total Contract	

**USE ATTACHMENT D-2 CONTINUATION PAGE AS NEEDED**

### SUMMARY

<b>TOTAL MBE PARTICIPATION:</b>	_____ %
<b>TOTAL WOMAN-OWNED MBE PARTICIPATION:</b>	_____ %
<b>TOTAL AFRICAN AMERICAN-OWNED MBE PARTICIPATION:</b>	_____ %

Document Prepared By: (please print or type)

Name: \_\_\_\_\_ Title: \_\_\_\_\_

SUBMIT AS A PDF FILE WITH TO RESPONSE

**ATTACHMENT 2 – MINORITY BUSINESS ENTERPRISE FORMS**

**FORM D – 2**

**MINORITY BUSINESS ENTERPRISE PARTICIPATION SCHEDULE (CONTINUED)**

List Information For Each Certified MBE Subcontractor On This Project	
Minority Firm Name	MBE Certification Number
Work To Be Performed/SIC	
Percentage of Total Contract	
Minority Firm Name	MBE Certification Number
Work To Be Performed/SIC	
Percentage of Total Contract	
Minority Firm Name	MBE Certification Number
Work To Be Performed/SIC	
Percentage of Total Contract	
Minority Firm Name	MBE Certification Number
Work To Be Performed/SIC	
Percentage of Total Contract	
Minority Firm Name	MBE Certification Number
Work To Be Performed/SIC	
Percentage of Total Contract	
Minority Firm Name	MBE Certification Number
Work To Be Performed/SIC	
Percentage of Total Contract	

SUBMIT AS A PDF FILE WITH TO RESPONSE

**ATTACHMENT 2 – MINORITY BUSINESS ENTERPRISE FORMS**

**FORM D – 3**

**OUTREACH EFFORTS COMPLIANCE STATEMENT**

In conjunction with the bid or offer submitted in response to TORFP # E00P2400385, I state the following:

1. Offeror identified opportunities to subcontract in these specific work categories:
  
2. Attached to this form are copies of written solicitations (with bidding instructions) used to solicit certified MBEs for these subcontract opportunities.
  
3. Offeror made the following attempts to contact personally the solicited MBEs:
  
4.  Offeror assisted MBEs to fulfill or to seek waiver of bonding requirements.  
  
(DESCRIBE EFFORTS)  
  
 This project does not involve bonding requirements.
  
5.  Offeror did/did not attend the pre-proposal conference  
 No pre-proposal conference was held.

\_\_\_\_\_  
Offeror Name

By: \_\_\_\_\_  
Name

\_\_\_\_\_  
Address

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

**SUBMIT WITHIN 10 BUSINESS DAYS OF RECEIVING NOTICE OF THE POTENTIAL AWARD**

**ATTACHMENT 2 – MINORITY BUSINESS ENTERPRISE FORMS**

**FORM D – 4**

**SUBCONTRACTOR PROJECT PARTICIPATION STATEMENT**

SUBMIT ONE FORM FOR EACH CERTIFIED MBE LISTED IN THE MBE PARTICIPATION SCHEDULE

Provided that \_\_\_\_\_ is awarded the TO Agreement in  
(Prime TO Contractor Name)

conjunction with TORFP No. E00P2400385, it and \_\_\_\_\_,  
(Subcontractor Name)

MDOT Certification No. \_\_\_\_\_, intend to enter into a contract by which the subcontractor shall:

(Describe work to be performed by MBE):

---

---

---

---

---

- No bonds are required of Subcontractor
- The following amount and type of bonds are required of Subcontractor:

By: \_\_\_\_\_  
Prime Contractor Signature

By: \_\_\_\_\_  
Subcontractor Signature

\_\_\_\_\_  
Name

\_\_\_\_\_  
Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

SUBMIT WITHIN 10 BUSINESS DAYS OF RECEIVING NOTICE OF THE POTENTIAL AWARD

# ATTACHMENT 2 – MINORITY BUSINESS ENTERPRISE FORMS

## FORM D – 5

### MINORITY BUSINESS ENTERPRISE PARTICIPATION TO CONTRACTOR PAID/UNPAID INVOICE REPORT

Report #: _____ Reporting Period (Month/Year): _____ <b>Report is due by the 15<sup>th</sup> of the following month.</b>	CATS II TORFP #E00P2400385 Contracting Unit _____ Contract Amount _____ MBE Sub Contract Amt _____ Contract Begin Date _____ Contract End Date _____ Services Provided _____
--	--

Prime TO Contractor:		Contact Person:	
Address:			
City:		State:	ZIP:
Phone:	FAX:		
Subcontractor Name:		Contact Person:	
Phone:	FAX:		
Subcontractor Services Provided:			
<b>List all unpaid invoices over 30 days old received from the MBE subcontractor named above:</b>			
1.			
2.			
3.			
Total Dollars Unpaid: \$ _____			

\*\*If more than one MBE subcontractor is used for this contract, please use separate forms.

