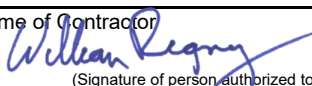
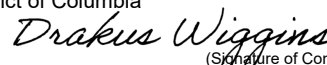


<b>AMENDMENT OF SOLICITATION / MODIFICATION OF CONTRACT</b>			1. Contract Number CFOPD-20-C-013	Page of Pages 1   1		
2. Amendment/Modification No. Modification 5	3. Effective Date See 16 C below	4. Requisition/Purchase Request No.	5. Solicitation Caption Modernized Integrated Tax System (MITS) Security Assessment Services			
6. Issued by: Office of the Chief Financial Officer Office of Contracts 1100 4 <sup>th</sup> Street, S.W. Suite E620 Washington, D.C. 20024 202-442-7012 (main)		Code	7. Administered by (If other than line 6)			
8. Name and Address of Contractor (No. street, city, county, state and zip code)  Limbic Systems, Inc. 2200 Pennsylvania Ave. NW Suite 400 Washington, DC 20037-1761 Attn: Marullus Williams, President and CEO 703-328-2977 (p) <a href="mailto:mwilliams@limbicsystems.com">mwilliams@limbicsystems.com</a>		9A. Amendment of Solicitation No.		9B. Dated (See Item 11)		
		X	10A. Modification of Contract/Order No. CFOPD-20-C-013		10B. Dated (See Item 13) January 3, 2020	
			Code		Facility	
		11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS				
<input type="checkbox"/> The above numbered solicitation is amended as set forth in item 14. The hour and date specified for receipt of Offers <input type="checkbox"/> is extended. <input type="checkbox"/> is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment: (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) BY separate letter or fax which includes a reference to the solicitation and amendment number. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such may be made by letter or fax, provided each letter or telegram makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.						
12. Accounting and Appropriation Data (If Required)						
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS , IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14						
X	A. This change order is issued pursuant to (Specify Authority): 27 DCMR Section 3601.2(c) and Section 1.8 Changes of the Contract					
	B. The above numbered contract/order is modified to reflect the administrative changes (such as changes in paying office, appropriation data etc.) set forth in item 14, pursuant to the DC Financial Responsibility and Management Assistance Authority.					
	C. This supplemental agreement is entered into pursuant to authority of:					
	D. Other (Specify type of modification and authority)					
<b>E. IMPORTANT:</b> Contractor <input type="checkbox"/> is not <input checked="" type="checkbox"/> is required to sign this document and return <u>1</u> copy to the issuing office.						
14. Description of Amendment/Modification (Organized by UCF Section headings, including solicitation/contract subject matter where feasible.)						
<p>1. The purpose of Modification No. 5 is to add Attachment A to provide MITS static application security testing and penetration testing and to replace Section B.5.5 Option Year 4 with Attachment B, with no change in the Option Year 4 not to exceed amount of \$86,856.69.</p> <p style="text-align: center;">All other terms and conditions shall remain unchanged.</p>						
Except as provided herein, all terms and conditions of the document is referenced in Item 9A or 10A remain unchanged and in full force and effect.						
15A. Name and Title of Signer (Type or print) William Rigney, VP			16A. Name of Contracting Officer Dorothy Whisler Fortune, Esq., CPPO, Drakus Wiggins, CPPB, CPPO or Anthony A. Stover, CPPO			
15B. Name of Contractor  (Signature of person authorized to sign)		15C. Date Signed 5/30/24	16B. District of Columbia  (Signature of Contracting Officer)		16C. Date Signed 06/03/2024	

