UTA IT SOFTWARE AND ASSOCIATED SERVICES SUPPLY AGREEMENT
Updated July 2021

UTA CONTRACT NO. __21-03463PP_____

Managed Security Services

THIS IT SOFTWARE AND ASSOCIATED SERVICES SUPPLY AGREEMENT ("Contract") is entered into and made effective as of the date of last signature below. ("Effective Date") by and between UTAH TRANSIT AUTHORITY, a public transit district organized under the laws of the State of Utah ("UTA"), and Optiv Security Inc. a Colorado based cybersecurity consulting group having offices at 1144th 15th Street, Suite 2900 Denver, CO 80202 (the "Contractor").

RECITALS

WHEREAS, on August 27, 2021 UTA received competitive proposals to provide security services and (as applicable) all associated hardware, software, tools, installation services, commissioning and testing services, training and documentation according to the terms, conditions and specifications prepared by UTA in 21-03463PP (the "RFP"); and

WHEREAS, UTA desires to award a contract for security management services to Consultant based on best value procurement; and

WHEREAS, UTA wishes to procure the Software and/or Services according to the terms, conditions and specifications listed in the RFP (as subsequently amended through negotiation by the parties); and

WHEREAS, the Optiv 21-03463 proposal submitted by the Contractor in response to the RFP ("Contractor's Proposal) was deemed to be the most advantageous to UTA; and

WHEREAS, Contractor is willing to furnish the Software and Services according to the terms, conditions and specifications of the Contract.

AGREEMENT

NOW, THEREFORE, in accordance with the foregoing Recitals, which are incorporated herein by reference, and for and in consideration of the mutual covenants and agreements hereafter set forth, the mutual benefits to the parties to be derived here from, and for other valuable consideration, the receipt and sufficiency of which the parties acknowledge, it is hereby agreed as follows:

1. SOFTWARE AND ASSOCIATED SERVICES TO BE PROVIDED BY CONTRACTOR

Contractor hereby agrees to furnish and deliver the Services in accordance with the Contract as described in Exhibit A (Product Description and Statement of Associated Services) (including performing any installation, testing commissioning and other Services described in the Contract).

2. TERM

This Contract shall commence as of the Effective Date. The Contract shall remain in full force and effect for purchases of Software and Services (made via purchase order or other agreed order method) during a 3 year period expiring 3 years after last signature on this agreement UTA may, at its sole election and in its sole discretion, extend the initial term for up to 2 additional one-year option

periods, for a total Contract period not to exceed FIVE (5) years. Extension options may be exercised by UTA upon providing Contractor with notice of such election at least thirty (30) days prior to the expiration of the initial term or then-expiring option period (as applicable). The Contract may be further extended if the Contractor and UTA mutually agree to an extension evidenced in writing. The rights and obligations of UTA and Contractor under the Contract shall at all times be subject to and conditioned upon the provisions of the Contract.

3. COMPENSATION AND FEES

UTA shall pay Contractor in accordance with the payment milestones or other terms described in Exhibit B. If Exhibit B does not specify any milestones or other payment provisions, then payment shall be invoiced after the Services have been performed. Advanced Payments shall only be made with approval from Chief Procurement officer. Advanced Payments shall only be made by Approval from UTA Chief Procurement Officer.

4. INCORPORATED DOCUMENTS

a. The following documents hereinafter listed in chronological order, with most recent document taking precedence over any conflicting provisions contained in prior documents (where applicable), are hereby incorporated into the Contract by reference and made a part hereof:

1. The terms and conditions of this Software and Associated Services Supply Agreement (including any exhibits and attachments hereto).

2. UTA's RFP including, without limitation, all attached or incorporated terms, conditions, federal clauses (as applicable), drawings, plans, specifications and standards and other descriptions of the Software and Services;

3. Contractor's Proposal including, without limitation, all federal certifications (as applicable); and

4. The Optiv Terms of Purchase.

b. The above-referenced documents are made as fully a part of the Contract as if hereto attached or herein repeated. The Contract (including the documents listed above) constitute the complete contract between the parties.

c. If this procurement is funded by federal dollars, the mandatory FTA terms and conditions contained at Exhibit C will also apply.