**Return one copy of this form to the following address:**

(TO MANAGER OF APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)	(TO PROCUREMENT OFFICER OR APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)
--	--

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

SUBMIT AS REQUIRED IN TO CONTRACTOR MBE REPORTING REQUIREMENTS

# ATTACHMENT 2 – MINORITY BUSINESS ENTERPRISE FORMS

## FORM D – 6

### MINORITY BUSINESS ENTERPRISE PARTICIPATION SUBCONTRACTOR PAID/UNPAID INVOICE REPORT

Report #: _____  Reporting Period (Month/Year): ___/_____  <b>Report Due By the 15<sup>th</sup> of the following Month.</b>	CATS II TORFP #E00P2400385 Contracting Unit _____ Contract Amount _____ MBE Sub Contract Amt _____ Contract Begin Date _____ Contract End Date _____ Services Provided _____	
MBE Subcontractor Name: _____		
MDOT Certification #: _____		
Contact Person: _____		
Address: _____		
City: _____	State: _____	ZIP: _____
Phone: _____	FAX: _____	
Subcontractor Services Provided: _____		
<b>List all payments received from Prime TO Contractor during reporting period indicated above.</b>  1. 2. 3.  Total Dollars Paid: \$ _____	<b>List dates and amounts of any unpaid invoices over 30 days old.</b>  1. 2. 3.  Total Dollars Unpaid: \$ _____	
Prime TO Contractor: _____ Contact Person: _____		

**Return one copy of this form to the following address:**

(TO MANAGER OF APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)	(TO PROCUREMENT OFFICER OR APPLICABLE POC NAME, TITLE) (AGENCY NAME) (ADDRESS, ROOM NUMBER) (CITY, STATE ZIP) (EMAIL ADDRESS)
--	--

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**SUBMIT AS REQUIRED IN TO CONTRACTOR MBE REPORTING REQUIREMENTS**



## CATS II TORFP# E00P2400385 OF MASTER CONTRACT #060B9800035

This Task Order Agreement (“TO Agreement”) is made this day of Month, 201~~X~~ by and between Task Order Contractor (TO Contractor) and the STATE OF MARYLAND, TO Requesting Agency.

IN CONSIDERATION of the mutual premises and the covenants herein contained and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions. In this TO Agreement, the following words have the meanings indicated:
  - a. “Agency” means the TO Requesting Agency, as identified in the CATS II TORFP # E00P2400385.
  - b. “CATS II TORFP” means the Task Order Request for Proposals # E00P2400385, dated MONTH DAY, YEAR, including any addenda.
  - c. “Master Contract” means the CATS II Master Contract between the Maryland Department of Information Technology and TO Contractor dated \_\_\_\_\_.
  - d. “TO Procurement Officer” means TO Procurement Officer. The Agency may change the TO Procurement Officer at any time by written notice to the TO Contractor.
  - e. “TO Agreement” means this signed TO Agreement between TO Requesting Agency and TO Contractor.
  - f. “TO Contractor” means the CATS II Master Contractor awarded this TO Agreement, whose principal business address is \_\_\_\_\_.
  - g. “TO Manager” means TO Manager of the Agency. The Agency may change the TO Manager at any time by written notice to the TO Contractor.
  - h. “TO Proposal - Technical” means the TO Contractor’s technical response to the CATS II TORFP dated date of TO Proposal – Technical.
  - i. “TO Proposal – Financial” means the TO Contractor’s financial response to the CATS II TORFP dated date of TO Proposal - Financial.
  - j. “TO Proposal” collectively refers to the TO Proposal – Technical and TO Proposal – Financial.
2. Scope of Work
  - 2.1 This TO Agreement incorporates all of the terms and conditions of the Master Contract and shall not in any way amend, conflict with or supersede the Master Contract.
  - 2.2 The TO Contractor shall, in full satisfaction of the specific requirements of this TO Agreement, provide the services set forth in Section 2 of the CATS II TORFP. These services shall be provided in accordance with the Master Contract, this TO Agreement, and the following Exhibits, which are attached and incorporated herein by reference. If there is any conflict among the Master Contract, this TO Agreement, and these Exhibits, the terms of the Master Contract shall govern. If there is any conflict between this TO Agreement and any of these Exhibits, the following order of precedence shall determine the prevailing provision:
    - a. The TO Agreement,
    - b. Exhibit A – CATS II TORFP
    - c. Exhibit B – TO Proposal-Technical
    - d. Exhibit C – TO Proposal-Financial
  - 2.3 The TO Procurement Officer may, at any time, by written order, make changes in the work within the general scope of the TO Agreement. No other order, statement or conduct of the TO Procurement Officer or

