HEALTH AND HUMAN SERVICES COMMISSION
CONTRACT NO. 529-18-0089-00001

AMENDMENT NO. 3

The **HEALTH AND HUMAN SERVICES COMMISSION** ("**HHSC**") and **THE GREENTREE GROUP** ("**CONTRACTOR"**), who are collectively referred to herein as the "Parties" to that certain firm-fixed-price contract for Texas Integrated Eligibility Redesign System (TIERS) Independent Verification and Validation (IV&V) Services with an Effective Date of October 27, 2017, and denominated as HHSC Contract No. 529-18-0089-00001 (the "Contract"), as amended, now desire to further amend the Contract.

WHEREAS, the Parties desire to revise **EXHIBIT D-1, VENDOR REQUIREMENTS AND STATEMENT OF WORK (SOW) FOR TIERS OPERATIONS SECURITY ASSESSMENT SERVICES (TOSAS) AND AGREED UPON EXCERPTS FROM CONTRACTOR RESPONSE**;

WHEREAS, the Parties desire to revise **EXHIBIT E-3, TOSAS COST TABLES AND RATE SCHEDULE**;

WHEREAS, the Parties desire to revise the Contract Budget; and

WHEREAS, the Parties have chosen to exercise their option to amend the Contract in accordance with **EXHIBIT C** to the Contract, **HHS UNIFORM TERMS AND CONDITIONS -VENDOR (version 2.13), SECTION 8.1, AMENDMENT**.

NOW, THEREFORE, the Parties hereby amend the Contract as follows:

1. **EXHIBIT D, STATEMENT OF WORK** to the Contract is hereby further supplemented with the addition of **EXHIBIT D-2, REVISED VENDOR REQUIREMENTS AND STATEMENT OF WORK (SOW) FOR TOSAS AND AGREED UPON EXCERPTS FROM CONTRACTOR RESPONSE**.

2. **EXHIBIT E-3, TOSAS COST TABLES AND RATE SCHEDULE** is hereby deleted in its entirety and replaced with **EXHIBIT E-4, TOSAS COST TABLES AND RATE SCHEDULE** demonstrating a reduction in Contractor fees of **$210,335.00** relative to the Contractor fees stated in **EXHIBIT E-3**.

3. **SECTION IV, BUDGET** of the Contract is hereby deleted in its entirety and replaced with the following:

   IV. BUDGET

The total amount of this Contract will not exceed **$7,714,187.29**. All expenditures under the Contract will be in accordance with **EXHIBIT E, COST AND RATE SCHEDULES** and **EXHIBIT E-4, TOSAS COST TABLES AND RATE SCHEDULE**.

4. The Contract is hereby amended to exercise **OPTION 1 TERM** in **EXHIBIT E-4, TOSAS COST TABLES AND RATE SCHEDULE**.

5. HHSC makes no guarantee of volume, usage, or total compensation to be paid under the Contract. The Contract is subject to appropriations and the continuing availability of funds.

6. This Amendment shall be effective as of the date last signed below.

7. Except as modified by this Amendment, all terms and conditions of the Contract, as amended, shall remain in full force and effect.

8. Any further revisions to the Contract shall be by written agreement of the Parties.

SIGNATURE PAGE FOLLOWS

SIGNATURE PAGE FOR AMENDMENT NO. 3
HHSC CONTRACT NO. 529-18-0089-00001

HEALTH AND HUMAN SERVICES COMMISSION

BY: DocuSigned by: Maurice McCreary F30843A81CCD41C...

Maurice McCreary

COO

DATE: February 10, 2022

THE GREENTREE GROUP

BY: DocuSigned by: Jennifer Shaefer E76CF489A29747D...

Jennifer Shaefer

Contracts Manager

DATE: February 9, 2022

THE FOLLOWING DOCUMENTS ARE ATTACHED TO AND INCORPORATED AS PART OF THE CONTRACT:

EXHIBIT D-2: REVISED VENDOR REQUIREMENTS AND STATEMENT OF WORK (SOW) FOR TIERS OPERATIONS SECURITY ASSESSMENT SERVICES (TOSAS) AND AGREED UPON EXCERPTS FROM CONTRACTOR RESPONSE

EXHIBIT E-4: REVISED TIERS OPERATIONS SECURITY ASSESSMENT SERVICES (TOSAS) COST TABLES AND RATE SCHEDULE

EXHIBIT D-2: REVISED VENDOR REQUIREMENTS AND STATEMENT OF WORK (SOW) FOR TIERS OPERATIONS SECURITY ASSESSMENT SERVICES (TOSAS) AND AGREED UPON EXCERPTS FROM CONTRACTOR RESPONSE

TEXAS HEALTH AND HUMAN SERVICES COMMISSION

AMENDED CONTRACT: TIERS IV&V SERVICES

HHSC CONTRACT NO. 529-18-0089-00001

1. DESCRIPTION OF SERVICES/STATEMENT OF WORK (SOW)

1.1. ANNUAL SECURITY CONTROLS ASSESSMENT ATTESTATION

Contractor will conduct up to one (1) annual Minimal Acceptable Risk Standards for Exchanges (MARS-E) Version 2.0 or later security and privacy controls assessment engagements during the contract term. Each Assessment will produce a *Security and Privacy Assessment Report (SAR)* of approximately twenty-six (26) security and privacy controls families against approximately eighteen (18) Texas Integrated Eligibility Redesign System (TIERS) Data Center Services and Operations (DCS&O) platforms. Assessment documentation is due to HHSC no later than 30 days prior to the HHSC due date to CMS each engagement year, or as mutually agreed. CMS assessment due dates are published in the *CMS MARS-E Timelines and Artifacts List*, and based on the state's Authority to Connect renewal date, which is 3/09/2023 for HHSC TIERS.