5. ORDER OF PRECEDENCE

The Order of Precedence for this contract is as follows:

- UTA Contract including all attachments and terms and conditions
- UTA Solicitation Terms
- Contractor’s Bid or Proposal including proposed terms or conditions (Optiv Terms of Purchase)

6. LAWS AND REGULATIONS

Contractor and any and all Software and/or Services furnished under the Contract will comply fully with all applicable Federal and State laws and regulations, including those related to safety and environmental protection. Contractor shall also comply with all applicable licensure and certification requirements.

7. INVOICING PROCEDURES

a. Other than items approved by UTA Chief Procurement Officer as advanced Payment. Contractor shall submit invoices to ap@rideuta.com for processing and payment. In order to timely process invoices, Contractor shall include the following information on each invoice:
   i. Contractor Name
   ii. Unique Invoice Number
   iii. PO Number
   iv. Invoice Date
   v. Detailed Description of Charges
   vi. Total Dollar Amount Due

b. UTA shall have the right to disapprove (and withhold from payment) specific line items of each invoice to address non-conforming Goods or Services. Approval by UTA shall not be unreasonably withheld. Payment for all invoice amounts not specifically disapproved or offset by UTA shall be provided to Contractor within thirty (30) calendar days of invoice submittal.

8. WARRANTY OF SOFTWARE AND SERVICES

a. CONTRACTOR Representations, Warranties, and Covenants.

i. General. CONTRACTOR represents and warrants to UTA that (i) this Contract have been validly executed and delivered by CONTRACTOR and that this Contract constitute the legal, valid, and binding obligation of CONTRACTOR enforceable against CONTRACTOR, (ii) CONTRACTOR has all requisite corporate power and authority to enter into this Contract and to carry out the transactions contemplated by this Contract, (iii) the execution, delivery, and performance of his Contract and the consummation of the transactions contemplated by this Contract have been duly authorized by all requisite corporate action on the part of CONTRACTOR, (iv) CONTRACTOR's execution and delivery of this Contract and CONTRACTOR's performance or compliance with this Contract will not conflict with, result in a breach of, constitute a default under, or require the consent of any third party under any license, sublicense, lease, contract, agreement, or instrument to which CONTRACTOR is bound or to which CONTRACTOR's properties are subject, and (v) there are no pending or threatened lawsuits, actions, or any other legal or administrative proceedings against CONTRACTOR which, if adversely determined against CONTRACTOR, would have a material adverse effect CONTRACTOR's ability to perform its obligations under this Contract.

ii. Third-Party Product. Contractor warrants that it has full right, power, and authority to sublicense the Sublicenses and to resell the Third-Party Products to UTA, and that the Third-Party Products are free and clear of all liens and similar encumbrances of any kind.

iii. Contractor Resource Performance. Contractor warrants that Contractor Resources, when used as permitted by Contractor and in accordance with the instructions in the documentation, will operate substantially as described in the Order. Contractor will, at its own expense, use commercially reasonable efforts to (a) correct any reproducible error that UTA reports to Contractor in writing regarding an Contractor Resource, or (b) replace the defective Contractor Resource. In the event that Contractor, in its sole discretion, may not achieve either (a) or (b) as a remedy for breach of this warranty, Contractor agrees to accept return of the non-conforming

Contractor Resource, terminate the Order related thereto, and refund UTA all prepaid fees related to the non-conforming Contractor Resource.

iv. Service Performance. Contractor shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform Services in a professional and workmanlike manner in accordance with applicable laws and governmental regulations. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Contractor
or by third-party Vendors, or because of other causes beyond Contractor's reasonable control, but Contractor shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption. HOWEVER, CONTRACTOR DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. Notwithstanding the forgoing, interruptions of service will adhere to the Optiv Security Operations Service Level Management document previously provided, and available upon request.

Disclaimers of Warranty. CONTRACTOR WILL NOT BE RESPONSIBLE FOR NONCONFORMITIES IN SERVICE ARISING FROM INACCURATE OR INCOMPLETE DATA OR INFORMATION PROVIDED BY UTA, FOR FAILURES OR DELAYS CAUSED BY UTA'S FAILURE TO PERFORM ITS OBLIGATIONS UNDER THE ORDER OR THIS CONTRACT, OR FOR FAILURES, DAMAGES OR DELAYS CAUSED BY THIRD PARTY PROVIDERS, THIRD PARTY VENDORS, OR THIRD-PARTY PRODUCTS. EXCEPT AS EXPRESSLY PROVIDED HEREIN, THE SERVICES ARE PROVIDED "AS-IS" AND CONTRACTOR HEREBY WAIVES AND DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

b. UTA's Representations, Warranties, Covenants and Responsibilities.