any other person shall be treated as a change or entitle the TO Contractor to an equitable adjustment under this Section. Except as otherwise provided in this TO Agreement, if any change under this Section causes an increase or decrease in the TO Contractor's cost of, or the time required for, the performance of any part of the work, whether or not changed by the order, an equitable adjustment in the TO Agreement price shall be made and the TO Agreement modified in writing accordingly. The TO Contractor must assert in writing its right to an adjustment under this Section within thirty (30) days of receipt of written change order and shall include a written statement setting forth the nature and cost of such claim. No claim by the TO Contractor shall be allowed if asserted after final payment under this TO Agreement. Failure to agree to an adjustment under this Section shall be a dispute under the Disputes clause of the Master Contract. Nothing in this Section shall excuse the TO Contractor from proceeding with the TO Agreement as changed.

3. Time for Performance

Unless terminated earlier as provided in the Master Contract, the TO Contractor shall provide the services described in the TO Proposal and in accordance with the CATS II TORFP on receipt of a Notice to Proceed from the TO Manager. The term of this TO Agreement is for a period of \_\_\_\_\_, commencing on the date of Notice to Proceed and terminating on **Month Day, Year**.

4. Consideration and Payment

- 4.1 The consideration to be paid the TO Contractor shall be done so in accordance with the CATS II TORFP and shall not exceed the total amount of the task order. Any work performed by the TO Contractor in excess of the not-to-exceed ceiling amount of the TO Agreement without the prior written approval of the TO Manager is at the TO Contractor's risk of non-payment.
- 4.2 Payments to the TO Contractor shall be made as outlined in Section 2 of the CATS II TORFP, but no later than thirty (30) days after the Agency's receipt of an invoice for services provided by the TO Contractor, acceptance by the Agency of services provided by the TO Contractor, and pursuant to the conditions outlined in Section 4 of this Agreement.
- 4.3 Each invoice for services rendered must include the TO Contractor's Federal Tax Identification Number which is \_\_\_\_\_. Charges for late payment of invoices other than as prescribed by Title 15, Subtitle 1, of the State Finance and Procurement Article, Annotated Code of Maryland, as from time-to-time amended, are prohibited. Invoices must be submitted to the Comptroller of Maryland, Information Technology Division, P. O. Box 2367, Annapolis, MD 21404-2367, ATTN: Fiscal Services.
- 4.4 In addition to any other available remedies, if, in the opinion of the TO Procurement Officer, the TO Contractor fails to perform in a satisfactory and timely manner, the TO Procurement Officer may refuse or limit approval of any invoice for payment, and may cause payments to the TO Contractor to be reduced or withheld until such time as the TO Contractor meets performance standards as established by the TO Procurement Officer.

IN WITNESS THEREOF, the parties have executed this TO Agreement as of the date hereinabove set forth.

**TO Contractor Name**

\_\_\_\_\_  
By: Type or Print TO Contractor POC

\_\_\_\_\_  
Date

Witness: \_\_\_\_\_

STATE OF MARYLAND, COMPTROLLER OF MARYLAND  
INFORMATION TECHNOLOGY DIVISION

\_\_\_\_\_  
By: Lavinia Lee, TO Procurement Officer

\_\_\_\_\_  
Date

Witness: \_\_\_\_\_

## **ATTACHMENT 4 – CONFLICT OF INTEREST AFFIDAVIT AND DISCLOSURE**

- A) "Conflict of interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the State, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage.
- B) "Person" has the meaning stated in COMAR 21.01.02.01B(64) and includes a bidder, Offeror, Contractor, consultant, subcontractor or subconsultant at any tier, and also includes an employee or agent of any of these if the employee or agent has or will have the authority to control or supervise all or a portion of the work for which a bid or offer is made.
- C) The bidder or Offeror warrants that, except as disclosed in §D, below, there are no relevant facts or circumstances now giving rise or which could, in the future, give rise to a conflict of interest.
- D) The following facts or circumstances give rise or could in the future give rise to a conflict of interest (explain in detail—attach additional sheets if necessary):
- E) The bidder or Offeror agrees that if an actual or potential conflict of interest arises after the date of this affidavit, the bidder or Offeror shall immediately make a full disclosure in writing to the procurement officer of all relevant facts and circumstances. This disclosure shall include a description of actions which the bidder or Offeror has taken and proposes to take to avoid, mitigate, or neutralize the actual or potential conflict of interest. If the contract has been awarded and performance of the contract has begun, the Contractor shall continue performance until notified by the procurement officer of any contrary action to be taken.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date: \_\_\_\_\_ By: \_\_\_\_\_

(Authorized Representative and Affiant)

SUBMIT AS A .PDF FILE WITH TO RESPONSE

## **ATTACHMENT 5 – LABOR CLASSIFICATION PERSONNEL RESUME SUMMARY**

### **INSTRUCTIONS:**

1. Master Contractors must comply with all personnel requirements under the Master Contract RFP 060B9800035.
2. Only labor categories proposed in the Master Contractors Financial Proposal may be proposed under the CATS II TORFP process.
3. For each person proposed in any of the labor categories, complete one Labor Category Personnel Resume Summary to document how the proposed person meets each of the minimum requirements. This summary is required at the time of the interview.