## Attachment A

# 1. Static Application Security Testing (SAST) Approach and Methodology

## Approach and Methodology

1. The Contractor shall provide a complete assessment of vulnerabilities in the MITS source code, and after determining the source code vulnerabilities, a Corrective Action Plan shall be created that shall enable OCFO to honor their fiduciary and IRS responsibilities.
2. The Contractor shall act as the trusted advisor to, and to provide support for, the DC OCFO.
3. The assessment methodology shall be based on the NIST SP 500 series (Source Code Analysis), NIST Internal Report 8397 (Guidelines on Minimum Standards for Developer Verification of Software) and OWASP Static Code Analysis.
4. The Contractor shall provide the DC Government with a report that provides a comprehensive security assessment of the MITS source code. The report shall provide assessment results for the MITS C# (.NET Framework) code base and shall contain a granular assessment of compliance with relevant IRS Pub. 1075 controls.

## Tools and Techniques

5. The Contractor's approach and methodology shall consist of the following phases.

### Phase 1: Project Initiation and Documentation Gathering

6. Phase 1 shall begin with a kick-off meeting. The Contractor shall prepare a Kick-Off Presentation. The primary purpose of the kick-off meeting shall be to facilitate appropriate introductions, review task scope, validate project expectations, review the draft schedule, and coordinate next steps and action items. The Contractor shall submit a Final Schedule for review and concurrence within two weeks after the kick-off meeting.

## Phase 2: Perform Static Code Analysis

7. After the completion of Phase I, the Contractor shall take actions to perform Static Code Analysis of the MITS source code. The first action shall be to develop specific procedures for SAST testing to ensure comprehensive automated and manual testing of source code.
8. Automated testing of the MITS source code shall include the use of commercial off the shelf (COTS) and open-source software that performs input analysis of source code and compares the output to expected industry secure coding practices. The software shall include custom scanning configurations based on the MITS C# source code leveraging the .Net Framework. The software shall perform searches for the use of:
  - a. Deprecated functions
  - b. Patterns indicating possible vulnerabilities
  - c. Validation that all code implements defined functions and protocols
  - d. Control flaws and data values within the source code
  - e. Hardcoded passwords
  - f. Private encryption keys
9. In addition to running automated SAST software scanners, manual and automated open-source code analysis shall be performed using COTS and open-source software and manual review to ensure complete analysis of open-source code for malware and malformed design (potentially leading to data leakage or backdoor access).
10. The Contractor shall manage all MITS custom code in a dedicated cloud environment that ensures the confidentiality and integrity of OCFO data, source code, and scan results. All data shall be encrypted in-transit and at-rest in accordance with IRS Pub-1075 security requirements and District of Columbia OCFO security policies and procedures. Upon completion of all SAST activities, the code and reports shall be permanently removed from the cloud environment to include deleting all storage accounts. No other customer data shall be co-mingled at any time during or after the engagement.
11. Key activities shall include the following:
  - a. Draft and finalize the Rules of Engagement (ROE) to establish the Static code assessment process. The ROE shall include schedule, tools, methodology, procedures, personnel, reporting, and acknowledgement with signature authorities.
  - b. Perform automated and manual code vulnerability scans and produce scan reports to be reviewed with the customer in support of defining a snapshot of the existing security posture.

### Phase 3: Document SAST Results

12. The results of the SAST shall be summarized and included in the Initial Report (Deliverable). The Initial Report shall include the assessment methodology, assessment results, and identified risks.
13. The Initial Report shall detail the status of secure coding best practices and a detailed report of all findings obtained from the manual and automated testing activities. The Initial Report shall provide a comprehensive, granular, and detailed SAST of the MITS source code. The assessment shall be conducted in coordination with the OCFO Office of the Chief Information Officer and Tax Systems Groups.
14. The Contractor is responsible for analyzing results, researching corrective actions to remediate findings, as well as making recommendations for compensating controls. In addition, all vulnerabilities shall be assessed according to NIST SP 800-30, where the Contractor shall enumerate findings with an associated likelihood, impact, and risk level. Working collaboratively with the DC OCFO the Contractor shall recommend a timeframe for mitigating the risks (e.g., High – 30 days, Medium – 60 days and Low – 90 days or as recommended by the organization).
15. The Contractor shall also produce a Corrective Action Plan (Deliverable) with feedback from key MITS stakeholders to include information system owner(s). The Corrective Action Plan shall document all open findings, define remediation or mitigation actions, and closure requirements, i.e., start/complete dates, verification of completion.
16. Sensitive information, including scan data obtained from the testing process, shall be protected through the use of disk encryption on the Contractor equipment. In addition, the secure format and medium for the transmission of information between the Contractor and DC OCFO personnel will be agreed upon at the project kick off meeting.