i. General. UTA represents and warrants to CONTRACTOR that (i) this Contract have been validly executed and delivered by UTA and that this Contract constitute the legal, valid, and binding obligation of UTA enforceable against UTA, (ii) UTA has all requisite corporate power and authority to enter into this Contract and to carry out the transactions contemplated by this Contract, and (iii) the execution, delivery, and performance of this Contract and the consummation of the transactions contemplated by this Contract have been duly authorized by all requisite corporate action on the part of UTA. In addition, UTA represents, warrants, and agrees that UTA is solely responsible for: (A) UTA's information security program, environment, controls, and processes, (B) making all management decisions related to UTA's information security program, environment, controls, and processes, (C) the decision whether to implement, and the actual implementation, of any recommendations made by Contractor, and (D) determining the sufficiency of any Services or Third-Party Products purchased by UTA.

ii. Services. UTA agrees to reasonably cooperate with Contractor in the performance of the Services. UTA represents and warrants that it will (i) comply with all relevant security industry standards and practices, and (ii) use the Services only in compliance with Contractor's standard published policies then in effect and all applicable laws and regulations.

Although Contractor has no obligation to monitor UTA's use of the Services, Contractor may do so and may prohibit any use of the Services it believes may be (or is alleged to be) in violation of the foregoing. UTA shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Services, including, without limitation, modems, hardware, servers, software, operating systems, networking, web servers and the like (collectively, "Equipment"). UTA shall also be responsible for maintaining the security of the Equipment, UTA account, passwords (including but not limited to administrative and User passwords) and files, and for all uses of UTA account or the Equipment with or without UTA's knowledge or consent.

iii. Third-Party Products. UTA acknowledges that (i) it has made the selection of the Third-Party Products based on its own judgment and expressly disclaims any reliance upon statements made by Contractor, (ii) UTA's use of the Third-Party Products is subject to the applicable Vendor's end user license agreement, service level agreement, terms of use or service, or other end user agreements or documents, (iii) the only representations, warranties, indemnities, and other terms relating to the Third-Party Products are those offered by the applicable Vendor, and Contractor will have no responsibility in connection therewith, (iv) it expressly waives any claim against Contractor based upon any infringement or alleged infringement of any patent, copyright, trademark, or other intellectual property rights with respect to the Third- Party Products, and (v) it assumes all responsibility for ensuring that the Third-Party Products are used in accordance with all applicable laws and regulations.

9. OWNERSHIP OF DESIGNS, DRAWINGS, AND WORK PRODUCT

INTELLECTUAL PROPERTY OWNERSHIP. Deliverables, as specified in an Order, shall be the property of UTA. To the extent Contractor Intellectual Property is incorporated into any Deliverables, Contractor grants to UTA an irrevocable, nonexclusive, royalty-free, limited license for UTA to use Contractor Intellectual Property to the extent necessary to use such Deliverable for its internal purposes only. All Contractor Intellectual Property is and shall remain the sole and exclusive property of Contractor. UTA shall not have or acquire any right, claim, title, or interest in or to any Contractor Intellectual Property. UTA acknowledges that Contractor may (a) retain archival copies of any and all derivative works of Deliverables and work product and (b) may use and disclose general statistics and non-UTA identifiable information regarding vulnerabilities and security issues but only if the identity of the UTA is not disclosed and cannot be reasonably ascertained or inferred. Upon the request of the other Party, each Party shall take such actions, and shall cause its personnel to take such actions, including execution and delivery of all documents, as may be appropriate or desirable to confirm such rights. The information contained in the Contractor Resources is Confidential Information of Contractor, contains trade secrets, and is proprietary know-how belonging to Contractor. UTA is granted access to the Contractor Resources and Sublicense subject to UTA's obligation to hold the information provided in confidence. Further, the presence of copyright notices on the Confidential Information does not constitute publication or otherwise impair the confidential nature thereof. UTA agrees not to use, print, copy, provide, or otherwise make available, in whole or in part, any portion of the Confidential Information or modifications of it or related material except in accordance with this Contract.