The Contractor assessment engagement period is four months for the assessment, and one month for documentation. Federal Fiscal Years 2022 and 2023 (Years Three and One, below) were included as an Option under the Amendment 2 SOW in Exhibit D-1, that HHSC is electing to exercise under Amendment 3. Due to CMS changes to the Authority to Connect schedule published in August 2021, Exhibit D-2 updates the SOW schedule and associated deliverables, and removes deliverables provided under the initial term.

HHSC will provide the Contractor at a minimum thirty (30) days' notice if it elects to exercise the Termination for Convenience clause included in the Contract Uniform Terms and Conditions.

Table 1: Security Assessment Services Schedule

Federal Fiscal Year	Security Assessment Service
2022	Year Three (Y3) Attestation of Security Controls - will encompass approximately 608 individual security and privacy control elements.
2023	Year One (Y1) Attestation of Security Controls - due to CMS schedule changes, the Y1 Attestation does not fall within the scope of this contract. Other TOSAS work will be performed in 2023 in accordance with the Contract.

Contractor may be required to perform assessments on the following platforms including but not limited to:

1. CISHHS – Chief Information Security Office, HHS
2. CTOHHS – Chief Technology Officer, HHS
3. DEVAPP – Development, Applications
4. FACDCS – Facilities, Data Center Services
5. FACSDC – Facilities, San Angelo Data Center
6. FACWDC – Facilities, Winters Data Center
7. IAMAPP – Identity Access Management, Applications
8. LNXDCS – Linux, Data Center Services
9. MDWOPS – Middleware, Operations
10. MGROPS – Manager Operations
11. NTWDCS – Network, Data Center Services
12. NTWOPS – Network, Operations
13. ORCOPS – Oracle, Operations
14. PRVHHS – Privacy, HHS
15. SLRDCS – Solaris, Data Center Services
16. SPMOPS – Security Program Management, Operations
17. WINDCS – Windows, Data Center Services
18. WINOPS – Windows, Operations

The CMS document suite of guidance, requirements, and templates known as (MARS-E) is located at the following link:

http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/4-MARS-E-v2-0-AE-ACA-SSP-11102015.pdf.

Contractor will comply with the current guidance provided by CMS as outlined in the *Framework for the Independent Assessment of Security and Privacy Controls*. The Contractor will use the *Security and Privacy Assessment Report (SAR)* and the *Security and Privacy Assessor Workbook (SAW)* as directed by CMS. The Contractor will support HHSC with the completion of the *Annual Security and Privacy Attestation Memorandum*.

Contractor will provide a descriptive analysis of the vulnerabilities identified throughout the assessment process. For each vulnerability identified, a suggested corrective action plan must be included to help reduce the impact of each discovered vulnerability. A business risk level assessment value must be assigned to each identified vulnerability, an Ease-of-Fix and Estimated Work Effort values must be assigned to demonstrate how simple or difficult it might be to complete the reasonable and appropriate corrective actions required to close or reduce the impact of each vulnerability.

Contractor will notify the TIERS Information Systems Security Officer (ISSO) and the platform's Subject Matter Expert (SME) of the discovered vulnerability, develop a suggested corrective action plan, and document each open control's status in the weekly report. The suggested corrective action plan may be used to populate the Plan of Action and Milestone (POA&M) document for submission to CMS by HHSC.

Contractor will review security exceptions to validate the TIERS ISSO, Chief Information Security Officer (CISO) and executive management's acceptance of risk for a particular control and indicate management's acceptance of risk within the SAR. Contractor will document in the SAR the exception form ID number, the risk type (as indicated on the Evidence Tracking Form) and any compensating controls or risk response plan included within the exception form.

Contractor will work with HHSC to solidify evidentiary documentation to pass a control or help with further understanding on how to remediate said control. Contractor will provide a Risk Assessment associated with any findings as a result of each Assessment as indicated in the Framework of Independent Assessment of Security and Privacy Controls published by CMS.

Contractor will complete the annual attestation memorandum identified in the CMS Annual Security and Privacy Attestation Procedures for the Affordable Care Act Information Systems. Contractor will work with the TIERS ISSO to develop the weakness identifiers for discovered vulnerabilities.

1.2. VENDOR REQUIREMENTS

Contractor will work with the TIERS ISSO and designated platform SMEs to determine whether submitted evidence supports that the controls are in place, relevant and sufficient to indicate a "pass" or not sufficient indicating a "fail", and document detailed findings for each platform's control in the SAR.

Contractor will document controls indicated as a "fail" in the TIERS Security Evidence Collection and Tracking SharePoint (E-CATs) site or other HHSC approved Evidence Collection tracking tool. For each control element in-scope in E-CATs, Contractor must document that the control is either in-place or not-in-place, indicate that the implementation evidence provided is either sufficient or insufficient, recommend what additional evidence may be needed and what remediation of the control may be needed to obtain a "pass" against the control. State staff will remediate the control and upload evidence that the control is in-place in E-CATs. Contractor will validate the updated control status in E-CATs and in the SAR.