For example: If you propose John Smith, who is your subcontractor, and you believe he meets the requirements of the Group Facilitator, you will complete the top section of the form by entering John Smith's name and the subcontractor's company name. You will then complete the right side of the Group Facilitator form documenting how the individual meets each of the requirements. Where there is a time requirement such as three months experience, you must provide the dates—from and to—showing an amount of time that equals or exceeds mandatory time requirement; in this case, three (3) months.

4. Each form also includes examples of duties to perform. The proposed person must be able to fulfill those duties.
5. For each subject matter expert, the State will identify the particular area of expertise and the Master Contractor shall provide proof the individual has qualifications within that area of expertise.
6. Additional information may be attached to each Labor Category Personnel Resume Summary that may assist a full and complete understanding of the individual being proposed.

**ATTACHMENT 5 – LABOR CLASSIFICATION PERSONNEL RESUME  
SUMMARY (CONTINUED)**

Proposed Individual's Name/Company:	How does the proposed individual meet each requirement?
<b>LABOR CLASSIFICATION TITLE – (INSERT LABOR CATEGORY NAME)</b>	
Education: (Insert the education description from the CATS II RFP from Section 2.10 for the applicable labor category.)	
Experience: (Insert the experience description from the CATS II RFP from Section 2.10 for the applicable labor category.)	
Duties: (Insert the duties description from the CATS II RFP from Section 2.10 for the applicable labor category.)	

The information provided on this form for this labor class is true and correct to the best of my knowledge:

**Contractor's Contract Administrator:**

\_\_\_\_\_  
Signature Date

**Proposed Individual:**

\_\_\_\_\_  
Signature Date

SUBMIT WITH TECHNICAL PROPOSAL  
SIGNATURE REQUIRED AT THE TIME OF THE INTERVIEW

## ATTACHMENT 6 – DIRECTIONS

### TO THE PRE-TO PROPOSAL CONFERENCE

COMPTROLLER OF MARYLAND  
DATA CENTER BUILDING  
108 CARROLL STREET  
ANNAPOLIS, MD

**Hint: If you want to use MapQuest, please use 80 Calvert Street as your destination not 108 Carroll Street, when using Carroll Street it will misdirect you to a location in Hillsmere Shores.**

#### DIRECTIONS TO THE LOUIS L. GOLDSTEIN TREASURY BUILDING LOBBY FROM THE BALTIMORE AREA

Take I-97 south until it merges with Rt. 50 East,  
Stay on Rt. 50 East towards Annapolis. (Approximately 1 mile)  
Take exit 24 (Rt. 70 South/Rowe Blvd.)

Bear to the right toward Annapolis South.

Come through two lights (less than 1 mile).

First light will be Farragut to the right and Melvin Avenue to the left.

The second light will be Taylor Avenue.

The road will stay straight and then bear off to the right (which you should do) at the next traffic light (Calvert Street) turn right onto Calvert Street.

(to the left of the light at Calvert Street is the Louis L. Goldstein Treasury Bldg.)

There will be a parking garage on Clay Street (first road on the right - Whitmore Parking Garage)

Or another parking garage on the left (Gott Parking Garage).

When exiting either garage walk towards the Louis L. Goldstein Treasury Bldg. into the Lobby where there will be a guard and someone to greet you. You must sign in and tell them you are meeting with me at the Data Center.

The guard will direct you to the Data Center Building, which requires you to exit the Treasury Building, cross a courtyard, walk through the Revenue Administration Building. After you exit the Revenue Administration Building, the Data Center is to the right.

Call Leslie if you need additional directions at (410) 260-7503.

## ATTACHMENT 7 – NOTICE TO PROCEED

Month Day, Year

TO Contractor Name

TO Contractor Mailing Address

Re: CATS II Task Order Agreement #E00P2400385

Dear TO Contractor Contact:

This letter is your official Notice to Proceed as of Month Day, Year, for the above-referenced Task Order (TO) Agreement. TO Manager of the TO Requesting Agency will serve as your contact person on this Task Order. TO Manager can be reached at telephone # and email address.

Enclosed is an original, fully executed TO Agreement and purchase order.