10. LIMITED LICENSE GRANT AND RESTRICTIONS- CONTRACTOR RESOURCES AND SUBLICENSES

a. License and Ownership. Contractor grants to UTA a non-exclusive, nontransferable, non-assignable, limited right and license to access and use specified Contractor Resources or

Sublicenses, as applicable. Notwithstanding anything to the contrary in this Contract, Contractor, its licensors and/or Vendors, as applicable, own and retain all right, title and interest in and to the Contractor Intellectual Property, as well as the Intellectual Property Rights in the Contractor Property and Sublicensed Property including any enhancements, modifications or derivative works thereof. UTA retains all ownership rights to UTA Data and UTA Content. Unless a particular right is expressly granted herein, it is expressly excluded from this license.

b. Restrictions. UTA may only use the Contractor Resources and the Sublicenses for its own lawful, internal business purposes. Except as expressly permitted by this Contract or the executed Order, UTA will not, and will not allow any third party to: (a) copy, modify, adapt, alter, translate, or create derivative works of the Contractor Resources or Sublicenses; (b) sell, resell, lend, loan, lease, license, operate as a service bureau, managed service, sublicense or transfer the Contractor Resources or Sublicenses; (c) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code for the Contractor Resources or Sublicenses (except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation); (d) knowingly take any action that would cause the Contractor Resources or Sublicenses to be placed in the public domain; (e) remove, alter or obscure any proprietary notices of Contractor, its licensors or Vendors included in the Contractor Resources, Sublicenses or Order documents; or (f) use the Contractor Resources or Sublicenses for timesharing or service bureau purposes or otherwise for the benefit of a third party, or remove any proprietary notices or labels. UTA will not allow any access to or use of the Contractor Resources or Sublicenses by anyone other than UTA, or its employees, contractors or agents, and any such use must be consistent with the terms, conditions and restrictions set forth in this Contract. UTA will be responsible for its Users' compliance with this Contract and liable for its Users' breach thereof. UTA will ensure that it has obtained all necessary consents and approvals for Contractor to access UTA Data for the purposes permitted under this Contract. If UTA is in breach of this Section, and such breach is not cured in accordance with this Contract, Contractor may suspend access to the Contractor Resources and/or Sublicenses, in addition to any other rights and remedies Contractor may have at law or in equity. Notwithstanding the forgoing, both Parties acknowledge that UTA as a public transit district of the State of Utah, is subject to and will comply with the Utah Government Records Access and Management Act (GRAMA) . UTA's good faith compliance with GRAMA will not be deemed as a breach of this Agreement.

11. IMPORT/EXPORT.

UTA acknowledges that the Contractor Resources, Sublicenses, and Third-Party Products, as well as any technical data related thereto, may be subject to Export Control Laws and UTA hereby agrees not to export, re-export, or otherwise distribute such products in violation of any Export Control Laws. UTA warrants that it will not purchase, export, or re-export any Contractor Resources, Sublicenses, or Third-Party Products with knowledge they will be used in the design, development, production, or use of chemical, biological, nuclear, or ballistic weapons, or in a facility engaged in such activities, unless permitted by applicable laws. UTA further warrants it will not export or re-export, directly or indirectly, any such products to embargoed countries or transfer or sell such products to companies or individuals listed on applicable restricted parties lists including, without limitation, the Denied Persons List published by the United States Department of Commerce and the Specially Designated National List published by the United States Department of the Treasury.

12. RISK OF LOSS AND TITLE TO THIRD-PARTY PRODUCTS.

Title to Third-Party Products shall vest in UTA upon receipt and acceptance at UTA's facility Contractor will ship and deliver the Third-Party Products to the UTA's specified place of delivery using a carrier selected by Contractor; provided, however, that UTA shall be responsible for clearing any necessary customs with respect to the Third-Party Products. Contractor shall bear the risk of loss, damage, and destruction from every cause once the Third-Party Products have been delivered to the carrier. UTA shall unload and inspect the Third-Party Products upon delivery, and UTA shall be responsible for notifying Contractor of any defect or damage to the Third-Party Products or of any claim arising hereunder within ten (10) days of the delivery of the Third-Party Products. UTA's failure to advise Contractor of such defect, damage, or claim within the specified time period will release Contractor and the carrier from any liability for damages related thereto.