HHSC considers the SAR and SAW living documents until the final versions are accepted by HHSC. Throughout each engagement, Contractor will make every effort to ensure the requirements of each control are satisfied for each platform by working with the TIERS ISSO and platform SMEs. For any control that is found to be a fail or for which the evidence supporting that the control is in place is found to be insufficient, Contractor will indicate the status of the control for each platform on the TIERS E-CATs site and in the SAR/SAW. As Platform Owners provide additional evidence of remediation of controls, Contractor will re-assess newly remediated controls for compliance and update the SAR/SAW accordingly up to and including the mutually agreed upon Evidence Final Due Date.

Contractor will comply with current CMS and TIERS DCS&O assessment guidance, use CMS provided templates and follow CMS security and privacy control assessment methodology as found in its *Framework for Independent Assessment of Security and Privacy Controls, Security and Privacy Assessment Plan (SAP), Security and Privacy*

Assessment Report, *Security and Privacy Assessor Workbook*, *Annual Security and Privacy Attestation Memorandum*, and any further required processes, procedures, forms, or templates promulgated by CMS applicable to this SOW.

During the assessment process, Contractor will utilize:

1. The latest National Institute of Standards and Technology (NIST) Special Publications 800-53A Revision Assessing Security and Privacy Controls in Federal Information Systems and Organizations (or any future adopted versions) found at the following link: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf
2. Additionally, Contractor will utilize the Assessment Methods and Objects defined in the most current version of Volume II: Minimum Acceptable Risk Standards for Exchanges found at the following link: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance#MinimumAcceptableRiskStandards

The assessment methods must consist of interviews with the owners from approximately eighteen (18) platforms examining policies, processes and procedures, and testing of controls as outlined in the guidance documents.

1.3. WEEKLY METRICS REPORTING

HHSC TIERS collects and maintains all evidence for all controls in an HHSC approved Evidence Collection tracking tool. Contractor will ensure all activity performed against any control is properly updated in the site to support generation of weekly metric reports used to produce a dashboard on the progress of the attestation assessment. The report indicates by platform, the number of controls failing, and the number of controls remaining where work is in progress. Figure 1 – HHSC Weekly Metrics Report is a sample of how the weekly metrics report might appear; actual reporting may differ as mutually agreed.

Figure 1 - HHSC Weekly Metrics Report

Metric	CISHHS	CTOHHS	DEVAPP	FACDCS	FACSDC	FACWDC	IAMAPP	LNXDCS	MDWOPS	MGROPS	NTWDCS	NTWOPS	ORCOPS	PRVHHS	SLRDCS	SPMOPS	WINDCS	WINOPS	Totals
Count	15	12	3	21	29	34	83	94	1	1	87	139	90	68	106	207	66	97	1153
Inherited, Out-of-Scope, N/A	1	6	2	16	23	27	19	36	1	1	30	20	17	21	20	44	14	20	318
Count in-Scope	14	6	1	5	6	7	64	58	0	0	57	119	73	47	86	163	52	77	835
Pending Platform Owner	14	6	0	3	2	1	1	7	0	0	1	2	16	2	15	15	3	20	108
% Platform Complete	0.0%	0.0%	100.0%	40.0%	66.7%	85.7%	98.4%	87.9%	100.0%	100.0%	98.2%	98.3%	78.1%	95.7%	82.6%	90.8%	94.2%	74.0%	87.1%
Pending Review	0	0	0	0	24	0	0	0	0	0	0	0	0	0	0	0	0	0	24
TPA Assessed - Accepted	1	6	3	15	3	33	80	85	1	1	84	136	71	56	87	186	62	76	986
TPA Assessed - Rejected	4	1	0	2	2	1	1	4	0	0	1	2	16	2	15	8	3	15	77
% TPA Assessed	33.3%	58.3%	100.0%	81.0%	17.2%	100.0%	97.6%	94.7%	100.0%	100.0%	97.7%	99.3%	96.7%	85.3%	96.2%	93.7%	98.5%	93.8%	92.2%

Contractor will ensure all activity associated with collection, evaluation, determination of, or findings associated with all evidence submitted, is properly updated in the HHSC approved Evidence Collection tracking tool.

Contractor will document in a Weekly Progress Report, details of each platform's control that has been assessed and rejected. As Platform Owners respond with additional evidence of that control's implementation, Contractor will re-evaluate that control and if that control's evidence is determined to be acceptable, that previously rejected control's details

will be identified on the weekly report for one week as being accepted and thereafter may be removed from the report.

Contractor will report the details of any delays or issues impacting the project in any way in the Weekly Progress Report. Contractor will also report how the issue is being corrected, or how the risk is being mitigated, to the ISSO within 24 hours of discovery.

Contractor will escalate any identified issues with any HHSC resources that cause, or may potentially cause, project delays to the ISSO or TIERS PM within 24 hours of discovery.

1.4. DELIVERABLES

To meet the objectives of the SOW, the Contractor must provide deliverables as described to meet applicable business, technical, security, management, and administrative objectives. The deliverables must also align with objectives of the enterprise service delivery model, and support HHSC's ability to deliver future sustainable services.

Table 2 below summarizes the Deliverables that Contractor will provide during each Engagement year of the project.