### Phase 4: SAST Documentation Delivery

17. During Phase 4 the Contractor shall provide the Initial Report to DC OFCO such that the customer stakeholders can review and provide comments. Based on the finding results, DC OCFO will be given a period of time to remediate findings such that a Final Report shall be generated to include any control modifications in the environment since the initial report was generated.
18. Once the final risk assessment report has been drafted, the Contractor shall schedule a final risk assessment report briefing with DC-OCFO, Fast Enterprises, and additional key system personnel. The final Risk Assessment Report briefing shall include a comprehensive review of all findings in conjunction with providing a Correction Action Plan that addresses step-by-step processes for remediating each finding. The final Risk Assessment Report

shall include a summary of the scope of the assessment, what assessment methodologies were used, timelines completed, and personnel involved. Each finding shall include a unique ID, security control description and identifier, recommended remediation, threat, and determination of

19. Risk Score based on the likelihood X impact for the Confidentiality, Integrity, and Availability of data within MITS being compromised in accordance with NIST SP 800-30.
20. Upon completion of all Corrective Actions, multiple IV&V (Independent Verification and Validation) remediation scans for identified weaknesses and/or gaps shall be performed and updated MITS Static Code Analysis and Assessment Report provided.
21. The Contractor shall complete the Planning Tasks and provide the Deliverables in Table 1 as follows:

**TABLE 1 – DELIVERABLES**

Planning Tasks	Deliverables
1. Phases 1 & 2: Perform SAST	<ol style="list-style-type: none"> <li>1. Kick-Off Presentation</li> <li>2. Final Project Schedule</li> <li>3. Rules of Engagement (ROE)</li> </ol>
2. Phases 3 & 4: SAST Documentation Delivery	<ol style="list-style-type: none"> <li>4. MITS Static Code Analysis &amp; Assessment Report (Contract Required Deliverable)</li> <li>5. POA&amp;M / Corrective Action Plan (Contract Required Deliverable)</li> <li>6. IV&amp;V iterative scans of all source code post corrective actions</li> <li>7. MITS IV&amp;V Static Code Analysis &amp; Assessment Report (Updated)</li> </ol>

## 2. Penetration Testing Approach and Methodology

1. The Contractor's penetration testing shall identify vulnerabilities that exist in a system, application, or network that may or may not have existing security measures in place. The Contractor's penetration testing shall involve the use of testing methods conducted by trusted individuals that are similarly used by hostile intruders or hackers.
2. The Contractor shall employ real-world attack methods in an attempt to circumvent the security supporting MITS. Application testing shall be performed as an anonymous user. Testing shall involve launching real attacks on target systems. The penetration testing approach and methodology shall be based on the industry standards including Penetration Testing Execution Standard (PTES), Open-Source Security Testing Methodology (OSSTMM), NIST SP 800-115, and Technical Guide to Information Security Testing and Assessment.
3. The Contractor shall use Penetration Testing Tools from the following list:
  - a. Kali Linux – Tool suite consists of:
    - i. Information gathering
    - ii. Sniffing and spoofing
    - iii. Vulnerability analysis
    - iv. Exploitation
    - v. Password attacks
    - vi. Wireless attacks
  - b. Nmap
  - c. Wireshark
  - d. Nessus
  - e. Metasploit/Nexpose
  - f. Burp Suite Pro
  - g. Command Line Tools
4. The Contractor shall use a four-phase approach to perform the penetration testing. The figure below depicts the four-phase approach to performing penetration testing:



5. To complete a successful Penetration test, OCFO will provide all web site addresses and external IP addresses and address spaces for all edge / DMX devices. The four phases of Penetration Testing begin with the 1st Phase (Planning), the initiation of the project with the management team and the establishment of the Rules of Engagement (RoE). The 2nd phase (Discovery) includes information gathering, scanning and vulnerability analysis. The 3rd phase (Attacking) shall verify potential vulnerabilities through attempted exploit techniques. The 4th phase (Reporting) shall occur as output for all three phases with deliverables provided to OCFO.
6. Figure 2 depicts key activities within the four phases.

Planning Phase I	Discovery Phase II	Attacking Phase III	Reporting Phase IV
<ul style="list-style-type: none"><li>•Management Approval</li><li>•Rules of Engagement</li></ul>	<ul style="list-style-type: none"><li>•Information Gathering and Scanning</li><li>•Vulnerability Analysis</li></ul>	<ul style="list-style-type: none"><li>•Access</li><li>•Privilege Escalation</li><li>•System Browsing</li><li>•Additional Tools</li></ul>	<ul style="list-style-type: none"><li>•Logs</li><li>•Vulnerability Review</li><li>•Executive Briefing</li></ul>

## Planning

7. The Planning phase initiates the process and is critical to the success of the overall test. The Contractor shall use its internal project templates and Rules of Engagement (RoE) documents to work with the District and establish the project management plan, testing scope to include personnel, escalation methodology, tools, and timetables. The tests may include internal and external attempts to penetrate customer IT

infrastructure and applications.

8. During this phase, DC Government must identify the corporate point of contact(s) who is authorized to request that penetration testing be performed on third-party hosted infrastructure). The RoE shall provide detailed requirements and approvals that are required supporting scanning in-scope web sites and IT infrastructure components hosted Fast Enterprises.
9. In support of performing internal (white box) penetration testing, the Contractor shall request all internal web site addresses and resources (infrastructure edge and boundary devices) supporting the system as well as direct access to the environment.
10. For external (black box) penetration testing, the Contractor shall not request information pertaining to external IP addresses or address spaces for all edge and DMZ devices.
11. As this system is comprised of customized COTS software, penetration testing activities may be limited in scope to ONLY testing environments as provisioned by FAST Enterprises and approved by DC-OCFO.
12. The Contractor shall complete the Planning Tasks and provide the Deliverables in Table 2 as follows:

**TABLE 2 – PLANNING TASKS AND DELIVERABLES**

<b>Planning Tasks</b>	<b>Deliverables</b>
1. Project Initiation and Kick-off / Identify Stakeholders	1. Overview Kick off Meeting
2. Establish test boundaries, roles and responsibilities, and timeline	2. Rules of Engagement

## Discovery

13. The Discovery phase is the cornerstone of all activities. The Contractor shall break this phase into two execution periods. The first execution period includes gathering information about the target applications and systems. For “Black Box” testing, the Discovery Phase consists of gathering information as an external entity attempting to understand the support for MITS infrastructure components and application. This includes network port and service identification which is used to define targets. Depending on the type of testing (Black-Box vs White Box) additional information can be gathered including:



- a. **Host name and IP addresses** through the use of Network sniffing tools (Wireshark, NMAP, etc.)
  - b. **User names and contact information** by using web sites and directory services within compromised environments
  - c. **System information** by NetBIOS enumeration
  - d. **Application and service information** from banners and patch information
14. Externally facing assets, to include web sites, within the defined scope shall be tested remotely, from the perspective of an outside attacker. The Contractor shall use automated tools and manual techniques to enumerate vulnerabilities such as is identified by the Open Web Application Security Project (OWASP) Top 10 which include, but are not limited to, injections (SQL), broken authentication, security misconfigurations, and cross site scripting. In addition to externally facing assets and web sites, the Contractor shall also request internal access to web sites in an attempt to enumerate similar vulnerabilities using automated tools and manual techniques.
15. Prior to performing any automated scanning activities for capturing system information; including potential vulnerabilities, the Contractor shall review all scan tool configurations and customize any configurations based on the known environment and information gathered to reduce the potential for false positive findings. In addition, the Contractor shall use multiple automated scan tools in order to compare results and verify findings as applicable. As part of the results analysis, the Contractor shall also use manual testing, where applicable, to validate findings and reduce the potential for false positive results.
16. In support of Social Engineering activities, the Contractor shall use automated and manual testing methodologies to determine system personnel susceptibility to various Social Engineering techniques. The intent of Social Engineering during Phase 2 – Discovery is to determine potential threats that can be exploited through common practices such as impersonations through digital (e-mail, IM, phone) and non-digital (conversations via phone or in person) means to capture system information such as logins and passwords, system sensitive information, and data. Techniques used may include, but are not limited to, various forms of phishing through e-mail, websites, and impersonations through direct calling.
17. In Phase 3 – Attacking, information gained as a result of the Social Engineering techniques shall be used in an attempt to successfully access system resources, data, and / or personnel accounts.
18. The second execution period during Phase II is performing vulnerability analysis using automated vulnerability scanners and manual vulnerability test methodologies. This approach shall enable the tester to determine what vulnerabilities may be exploited during Phase III.

19. The Contractor shall complete the Discovery Tasks and provide the Outputs in Table 3 as follows:

TABLE 3 – DISCOVERY TASKS AND OUTPUTS

Discovery Tasks	Outputs
1. Information Gathering	1. Complete list of host information to be attacked including host names, IP addresses, system information, and application/service information
2. Vulnerability Analysis	2. Complete list of vulnerabilities identified per host scanned
3. Social Engineering	3. Use common techniques to determine susceptibility of personnel to phishing scams and impersonation.

## Attacking

20. This phase builds on the Discovery Phase attempting to exploit vulnerabilities based on information obtained about the web applications and publicly available IT infrastructure. During this phase, successful attacks shall validate vulnerabilities and safeguards are identified to mitigate or remediate these attack vectors. Some attacks shall grant access but do not allow privilege escalation. The tester shall then institute additional techniques to perform privilege escalation attempting to determine the actual risks of exploited vulnerabilities. Other tools may be used once an attack has been proven to be successful attempting to gain more information about the network or applications and to uncover other attack vectors and vulnerabilities.

21. Typical vulnerabilities the Contractor shall attempt to exploit may include:

- a. Web Site Vulnerabilities (Cross-site scripting, SQL injections, Cross-site Request Forgery)
- b. Misconfigurations
- c. Kernel Flaws
- d. Buffer Overflows
- e. Insufficient Input Validation
- f. Missing Vendor Application and O/S Security Patches and Fixes
- g. Incorrect and incorrectly configured File and Directory Permissions

22. Web site / External application and resource testing shall combine anonymous and

authenticated test methods, as applicable. Testing involves launching real attacks on target systems. The Contractor’s penetration testing approach and methodology shall be based on the industry standards including Penetration Testing Execution Standard (PTES), Open-Source Security Testing Methodology (OSSTMM), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, and the Open Web Application Security Project (OWASP). Successful attacks shall validate vulnerabilities and safeguards shall be identified to mitigate and / or remediate these attack vectors. Some attacks shall grant access but may not allow privilege escalation. The tester shall then institute additional techniques to perform privilege escalation attempting to determine the actual risks of exploited vulnerabilities. Other tools may be used once an attack has been proven to be successful in attempting to gain more information about the network or applications and to uncover other attack vectors and vulnerabilities. This same process would also be used for internal web sites.