Sincerely,

TO Procurement Officer

Task Order Procurement Officer

Enclosures (2)

cc: TO Manager

Procurement Liaison Office, Department of Information Technology

Project Management Office, Department of Information Technology



# ATTACHMENT 8 – AGENCY RECEIPT OF DELIVERABLE FORM

I acknowledge receipt of the following:

TORFP Title: **Project Name for TORFP**

TO Agreement Number: #E00P2400385

Title of Deliverable: \_\_\_\_\_

TORFP Reference Section # \_\_\_\_\_

Deliverable Reference ID # \_\_\_\_\_

Name of TO Manager: **TO Manager**

\_\_\_\_\_  
TO Manager Signature

\_\_\_\_\_  
Date Signed

Name of TO Contractor's Project Manager: \_\_\_\_\_

\_\_\_\_\_  
TO Contractor's Project Manager Signature

\_\_\_\_\_  
Date Signed

SUBMIT AS REQUIRED IN SECTION 2.6 OF THE TORFP.

Comptroller of Maryland TORFP Web Application Security Assessment E00P2400385

# ATTACHMENT 9 – AGENCY ACCEPTANCE OF DELIVERABLE FORM

Agency Name: TO Requesting Agency

TORFP Title: TORFP Project Name

TO Manager: TO Manager and Phone Number

To:

The following deliverable, as required by TO Agreement #E00P2400385, has been received and reviewed in accordance with the TORFP.

Title of deliverable: \_\_\_\_\_

TORFP Contract Reference Number: Section # \_\_\_\_\_

Deliverable Reference ID # \_\_\_\_\_

This deliverable:

Is accepted as delivered.

Is rejected for the reason(s) indicated below.

REASON(S) FOR REJECTING DELIVERABLE:

OTHER COMMENTS:

\_\_\_\_\_  
TO Manager Signature

\_\_\_\_\_  
Date Signed

ISSUED BY THE TO MANAGER AS REQUIRED IN THE TORFP.

Comptroller of Maryland TORFP Web Application Security Assessment E00P2400385

## ATTACHMENT 10 – NON-DISCLOSURE AGREEMENT (OFFEROR)

This Non-Disclosure Agreement (the "Agreement") is made this \_\_\_ day of \_\_\_\_\_ 20\_\_, by and between \_\_\_\_\_ (hereinafter referred to as "the OFFEROR") and the State of Maryland (hereinafter referred to as "the State").

OFFEROR warrants and represents that it intends to submit a TO Proposal in response to CATS II TORFP #E00P2400385 for **TORFP Project Name**. In order for the OFFEROR to submit a TO Proposal, it will be necessary for the State to provide the OFFEROR with access to certain confidential information including, but not limited, to \_\_\_\_\_. All such information provided by the State shall be considered Confidential Information regardless of the form, format, or media upon which or in which such information is contained or provided, regardless of whether it is oral, written, electronic, or any other form, and regardless of whether the information is marked as "Confidential Information". As a condition for its receipt and access to the Confidential Information described above, the OFFEROR agrees as follows:

1. OFFEROR will not copy, disclose, publish, release, transfer, disseminate or use for any purpose in any form any Confidential Information received under Section 1.7, except in connection with the preparation of its TO Proposal.
2. Each employee or agent of the OFFEROR who receives or has access to the Confidential Information shall execute a copy of this Agreement and the OFFEROR shall provide originals of such executed Agreements to the State. Each employee or agent of the OFFEROR who signs this Agreement shall be subject to the same terms, conditions, requirements and liabilities set forth herein that are applicable to the OFFEROR.
3. OFFEROR shall return the Confidential Information to the State within five business days of the State's Notice of recommended award. If the OFFEROR does not submit a Proposal, the OFFEROR shall return the Confidential Information to **TO Procurement Officer, TO Requesting Agency** on or before the due date for Proposals.
4. OFFEROR acknowledges that the disclosure of the Confidential Information may cause irreparable harm to the State and agrees that the State may obtain an injunction to prevent the disclosure, copying, or other impermissible use of the Confidential Information. The State's rights and remedies hereunder are cumulative and the State expressly reserves any and all rights, remedies, claims and actions that it may have now or in the future to protect the Confidential Information and/or to seek damages for the OFFEROR'S failure to comply with the requirements of this Agreement. The OFFEROR consents to personal jurisdiction in the Maryland State Courts.
5. In the event the State suffers any losses, damages, liabilities, expenses, or costs (including, by way of example only, attorneys' fees and disbursements) that are attributable, in whole or in part to any failure by the OFFEROR or any employee or agent of the OFFEROR to comply with the requirements of this Agreement, OFFEROR and such employees and agents of OFFEROR shall hold harmless and indemnify the State from and against any such losses, damages, liabilities, expenses, and/or costs.
6. This Agreement shall be governed by the laws of the State of Maryland.
7. OFFEROR acknowledges that pursuant to Section 11-205.1 of the State Finance and Procurement Article of the Annotated Code of Maryland, a person may not willfully make a false or fraudulent statement or representation of a material fact in connection with a procurement contract. Persons making such statements are guilty of a felony and on conviction subject to a fine of not more than \$20,000 and/or imprisonment not exceeding five (5) years or both. OFFEROR further acknowledges that this Agreement is a statement made in connection with a procurement contract.
8. The individual signing below warrants and represents that they are fully authorized to bind the OFFEROR to the terms and conditions specified in this Agreement. If signed below by an individual employee or agent of the OFFEROR under Section 2 of this Agreement, such individual acknowledges that a failure to comply with the requirements specified in this Agreement may result in personal liability.