Table 2 - Deliverables

Deliverable No.	Deliverable Name	Frequency	Description
DEL-001	TOSAS Security Project Work Plan	Within seven (7) calendar days after the Start Date for Engagement Year 1 and each engagement period thereafter.	The Security Project Work Plan must include at a minimum: 1. A detailed schedule in MS Project for key activities including project tasks, and deliverables. 2. A logical sequence of tasks and deliverables. 3. A clear narrative definition of each task and deliverable. 4. Staff assignments for each task and deliverable. 5. A specific target completion date for each task and deliverable, at a minimum to include: a. Project Kickoff b. Initial Evidence Submit By Date, c. Initial Review of Evidence Submission Date, d. Final Remediated Evidence Submit Date, e. Final Review Date f. SAR and SAW Due Date. 6. Task and deliverable relationships and dependencies. 7. Identification of the critical path for the work plan to allow for the determination of impacts to any schedule slippage.

Deliverable No.	Deliverable Name	Frequency	Description
			8. The Security Project Work Plan "actual" schedule is expected to be maintained current on at least a weekly basis.
DEL-002	*Security and Privacy Assessment Plan (SAP)*	At least 30 days prior to Assessment kickoff.	The SAP documents testing parameters to validate the security and privacy controls for TIERS. The information included within this SAP will assist in the preparation of the *Security and Privacy Assessment Report (SAR).* The SAP describes the Security Control Assessment methodology, schedule, and requirements the Contractor will use to evaluate the TIERS system. The goal of the Security and Privacy Assessment Plan is to clearly explain the information the Contractor expects to obtain prior to the assessment, the areas that will be examined, and the proposed scheduled activities the Contractor expects to perform during the assessment. The SAP must be jointly completed and agreed to before the start of the assessment by both TIERS IT and the Contractor. To expedite the process, this may be done during an assessment kickoff meeting.
DEL-003	TOSAS Monthly Progress Report	Monthly during each engagement period.	1. Provide updates on the progress of attestation assessment. 2. Identify and communicate risk and vulnerabilities with mitigating strategy to HHSC. 3. Security Project Work Plan updates including percent complete or changes to task and duration. 4. Planned activities for resource for following month.
DEL-004	TOSAS Weekly Progress Report	Weekly during Phase I	1. Provides updates on the progress of the attestation assessment 2. Will be delivered using mostly dashboards, tables, and graphs 3. Documents the status of each security control and details of each control that has been assessed and rejected 4. Reports on any identified risks or roadblocks that may impact the project along with mitigation strategies
DEL-005	*Security and Privacy Assessment Report (SAR)*	Each engagement period at the end of Phase I.	Contractor will produce for each Engagement, the SAR conforming to the requirements of this Statement of Work. The Contractor will prepare the SAR using the sample SAR report structure found in the *CMS Framework for the Independent Assessment of Security and Privacy Controls*.

Deliverable No.	Deliverable Name	Frequency	Description
			The SAR is due to the TIERS ISSO prior to the end date of Phase I. The content of the SAR will include management information to assist HHSC to render informed decisions. These decisions will assist HHSC in application of resources and staffing to correct system weaknesses and vulnerabilities. 1. The SAR will include, but is not limited to, the following information: a. Executive Summary b. Background c. Assessment Scope d. Summary of Findings e. Summary of Recommendations **2. Risk Assessment Report** Risk assessment reporting, remediation, and compensating controls recommendations a. Assessment Methodologies b. Test and Analysis c. Business Risk Reporting **3. Annual Security and Privacy Attestation Memorandum** Contractor will produce for each Engagement, the *Annual Security and Privacy Attestation Report* found in the *CMS Annual Security and Privacy Attestation Memorandum*.
DEL-006	*Security and Privacy Assessor Workbook (SAW)*	Each engagement period at the end of Phase I.	The SAW is to be completed during the assessment process. It contains the raw data and detailed findings to support the content of the SAR. It is to be submitted alongside the SAR at the end of the assessment period (Phase I).
DEL-007	TOSAS MARS-E Control Scoping Analysis	Contract Years 2022 and 2023	Report for misplaced, or out-of-scope controls. Delivery will take place prior to the 2022 assessment for Y3 controls and within calendar year 2023 for Y1 controls. The report will include: 1. Identification of misplaced controls 2. Recommendation of platform(s)/ owner(s) reassignment 3. Identification of controls that are out of scope for TIERS (such as agency controls)
DEL-008	TOSAS Evidence Automation	Contract Years 2022 and 2023	Guidelines for determining which evidence to use, based upon control type. Analysis of Y3 and Y1 controls to identify needed artifacts for the fulfillment of control requirements. Delivery will take place two month prior to

Deliverable No.	Deliverable Name	Frequency	Description
			2022 assessment for Y3 controls and within calendar year 2023 for Y1 controls.
DEL-009	TOSAS MARS-E 2.2 Gap Analysis	Contract Year 2023	Contractor will analyze new MARS-E 2.2 requirements and perform a gap analysis between current 2.0 and upcoming 2.2 standards. In addition, the report will highlight: 1. Restrictions between IS controls vs CMS controls a. The most restrictive control overlays and baselines 2. HHSC readiness to retain ATC after adoption of 2.2 standard