23. The Contractor shall complete the Attack Tasks and provide the Outputs in Table 4 as follows:

**TABLE 4 – ATTACK TASKS AND OUTPUTS**

<b>Attack Tasks</b>	<b>Outputs</b>
1. Password Cracking (as applicable)	1. Weak passwords and password policies
2. Web Site Pen Testing	2. Unauthorized data access and web site control
3. Publicly available IT infrastructure testing	3. IT infrastructure component control and unauthorized access
4. Social Engineering (as applicable)	4. Successful application or system access and personnel accounts exploited (Insider and Outsider attempts)

## Reporting

24. The Contractor shall provide reports throughout the testing lifecycle. This includes providing system logs and vulnerability reports to customer stakeholders as requested and providing a report in support of all findings as part of Phase II and Phase III activities.

25. The Penetration Testing process shall include the following deliverables:

- a. Phase 1 – Planning – Rules of Engagement (ROE) document: The ROE shall establish the testing scope, methodology, tools, timetables, communication, and personnel involved

with this process.

- b. Phase 2 – Discovery – system information generated from automated and manual tools and techniques to include asset lists, vulnerabilities, and logs.
- c. Phase 3 – Attacking – exploits defined and validated from automated and manual tools and techniques to include compromised accounts and data accessed.
- d. Phase 4 – Reporting– Penetration Test Report (PTR): The PTR includes an Executive Summary that includes the purpose, scope, consolidated list of findings, and origin of findings. In addition to the Executive Summary, a Detailed Findings and Recommendations section is included which contains:
  - Specific vulnerability
  - Severity level (Critical, High, Moderate, Low)
  - Affected component or application
  - Origin of vulnerability
  - Finding Description
  - References
  - Source output from tool(s) or methodology
  - Recommended Mitigation or Corrective Action

26. A draft PTR shall be submitted for an on-site / remote round table review of all pen testing findings with DC-OCFO, Fast Enterprises, and all key system personnel. As part of the round table review, the Contractor shall discuss each finding based on source, assessment methodology used, and result and provide remediation or mitigation solutions. After completion of the round table review, DC-OCFO and Fast Enterprises will be provisioned additional time to provide existing evidence or artifacts and new evidence for findings that can be remediated within the provisioned timeline.

27. The PTR shall be included as part of the Security Assessment deliverable package and shall include all supporting evidence and artifacts as captured for all process Phases.

28. Penetration Tests shall be performed as requested by the Director of Tax Systems Group (OCIO) as noted in the original CLIN 404. One Penetration Test shall be performed before “Go Live” the second / third calendar quarter of 2024, and the second Penetration Test shall be performed post “Go Live” between October – December 2024.

29. The Contractor shall complete the Reporting Tasks and provide the Outputs in Table 5 as follows:

**TABLE 5 – REPORTING TASKS AND OUTPUTS**

<b>Tasks</b>	<b>Outputs</b>
1. Planning Activities	1. Rules of Engagement (Deliverable)
2. Discovery Activities	2. Scan Results / Tool logs
3. Attack Activities	3. Vulnerabilities per Device (Deliverable)