13. GENERAL INDEMNIFICATION

General. Except to the extent caused by the acts, errors or omissions of the indemnified Party, each Party shall indemnify, defend and hold harmless the other Party and its Affiliates and their respective officers, directors, employees and agents from and against third party claims made against the indemnified Party for death, bodily injury or physical damage to or loss or destruction of any real or tangible personal property to the extent caused by the indemnifying Party's gross negligence or willful misconduct.

b. IP Infringement. Contractor shall hold UTA harmless from liability to third parties resulting from infringement by the Services of any United States patents issued before delivery of such Services or any copyright or misappropriation of any trade secret, provided Contractor is promptly notified of any and all threats, claims and proceedings related thereto and given reasonable assistance and the opportunity to assume sole control over defense and settlement. Contractor will not be responsible for any settlement it does not approve in writing. The foregoing obligations do not apply with respect to Services or portions or components thereof: (i) not supplied by Contractor, (ii) made in whole or in part in accordance to UTA specifications, (iii) that are modified by UTA after delivery, (iv) combined with other products, processes or materials where the alleged infringement relates to such combination which were unauthorized by Contractor, (v) where UTA continues use of the infringing Services following Contractor's supplying a modified, amended or replacement version of the Services, or (vi) where UTA's use of such Services is not strictly in accordance with this Contract. UTA will reimburse Contractor for any reasonable out-of-pocket expenses incurred by Contractor if the cause of the infringement is attributable to UTA's actions as stated in this paragraph. In the event of such a claim, action or allegation being brought or threatened or in the event an injunction is issued or threatened, Contractor may, at its sole option and expense, either procure for UTA the right to continue to use the Services, modify or replace the Services so as to avoid infringement, or accept the return of the infringing Services and return the license fee paid for such infringing Services. THE PROVISIONS OF THIS SECTION SET FORTH CONTRACTOR'S SOLE AND EXCLUSIVE OBLIGATIONS, AND UTA'S SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS AND/OR PROPRIETARY RIGHTS OF ANY KIND.

c. UTA's Use of Services. UTA represents, covenants, and warrants that UTA will use the Services (including but not limited to Sublicenses) only in compliance with this Contract, any relevant Service descriptions related to the Order and all applicable laws and regulations. UTA hereby agrees to defend, indemnify and hold harmless Contractor and applicable developers of the Sublicenses against any third party claims for damages, losses, liabilities, settlements and expenses (including reasonable costs and attorneys' fees) in connection with any claim or action that arises from an alleged violation based on UTA's gross negligence or willful misconduct or otherwise from UTA's

use of Services. Although Contractor has no obligation to monitor UTA's use of the Services, Contractor may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of the foregoing.

14. LIMITATION OF LIABILITY.

IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES, VENDORS OR SUPPLIERS, OR ANY OF THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, OR AGENTS, BE LIABLE TO THE OTHER PARTY OR ITS AFFILIATES, WHETHER IN CONTRACT OR IN TORT OR UNDER ANY OTHER LEGAL THEORY (INCLUDING, WITHOUT LIMITATION, STRICT LIABILITY AND NEGLIGENCE), FOR LOST PROFITS OR REVENUES, LOSS OF USE OR LOSS OR CORRUPTION OF DATA, FOR EQUIPMENT OR SYSTEMS OUTAGES OR DOWNTIME, OR FOR ANY INDIRECT, SPECIAL, EXEMPLARY, PUNITIVE, MULTIPLE, INCIDENTAL, CONSEQUENTIAL OR SIMILAR DAMAGES, ARISING OUT OF OR IN CONNECTION WITH THE ORDER OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL CONTRACTOR'S, CONTRACTOR'S AFFILIATES', THEIR VENDORS OR SUPPLIER'S, OR THEIR RESPECTIVE OFFICERS', DIRECTORS', EMPLOYEES' OR AGENTS' AGGREGATE LIABILITY FOR ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH THIS CONTRACT, THE SERVICES, THE CONTRACTOR RESOURCES AND SUBLICENSES, THE THIRD-PARTY PRODUCTS, THE ORDER AND OTHERWISE (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE AND INTENTIONAL ACTS OR OMISSIONS) EXCEED THE GREATER OF 3 TIMES THE AMOUNT OF FEES ACTUALLY PAID BY UTA TO CONTRACTOR FOR THE SPECIFIC SERVICES OR THIRD-PARTY PRODUCTS DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE DATE OF THE EVENT GIVING RISE TO SUCH CLAIM, OR FIVE MILLION DOLLARS ($5,000,000).