2. AGREED UPON EXCERPTS FROM THE GREENTREE GROUP RESPONSE

2.1. THE GREENTREE GROUP PROPOSED SOLUTION

As the selected Contractor, The Greentree Group fully understands the skills and requirements needed to successfully conduct and deliver security and privacy controls assessments. Greentree will staff the TOSAS project with 3 resources, known as the Security Team. The Security Team will be comprised of one full-time resource who will be the Security Team Lead for the TOSAS project and two additional resources who will be full-time during Phase I activities. The TIERS IV&V Team and the proposed Security Team will both be managed by the TIERS IV&V Project Manager to coordinate management, communication, and deliverables between the two projects. To minimize the impact of project ramp up time, the TIERS IV&V team members may provide knowledge transfer to the proposed Security Team to help them gain a better understanding of the TIERS organization and IT posture. Our Security Team will be tasked with conducting annual Minimal Acceptable Risk Standards for Exchanges (MARS-E) Version 2.0 or later security and privacy controls assessment engagements during the duration of the existing contract. The result of each engagement will be a *Security and Privacy Assessment Report* and *Security and Privacy Assessor Workbook* due to the TIERS Operations and TIERS Security stakeholders (or TIERS IT) based on timelines defined in the *CMS Security and Privacy MARS-E Timelines and Artifacts List*.

The Security Team will also be tasked with providing a SAP that will follow the reporting template provided by CMS for each assessment year. This plan will comply with the current guidance provided by CMS as outlined in the Framework for Independent Assessment of Security and Privacy Controls and will adhere to the Security and Privacy Report Template published by CMS. In addition, Greentree will monitor how TIERS IT adheres to the current or latest version of the CMS MARS-E and applicable HHS Information Security Controls.

Greentree envisions the delivery of the scope of work in two distinct periods of performance for each assessment (or calendar) year.

Phase I: Assessment Period

During the Assessment Period, which encompasses approximately 5 months of work during each assessment year, as the selected Contractor, Greentree will staff this effort with 3 resources. These 3 resources, known as the Security Team, will be 100% dedicated to the TOSAS project during this phase and will work diligently to deliver the Security and Privacy Assessment Report before its due date to HHSC.

As part of the assessment, the proposed Security Team will also be tasked to perform the following activities:

1. Conduct an annual Minimal Acceptable Risk Standards for Exchanges (MARS-E) Version 2.0 or later security and privacy controls assessment during Phase I of each assessment year
    a. Before the assessment begins, the Security Team will submit a completed *Security and Privacy Assessment Plan (SAP)* to HHSC and CMS per CMS' latest requirements.
    b. The output of the assessment will produce a *Security and Privacy Assessment Report (SAR)* and a *Security and Privacy Assessor Workbook (SAW)* to be delivered to TIERS IT no later than the date agreed upon with HHSC in order to meet with CMS-published deadlines.
    c. Utilize the latest revision of the National Institute of Standards and Technology (NIST) Special Publication 800-53A Assessing Security and Privacy Controls in Federal Information Systems and Organizations; the Assessment Methods and Objects defined in the most current version of Volume II: Minimum Acceptable Risk Standards for Exchanges; and applicable HHS IS-Controls.
2. Provide a descriptive analysis of the vulnerabilities identified throughout Phase I and notify the TIERS Information Systems Security Officer (ISSO) and the platform's Subject Matter Expert (SME) of the vulnerabilities
    a. Depending on the criticality of the identified vulnerability, we will notify the ISSO and SME in real-time; lower criticality vulnerabilities will be first communicated in the TOSAS Weekly Progress Report. Higher criticality findings discovered will be notified to TIERS ISSO immediately.
    b. Develop a suggested corrective action for each vulnerability identified to help reduce the impact of each discovered vulnerability and document each open control's status in the TOSAS Weekly Progress Report. *An open control is a security control that has not been satisfied in the current configuration, process, or policy.*
        i. The information in the TOSAS Weekly Progress Report will be delivered using dashboards, tables, and graphs where applicable.
        ii. Supporting details and other critical information will be documented in a narrative in the progress report.
    c. Assign a business risk level assessment value to each identified vulnerability.
    d. Identify appropriate corrective actions required to close or reduce the impact of each vulnerability.
3. Review security exceptions to validate the TIERS ISSO, Chief Information Security Officer (CISO), and executive management's acceptance of risk for a particular control and indicate management's acceptance of risk within the SAR

   a. Document in the SAR/SAW the exception form ID number, the risk type (as indicated on the Evidence Tracking Form), and any compensating controls or risk response plan included within the exception form and sign the SAR report
4. Work with HHSC to solidify evidentiary documentation to pass a control or help with further understanding on how to remediate said control
   a. Determine whether submitted evidence supports that the controls are in place, relevant, and sufficient to indicate a "pass" or not sufficient indicating a "fail" and document detailed findings for each platform's control in the SAR/SAW
      i. Document controls indicated as a "fail" in the TIERS Security Evidence Collection and Tracking SharePoint (E-CATs) site or other HHSC-approved Evidence Collection tracking tool
      ii. Document for each control element in-scope in E-CATs that the control is either in-place or not-in-place; indicate that the implementation evidence provided is either sufficient or insufficient; recommend what additional evidence may be needed; and what remediation of the control may be needed to obtain a "pass" against the control
      iii. Validate the updated control status in E-CATs and in the SAR once HHSC remediates the control and uploads evidence that the control is in-place in E-CATs
   b. Provide a Risk Assessment associated with any findings as a result of each Assessment as indicated in the Framework of Independent Assessment of Security and Privacy Controls published by CMS
5. Complete the annual attestation memorandum identified in the CMS Annual Security and Privacy Attestation Procedures for the Affordable Care Act Information Systems
   a. Work with the TIERS ISSO to develop the weakness identifiers for discovered vulnerabilities
6. Interview platform owners and examine policies, processes and procedures, and testing of controls as outlined in the guidance documents
7. Deliver a TOSAS Monthly Progress Report with updates on the progress of the attestation assessment, identified risks and vulnerabilities with mitigation strategies, updates to the Security Project Work Plan, and planned activities for the following month
   a. Conduct recurring meetings to discuss the TOSAS Monthly Progress Report