30. The roles and responsibilities shall be as follows in Table 6:

**TABLE 6 – ROLES AND RESPONSIBILITIES**

<b>Roles</b>	<b>Responsibilities</b>
Project Manager	Coordinate and submit all customer deliverables as part of the test lifecycle to include: <ol style="list-style-type: none"> <li>1. Rules of Engagement</li> <li>2. Scan Results</li> <li>3. Enumerated vulnerabilities / Tool Logs</li> <li>4. Penetration Test Report</li> </ol>
Senior Security Engineer / Pen Test Lead	<ol style="list-style-type: none"> <li>1. Lead team with the development and finalization of the Rules of Engagement</li> <li>2. Execute Discovery Phase activities to include information gathering, vulnerability analysis, and social engineering.</li> <li>3. Review results from Discovery Phase</li> <li>4. Determine exploits and methodology to perform attacks</li> <li>5. Execute Attack Phase activities</li> <li>6. Capture results from Attack Phase</li> <li>7. Compile results from Discovery and Attack Phase and draft Penetration Test Report</li> <li>8. Finalize and submit Penetration Test Report based on customer feedback</li> </ol>
Security Engineer	<ol style="list-style-type: none"> <li>1. Support Penetration Test Lead with all phases and activities as part of the testing to include:                             <ol style="list-style-type: none"> <li>a. Running automated and manual tools in support of Discovery Phase</li> <li>b. Penetration Test Plan and Penetration Test Report development support</li> </ol> </li> </ol>
DC OCFO	<ol style="list-style-type: none"> <li>1. Review, provide feedback, and approve PTP and PTR</li> <li>2. Provide and complete any required logistical matters / artifacts / access materials / internal coordination / approvals</li> <li>3. Provide subject matter experts (SMEs) in support of assessment questions and artifact requests</li> <li>4. Provide key personnel for reviewing and approval of Security Assessment Plan and Penetration Testing Rules of Engagement</li> <li>5. Coordinate with all parties for PTR and SAR reviews (round table / final) and review and approve all deliverables as part of the assessment and penetration testing processes</li> </ol>

FAST	<ol style="list-style-type: none"><li>1. Provide access to resources in support of assessments</li><li>2. Provide on-site and remote personnel (SMEs) supporting management, operational, and technical controls for MITS.</li><li>3. Provide remote collaboration with personnel for assessment and penetration testing results reviews</li><li>4. Provide prompt responses for all requested information to include review of evidence and artifacts pertaining to assessment controls.</li><li>5. Coordinate with DC-OCFO and DC-OCTO for all requirements related to penetration testing as in scope for given year.</li><li>6. Provide system access or collaboration in support of vulnerability scanning results for system infrastructure components and applications</li><li>7. Provide penetration testing support to include environment access to applications and infrastructure components, as applicable.</li></ol>
DC-OCTO	<ol style="list-style-type: none"><li>1. As applicable, receive notification from DC-OCFO and monitor all ingress / egress traffic generated in support of assessment activities, i.e., Penetration Testing (Social Engineering)</li></ol>

### 3. Payment Terms

The payment request for the Option Year 4 work herein shall be submitted as follows:

#### 1. Static Application Security Testing (SAST) Services

- b. Phases 3 & 4: SAST Documentation Delivery (Initial) (35% of total funding upon completion and CLIENT acceptance of deliverables)
  - MITS Static Code Analysis & Assessment Report
  - POA&M / Corrective Action Plan
- c. Phases 3 & 4: SAST Documentation Delivery (IV&V Iterative Scans) (15% of total funding upon completion and CLIENT acceptance of deliverables)
  - IV&V iterative scans of all source code post corrective actions.
  - MITS IV&V Static Code Analysis & Assessment Report

#### 2. Penetration Testing Services

- a. Phase 4: Reporting (25% of total funding upon completion and CLIENT acceptance of deliverables) (Initial Penetration Test prior to "Go Live")
  - Penetration Test Report (PTR)
- b. Phase 4: Reporting (25% of total funding upon completion and CLIENT acceptance of deliverables) (Second Penetration Test post to "Go Live")
  - Penetration Test Report (PTR)



**ATTACHMENT B**

**B.5.5 Option Year 4**

<b>CLIN</b>	<b>Item Description</b>	<b>Firm Fixed Unit Price</b>
401	Penetration Testing Services and Deliverables, prior to Core21 go live	\$21,714.17
402	SAST testing for Code Vulnerabilities prior to Core21 go live (Initial / IV&V Iterative Scans)	\$43,428.35
403	Penetration Testing Services and Deliverables, Post Go live	\$21,714.17
	<b>TOTAL</b>	<b>\$86,856.69</b>