OFFEROR: \_\_\_\_\_ BY: \_\_\_\_\_

NAME: \_\_\_\_\_ TITLE: \_\_\_\_\_

ADDRESS: \_\_\_\_\_

SUBMIT AS REQUIRED IN SECTION 1.6 OF THE TORFP

## ATTACHMENT 11 – NON-DISCLOSURE AGREEMENT (TO CONTRACTOR)

**THIS NON-DISCLOSURE AGREEMENT** (“Agreement”) is made as of this \_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_, by and between the State of Maryland (“the State”), acting by and through its **TO Requesting Agency** (the “Department”), and \_\_\_\_\_ (“TO Contractor”), a corporation with its principal business office located at \_\_\_\_\_ and its principal office in Maryland located at \_\_\_\_\_.

### RECITALS

**WHEREAS**, the TO Contractor has been awarded a Task Order Agreement (the “TO Agreement”) for **TORFP Title** TORFP No. **E00P2400385** dated \_\_\_\_\_, (the “TORFP”) issued under the Consulting and Technical Services procurement issued by the Department, Project Number 060B9800035; and

**WHEREAS**, in order for the TO Contractor to perform the work required under the TO Agreement, it will be necessary for the State to provide the TO Contractor and the TO Contractor’s employees and agents (collectively the “TO Contractor’s Personnel”) with access to certain confidential information regarding \_\_\_\_\_ (the “Confidential Information”).

**NOW, THEREFORE**, in consideration of being given access to the Confidential Information in connection with the TORFP and the TO Agreement, and for other good and valuable consideration, the receipt and sufficiency of which the parties acknowledge, the parties do hereby agree as follows:

1. Confidential Information means any and all information provided by or made available by the State to the TO Contractor in connection with the TO Agreement, regardless of the form, format, or media on or in which the Confidential Information is provided and regardless of whether any such Confidential Information is marked as such. Confidential Information includes, by way of example only, information that the TO Contractor views, takes notes from, copies (if the State agrees in writing to permit copying), possesses or is otherwise provided access to and use of by the State in relation to the TO Agreement.
2. TO Contractor shall not, without the State’s prior written consent, copy, disclose, publish, release, transfer, disseminate, use, or allow access for any purpose or in any form, any Confidential Information provided by the State except for the sole and exclusive purpose of performing under the TO Agreement. TO Contractor shall limit access to the Confidential Information to the TO Contractor’s Personnel who have a demonstrable need to know such Confidential Information in order to perform under the TO Agreement and who have agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information. The names of the TO Contractor’s Personnel are attached hereto and made a part hereof as Exhibit A. Each individual whose name appears on Exhibit A shall execute a copy of this Agreement and thereby be subject to the terms and conditions of this Agreement to the same extent as the TO Contractor. TO Contractor shall update Exhibit A by adding additional names as needed, from time to time.
3. If the TO Contractor intends to disseminate any portion of the Confidential Information to non-employee agents who are assisting in the TO Contractor’s performance of the TORFP or who will otherwise have a role in performing any aspect of the TORFP, the TO Contractor shall first obtain the written consent of the State to any such dissemination. The State may grant, deny, or condition any such consent, as it may deem appropriate in its sole and absolute subjective discretion.
4. TO Contractor hereby agrees to hold the Confidential Information in trust and in strictest confidence, to adopt or establish operating procedures and physical security measures, and to take all other measures necessary to protect the Confidential Information from inadvertent release or disclosure to unauthorized third parties and to prevent all or any portion of the Confidential Information from falling into the public domain or into the possession of persons not bound to maintain the confidentiality of the Confidential Information.
5. TO Contractor shall promptly advise the State in writing if it learns of any unauthorized use, misappropriation, or disclosure of the Confidential Information by any of the TO Contractor’s Personnel or the TO Contractor’s former Personnel. TO Contractor shall, at its own expense, cooperate with the State in seeking injunctive or other equitable relief against any such person(s).
6. TO Contractor shall, at its own expense, return to the Department, all copies of the Confidential Information in its care, custody, control or possession upon request of the Department or on termination of the TO Agreement.