Phase II: Monitoring Period

After the delivery of the SAR and SAW at the end of Phase I, two SME resources from the Security Team will drop off the project. During the Monitoring Period, which encompasses approximately 7 months of work during each assessment year, as the selected Contractor, Greentree will staff this effort with the Security Team Lead (one of the 3 resources from the Security Team). This resource will remain 100% dedicated to the TOSAS project throughout the Monitoring Period. Although activities and tasks during Phase II are expected to be lighter than the surge of work in the Assessment Period, TIERS IT will benefit from having a dedicated resource to observe additional work after the SAR and SAW are delivered at the end of Phase I. The Security Team Lead will continue to delivery Monthly Status Reports throughout Phase II.

Activities and tasks associated with this period include the following:

1. Attend key meetings and participate in discussions with TIERS IT on the status of open controls
2. Provide input on suggested corrective action plans for open controls
3. Validate TIERS IT's plans to remediate known vulnerabilities in accordance with CMS guidance and deadlines
4. Continue to report activities and open control statuses in TOSAS Monthly Progress Reports
5. Support HHSC SMEs by reviewing and providing independent assessment regarding the Evidence required to update the Plan of Action and Milestones (POA&M) findings
6. Monitor changes to CMS MARS-E version and its impacts on future assessment
7. Support HHSC in developing a response to post-SAR comments from CMS
8. Approve POA&M findings that meet or exceed MARS-E 2.0 or later requirements
9. Provide lessons learned and process improvement recommendations for future Phase I assessments
10. Assist in adding, modifying, removing, and rescoping controls to applicable platforms and deliver a MARS-E Control Scoping Report to HHSC in 2022 and 2023
11. Support automation of processes and tools (such as E-CATS and the assessment process)
12. Assist in the migration of MARS-E 2.0 to 2.2 standard
    a. Output is a MARS-E 2.2 Gap Analysis Report to be delivered in 2023
13. Automate evidence gathering process for platform owners
    a. Output is an Evidence Automation Report to HHSC in 2022 and 2023

2.2. DELIVERABLES AND WORK PRODUCTS

To meet the objectives of this SOW for TOSAS, the Contractor will provide additional deliverables to meet applicable business, technical, security, management, and administrative objectives. The deliverables will align with objectives of the enterprise service delivery model and support HHSC's ability to deliver future sustainable services.

In addition, Greentree acknowledges and accepts the following key performance measures and will deliver all work products at an acceptable quality level and in a manner consistent with acceptable industry standard, custom, and practice. Greentree recognizes that there will be liquidated damages for any non-conformance to any key performance measure listed in Table 33 below. The deliverable acceptance process will adhere to the agreed-upon process as stated in the original TIERS IV&V Services Contract.

Table 3 Key Performance Measures (KPMs)

KPM	KPM Name	Performance Evaluated	Non-Conformance	Frequency of Measurement
KPM - 01	Deliverable Timeliness	Each Deliverable identified in 2.1.4 must be submitted by the date specified in the HHSC-accepted Security Project Work Plan	Liquidated Damages in the amount of $100 for each day of non-conformance, not to exceed $3,000 in any given month.	Monthly
KPM-02	Resource Vacancy	At a minimum, Contractor must provide the number of FTEs identified for each Resource Role in the Security Project Work Plan for each month of the Engagement.	Liquidated Damages in the amount of $1000 for each Resource Role vacancy in any given Engagement month.	Monthly

The following deliverables will be delivered as part of the TOSAS project:

TOSAS Security Project Work Plan: Within seven (7) calendar days after the signed Contract amendment and each assessment year thereafter, Greentree will deliver a TOSAS Security Project Work Plan to include a detailed schedule in MS Project for key activities, project tasks, and deliverables. Staff assignments and target completion dates will be allocated for each task and deliverable. The Security Project Work Plan "actual" schedule will be maintained on a weekly basis and included in the TOSAS Weekly and Monthly Progress Reports during Phase I. The Security Project Work Plan schedule will be maintained on a monthly basis and reported on in the TOSAS Monthly Progress Report during Phase II.

***Security and Privacy Assessment Plan*:** At least 30 days prior to the Assessment kickoff, Greentree will deliver an SAP. The SAP must be jointly completed and agreed to before the start of the assessment by both TIERS and the Contractor. To expedite the process, this may be done during an assessment kickoff meeting. The SAP documents testing parameters to validate the security and privacy controls for TIERS. The information included within this SAP will assist in the preparation of the *Security and Privacy Assessment Report*.

The SAP describes the Security Control Assessment methodology, schedule, and requirements the Contractor will use to evaluate the TIERS system. The goal of the SAP is to clearly explain the information the Contractor expects to obtain prior to the assessment, the areas that will be examined, and the proposed scheduled activities the Contractor expects to perform during the assessment.