7. A breach of this Agreement by the TO Contractor or by the TO Contractor's Personnel shall constitute a breach of the TO Agreement between the TO Contractor and the State.
8. TO Contractor acknowledges that any failure by the TO Contractor or the TO Contractor's Personnel to abide by the terms and conditions of use of the Confidential Information may cause irreparable harm to the State and that monetary damages may be inadequate to compensate the State for such breach. Accordingly, the TO Contractor agrees that the State may obtain an injunction to prevent the disclosure, copying or improper use of the Confidential Information. The TO Contractor consents to personal jurisdiction in the Maryland State Courts. The State's rights and remedies hereunder are cumulative and the State expressly reserves any and all rights, remedies, claims and actions that it may have now or in the future to protect the Confidential Information and/or to seek damages from the TO Contractor and the TO Contractor's Personnel for a failure to comply with the requirements of this Agreement. In the event the State suffers any losses, damages, liabilities, expenses, or costs (including, by way of example only, attorneys' fees and disbursements) that are attributable, in whole or in part to any failure by the TO Contractor or any of the TO Contractor's Personnel to comply with the requirements of this Agreement, the TO Contractor shall hold harmless and indemnify the State from and against any such losses, damages, liabilities, expenses, and/or costs.
9. TO Contractor and each of the TO Contractor's Personnel who receive or have access to any Confidential Information shall execute a copy of an agreement substantially similar to this Agreement and the TO Contractor shall provide originals of such executed Agreements to the State.
10. The parties further agree that:
  - a. This Agreement shall be governed by the laws of the State of Maryland;
  - b. The rights and obligations of the TO Contractor under this Agreement may not be assigned or delegated, by operation of law or otherwise, without the prior written consent of the State;
  - c. The State makes no representations or warranties as to the accuracy or completeness of any Confidential Information;
  - d. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement;
  - e. Signatures exchanged by facsimile are effective for all purposes hereunder to the same extent as original signatures; and
  - f. The Recitals are not merely prefatory but are an integral part hereof.

**TO Contractor/TO Contractor's Personnel:**

**Comptroller of Maryland:**

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

SUBMIT AS REQUIRED IN SECTION 1.6 OF THE TORFP

Comptroller of Maryland TORFP Web Application Security Assessment E00P2400385

## ATTACHMENT 12 – TO CONTRACTOR SELF-REPORTING CHECKLIST

The purpose of this checklist is for CATS II Master Contractors to self-report on adherence to procedures for task orders (TO) awarded under the CATS II master contract. Requirements for TO management can be found in the CATS II master contract RFP and at the TORFP level. The Master Contractor is requested to complete and return this form by the **Checklist Due Date** below. Master Contractors may attach supporting documentation as needed. Please send the completed checklist and direct any related questions to [contractoversight@doit.state.md.us](mailto:contractoversight@doit.state.md.us) with the TO number in the subject line.

<b>Master Contractor:</b>	
<b>Master Contractor Contact / Phone:</b>	
<b>Procuring State Agency Name:</b>	
<b>TO Title:</b>	
<b>TO Number:</b>	
<b>TO Type (Fixed Price, T&amp;M, or Both):</b>	
<b>Checklist Issue Date:</b>	
<b>Checklist Due Date:</b>	
<b>Section 1 – Task Orders with Invoices Linked to Deliverables</b>	
<p>A) Was the original TORFP (Task Order Request for Proposals) structured to link invoice payments to distinct deliverables with specific acceptance criteria?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, skip to Section 2.)</b></p>	
<p>B) Do TO invoices match corresponding deliverable prices shown in the accepted Financial Proposal?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why) _____</b></p>	
<p>C) Is the deliverable acceptance process being adhered to as defined in the TORFP?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why) _____</b></p>	
<b>Section 2 – Task Orders with Invoices Linked to Time, Labor Rates and Materials</b>	
<p>A) If the TO involves material costs, are material costs passed to the agency without markup by the Master Contractor?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why) _____</b></p>	
<p>B) Are labor rates the same or less than the rates proposed in the accepted Financial Proposal?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why) _____</b></p>	
<p>C) Is the Master Contractor providing timesheets or other appropriate documentation to support invoices?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why) _____</b></p>	
<b>Section 3 – Substitution of Personnel</b>	