TOSAS Weekly Progress Report: The TOSAS Weekly Progress Report will be delivered on each Monday following the conclusion of the previous week unless otherwise agreed upon with HHSC. The TOSAS Weekly Progress Reports will only be delivered during Phase I of each assessment year. The content of the TOSAS Weekly Progress Report will be communicated through dashboards, tables, and metrics as applicable. Components of the progress report will include:

- Details of each platform control that has been assessed and rejected

- Reevaluation of each control as new evidence is provided by platform owners to determine if acceptable
- Reports on any identified risks or roadblocks that may impact the project along with mitigation strategies

TOSAS Monthly Progress Report: The TOSAS Monthly Progress Report will be delivered at the start of each month throughout the entire duration of each assessment year. The details will include updates on the progress of the assessment, identified risks and vulnerabilities with mitigating strategies, Security Project Work Plan updates (including percent complete or changes to task/duration), and planned activities for the following month. The required delivery, frequency, and approval of the monthly progress report will follow what is outlined in the agreed-upon in the original TIERS IV&V Services Contract SOW #1 unless otherwise stated.

***Security and Privacy Assessment Report*:** For each assessment year throughout the duration of the contract, the SAR will conform to the requirements of the SOW for TOSAS and will be delivered to the TIERS ISSO no later than 30 days prior to the HHSC due date to CMS, or by a CMS-approved extension date. At a minimum, the SAR will include the following information:

- Executive Summary
- Background
- Assessment Scope
- Summary of Findings
- Summary of Recommendations

A component of the SAR will also include a Risk Assessment Report and the Annual Security and Privacy Attestation Memorandum.

***Security and Privacy Assessor Workbook*:** The SAW is to be completed during the assessment process. It contains raw data and further details that support the content of the SAR. It is to be submitted alongside the SAR at the end of the assessment period (Phase I).

TOSAS MARS-E Control Scoping Analysis*:* The purpose of this report is to identify misplaced and out-of-scope controls. The report will include the identification of misplaced controls, recommendations for platform owner(s) reassignment, and identification of controls that are out of scope for TIERS (such as Agency controls). This report will be delivered prior to the start of the assessment period in 2022 for the Y3 controls and within the calendar year of 2023 for Y1 controls. The 2023 delivery date will be mutually agreed upon with TIERS IT.

TOSAS Evidence Automation Report*:* This report will contain guidelines for determining which evidence to use based on control type. The report will also identify which artifacts are needed to fulfill control requirements. The report will be delivered approximately two (2) months before the start of the assessment period in 2022 and will cover the Y3 controls. The report will be delivered during the calendar year of 2023 for Y1 controls. The 2023 delivery date will be mutually agreed upon with TIERS IT.

TOSAS MARS-E 2.2 Gap Analysis Report*:* The contractor will analyze the new MARS-E 2.2 requirements and perform a gap analysis between the current 2.0 standards

and the latest 2.2 version. In addition, the report will highlight the restrictions between Information Security (IS) controls versus CMS controls and will identify HHS' readiness to retain their ATC after adoption of the version 2.2 standards. This report will be delivered in 2023 on a delivery date mutually agreed upon with TIERS IT.

Responsibilities for Submission:

For all sections in which the Contractor is responsible, the SAR and SAW will be completed by the Security Team; however, some sections of the SAR template are the responsibility of HHSC to complete (e.g., vulnerability scan results, penetration test results, etc.). The Security Team Lead will submit the Contractor-completed sections of the SAR and SAW to TIERS stakeholders before the end of the assessment period (date agreed upon by Greentree and HHSC), and it will be the responsibility of HHSC to enter the results of the scans and penetration tests into the SAR before HHSC submits to CMS.

All sections under the responsibility of the Contractor will be complete before submission to HHSC, and HHSC must complete the remaining sections before their submission to CMS.

The following Figure 2 shows the deliverable timelines associated with this effort.

FFY 2022, Y3 Assessment												
Deliverable/Task (2022)	January	February	March	April	May	June	July	August	September	October	November	December
TOSAS Security Project Work Plan												
TOSAS Security Project Work Plan Updates												
TOSAS MARS-E Control Scoping Analysis												
TOSAS Evidence Automation Report												
Security and Privacy Assessment Plan (SAP)												
TOSAS Weekly Progress Report												
TOSAS Monthly Progress Report												
Security Assessment Report (SAR)												
Security Assessment Workbook (SAW)												
FFY 2023, Y1 Assessment												
Deliverable/Task (2023)	January	February	March	April	May	June	July	August	September	October	November	December
TOSAS Security Project Work Plan												
TOSAS Security Project Work Plan Updates												
TOSAS MARS-E Control Scoping Analysis												
TOSAS Evidence Automation Report												
TOSAS MARS-E 2.2 Gap Analysis Report												
TOSAS Monthly Progress Report												

Legend			
	Full Security Team (3 resources) engaged for Phase I		Security Team Lead engaged for Phase II

Figure 2 – Proposed New Deliverables Timeline

In Figure 2, The Greentree Group, as the selected Contractor, has proposed a timeline for the deliverables and tasks associated with the TOSAS project. The timeline above is a representative schedule for the deliverables associated with Phase I and Phase II. The 5-month Phase I period (shown in blue) may not always take place during the represented months above. Phase I will be adjusted (when needed) due to contractual reasons, possible CMS deadline changes, etc. HHSC will notify The Greentree Group approximately 45 days in advance of the start date for Phase I if HHSC and CMS agree to shifting the 5-month term. The Security Project Work Plan will set the exact calendar dates for Phase I and Phase II.

By executing this SOW for TOSAS, HHSC has committed to the scope of work set of deliverables as outlined in Assessment Year 3 and Assessment Year 1 (calendar years 2022 and 2023) as a combined option set.

In the proposed timeframe, the items in blue show Phase I – Assessment Period where the entire Security Team will be engaged, while the green items represent Phase II – Monitoring Period when only the Security Team Lead will be on the TOSAS project. During Phase II, the Security Team Lead will be solely responsible for the delivery of the TOSAS Monthly Progress Report. Refer to section 2.0 of this document for a detailed list of activities associated with each phase of the project. There will not be a TOSAS Weekly Progress Report delivery during Phase II.

By leveraging this approach, The Greentree Group is able to ramp up and dial back down our team to provide HHSC with the most effective means to successfully complete all deliverables while being cost efficient. Greentree has performed all these activities successfully in commercial, Federal, and State government environments. We know how to set a strong plan in place, adjust when necessary, and roll up our sleeves to deliver.

2.3. STAFFING APPROACH

The key to successful HHSC support is our highly qualified Security Team. Greentree has specifically designed a staffing approach for HHSC that is built for success. Our approach is a “best of breed” 3-person Security Team - mixing one full-time, dedicated resource with two additional surge support SMEs from January to May (approximately) of each assessment year (Phase I). The result is a Security Team with the experience to exceed the SOW for TOSAS expectations, structured with the flexibility to maintain momentum and tackle new challenges as they arise.

The TOSAS project will be led by the dedicated full-time resource, also known as the Security Team Lead, and will be the primary point of contact for this project. Overall, the TOSAS project and Security Team will fall under the direction of the TIERS IV&V Services contract Project Manager who will provide managerial oversight to the TOSAS project.

Our proposed Security Team Lead will not be leveraged on other client or Greentree projects. This is a complicated effort with multiple moving parts; our belief is that the Security Team Lead must be dedicated to the effort to understand all the necessary interdependencies and details, whom will be engaged in the HHSC delivery environment and working to produce and coordinate project deliverables and other activities.

For this project, Greentree anticipates the use of the two SMEs to assist with all key deliverables in Phase I. Our SMEs will bring experience and expertise in technology modernization, National Institute of Standards and Technology (NIST) framework, information security and privacy controls, security assessments, quality assurance, and risk management. Through our successful deliveries in other projects, we have determined that effective delivery is dependent upon having a dedicated resource in place and the strategic usage of SMEs during the surge support activities required in Phase I. This blend ensures that Greentree is addressing each need with the right skillset at the right time.

As stated before in Figure 2 above in the proposed timeframe, the items in blue represent when the entire Security Team will be engaged on the TOSAS project, while the green items show when only the Security Team Lead will be on the TOSAS project. All members of the Security Team and the Security Team Lead shall be approved by HHSC prior to onboarding.

The Contractor staff has garnered extensive experience in providing remote support to multiple projects across the country, both pre- and post-COVID. Given the current state of the COVID-19 pandemic, Greentree TOSAS support will be provided remotely until on-site support is feasible and allowed.

EXHIBIT E-4: REVISED TIERS OPERATIONS SECURITY ASSESSMENT SERVICES (TOSAS) COST TABLES AND RATE SCHEDULE

Texas Health and Human Services Commission

Amended Contract: TIERS IV&V Services

HHSC Contract No.: 529-18-0089-00001

TOTAL TOSAS COST

TOSAS Term	Total Cost
Initial Term: Date of Execution – 12/31/2021 FFY 2021, Y2 Assessment	$541,260.00
Option 1 Term: 1/1/2022 – 10/31/2023 FFY 2022 Y3 Assessment and FFY 2023 Y1 Assessment	$843,975.00
TOSAS TOTAL COST	**$1,385,235**

TOSAS INITIAL TERM, FFY 2021 Y2 Assessment

Payment Item #	Contract Artifact ID	Price
A2-1	TOSAS Security Project Work Plan – 2021	$18,600
A2-2	TOSAS Monthly Progress Report– 2021-01	$14,105
A2-3	TOSAS Monthly Progress Report– 2021-02	$14,105
A2-4	TOSAS Monthly Progress Report– 2021-03	$14,105
A2-5	TOSAS Monthly Progress Report– 2021-04	$14,105
A2-6	TOSAS Monthly Progress Report– 2021-05	$14,105
A2-7	TOSAS Monthly Progress Report– 2021-06	$14,105
A2-8	TOSAS Monthly Progress Report– 2021-07	$14,105
A2-9	TOSAS Monthly Progress Report– 2021-08	$14,105
A2-10	TOSAS Monthly Progress Report– 2021-09	$14,105
A2-11	TOSAS Monthly Progress Report– 2021-10	$14,105
A2-12	TOSAS Monthly Progress Report– 2021-11	$14,105
A2-13	TOSAS Monthly Progress Report– 2021-12	$14,105
A2-14	TOSAS Weekly Progress Reports – 2021	N/A
A2-15	TOSAS Security and Privacy Assessment Report – 2021	$353,400
INITIAL TERM TOTAL COST		**$541,260**