<p>A) Has there been any substitution of personnel?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, skip to Section 4.)</b></p>
<p>B) Did the Master Contractor request each personnel substitution in writing?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why)</b> _____</p>
<p>C) Does each accepted substitution possess equivalent or better education, experience and qualifications than incumbent personnel?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why)</b> _____</p>
<p>D) Was the substitute approved by the agency in writing?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why)</b> _____</p>
<p><b>Section 4 – MBE Participation</b></p>
<p>A) What is the MBE goal as a percentage of the TO value? <b>(If there is no MBE goal, skip to Section 5)</b>          %</p>
<p>B) Are MBE reports D-5 and D-6 submitted monthly?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why)</b> _____</p>
<p>C) What is the actual MBE percentage to date? (divide the dollar amount paid to date to the MBE by the total amount paid to date on the TO)          %  <b>(Example - \$3,000 was paid to date to the MBE subcontractor; \$10,000 was paid to date on the TO; the MBE percentage is 30% (3,000 ÷ 10,000 = 0.30))</b></p>
<p>D) Is this consistent with the planned MBE percentage at this stage of the project?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why)</b> _____</p>
<p>E) Has the Master Contractor expressed difficulty with meeting the MBE goal?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/>    <b>(If yes, explain the circumstances and any planned corrective actions)</b>          _____</p>
<p><b>Section 5 – TO Change Management</b></p>
<p>A) Is there a written change management procedure applicable to this TO?  <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>(If no, explain why)</b> _____</p>
<p>B) Does the change management procedure include the following?</p> <p><b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> Sections for change description, justification, and sign-off</p> <p><b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> Sections for impact on cost, scope, schedule, risk and quality (i.e., the impact of change on satisfying TO requirements)</p> <p><b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> A formal group charged with reviewing / approving / declining changes (e.g., change control board, steering committee, or management team)</p>

C) Have any change orders been executed?

Yes  No

**(If yes, explain expected or actual impact on TO cost, scope, schedule, risk and quality)**

\_\_\_\_\_

D) Is the change management procedure being followed?

Yes  No  (If no, explain why) \_\_\_\_\_



## ATTACHMENT 13 – LIVING WAGE AFFIDAVIT OF AGREEMENT

Contract No. \_\_\_\_\_

Name of Contractor \_\_\_\_\_

Address \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

### **If the Contract is Exempt from the Living Wage Law**

The Undersigned, being an authorized representative of the above named Contractor, hereby affirms that the Contract is exempt from Maryland's Living Wage Law for the following reasons: (check all that apply)

- Bidder/Offeror is a nonprofit organization
- Bidder/Offeror is a public service company
- Bidder/Offeror employs 10 or fewer employees and the proposed contract value is less than \$500,000
- Bidder/Offeror employs more than 10 employees and the proposed contract value is less than \$100,000

### **If the Contract is a Living Wage Contract**

A. The Undersigned, being an authorized representative of the above named Contractor, hereby affirms our commitment to comply with Title 18, State Finance and Procurement Article, Annotated Code of Maryland and, if required, to submit all payroll reports to the Commissioner of Labor and Industry with regard to the above stated contract. The Bidder/Offeror agrees to pay covered employees who are subject to living wage at least the living wage rate in effect at the time service is provided for hours spent on State contract activities, and to ensure that its Subcontractors who are not exempt also pay the required living wage rate to their covered employees who are subject to the living wage for hours spent on a State contract for services. The Contractor agrees to comply with, and ensure its Subcontractors comply with, the rate requirements during the initial term of the contract and all subsequent renewal periods, including any increases in the wage rate established by the Commissioner of Labor and Industry, automatically upon the effective date of the revised wage rate.

B. \_\_\_\_\_ (initial here if applicable) The Bidder/Offeror affirms it has no covered employees for the following reasons (check all that apply):

- All employee(s) proposed to work on the State contract will spend less than one-half of the employee's time during every work week on the State contract;
- All employee(s) proposed to work on the State contract will be 17 years of age or younger during the duration of the State contract; or
- All employee(s) proposed to work on the State contract will work less than 13 consecutive weeks on the State contract.

The Commissioner of Labor and Industry reserves the right to request payroll records and other data that the Commissioner deems sufficient to confirm these affirmations at any time.

Name of Authorized Representative: \_\_\_\_\_

Signature of Authorized Representative: \_\_\_\_\_

Date: \_\_\_\_\_ Title: \_\_\_\_\_

Witness Name (Typed or Printed): \_\_\_\_\_

Witness Signature & Date: \_\_\_\_\_

## **ATTACHMENT 14 – ADDITIONAL MANDATORY CONTRACT PROVISIONS**

The Comptroller of Maryland is required by the Internal Revenue Service to include the following language in contracts related to technology services:

### **I. PERFORMANCE**

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.
- (7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (8) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.
- (10) (Include any additional safeguards that may be appropriate.)

### **II. CRIMINAL/CIVIL SANCTIONS:**

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as five (5) years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as one (1) year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information* and Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

### III. INSPECTION:

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

**EXHIBIT A**

**TO CONTRACTOR'S EMPLOYEES AND AGENTS WHO WILL BE GIVEN  
ACCESS TO THE CONFIDENTIAL INFORMATION**

Printed Name and Address  
of Employee or Agent

Signature

Date

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____