15. <u>INSURANCE REQUIREMENTS</u>

The insurance requirements herein are minimum requirements for this Contract and in no way limit the indemnity covenants contained in this Contract. The Utah Transit Authority in no way warrants that the minimum limits contained herein are sufficient to protect the Contractor from liabilities that might arise out of the performance of the work under this contract by the Contractor, his agents, representatives, employees or subcontractors and Contractor is free to purchase additional insurance as may be determined necessary.

A. MINIMUM SCOPE AND LIMITS OF INSURANCE: Contractor shall provide coverage with limits of liability not less than those Stated below. An excess liability policy or umbrella liability policy may be used to meet the minimum liability requirements provided that the coverage is written on a "following form" basis.

1. Commercial General Liability – Occurrence Form

   Policy shall include bodily injury, property damage and broad form contractual liability coverage.

   - General Aggregate $4,000,000
   - Products – Completed Operations Aggregate $1,000,000

- Personal and Advertising Injury $1,000,000
- Each Occurrence $2,000,000

a. The policy shall be endorsed to include the following additional insured language: "The Utah Transit Authority shall be named as an additional insured with respect to liability arising out of the activities performed by, or on behalf of the Contractor".

2. Automobile Liability

Bodily Injury and Property Damage for any owned, hired, and non-owned vehicles used in the performance of this Contract.

Combined Single Limit (CSL) $2,000,000

a. The policy shall be endorsed to include the following additional insured language: "The Utah Transit Authority shall be named as an additional insured with respect to liability arising out of the activities performed by, or on behalf of the Contractor, including automobiles owned, leased, hired or borrowed by the Contractor".

3. Worker's Compensation and Employers' Liability

Workers' Compensation Statutory

Employers' Liability

Each Accident $100,000

Disease – Each Employee $100,000

Disease – Policy Limit $500,000

a. Policy shall contain a waiver of subrogation against the Utah Transit Authority.

b. This requirement shall not apply when a contractor or subcontractor is exempt under UCA 34A-2-103, AND when such contractor or subcontractor executes the appropriate waiver form.

4. Professional Liability (Errors and Omissions Liability)

The policy shall cover professional misconduct or lack of ordinary skill for those positions defined in the Scope of Services of this contract.

Each Claim $1,000,000

Annual Aggregate $2,000,000

a. In the event that the professional liability insurance required by this Contract is written on a claims-made basis, Contractor warrants that any retroactive date under the policy shall precede the effective date of this Contract; and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of three (3) years beginning at the time work under this Contract is completed.

5. Railroad Protective Liability Insurance (RRPLI) – Remove this section if not applicable

   During construction and maintenance within fifty (50) feet of an active railroad track, including but not limited to installation, repair or removal of facilities, equipment, services or materials, the Licensee and/or Licensee's Contractor must maintain "Railroad Protective Liability" insurance on behalf of UTA only as named insured, with a limit of not less than $2,000,000 per occurrence and an aggregate of $6,000,000.

   If the Licensee and/or Licensee's Contractor is not enrolling for this coverage under UTA's blanket RRPLI program, the policy provided must have the definition of "JOB LOCATION" AND "WORK" on the declaration page of the policy shall refer to this Agreement and shall describe all WORK or OPERATIONS performed under this Agreement.

B. ADDITIONAL INSURANCE REQUIREMENTS: The policies shall include, or be endorsed to include, the following provisions:

1. On insurance policies where the Utah Transit Authority is named as an additional insured, the Utah Transit Authority shall be an additional insured to the full limits of liability purchased by the Consultant. Insurance limits indicated in this agreement are minimum limits. Larger limits may be indicated after the consultant's assessment of the exposure for this contract; for their own protection and the protection of UTA.

2. The Contractor's insurance coverage shall be primary insurance and non-contributory with respect to all other available sources.

C. NOTICE OF CANCELLATION: Each insurance policy required by the insurance provisions of this Contract shall provide the required coverage and shall not be suspended, voided or canceled except after thirty (30) days prior written notice has been given to the Utah Transit Authority, except when cancellation is for non-payment of premium, then ten (10) days prior notice may be given. Such notice shall be sent directly to (Utah Transit Authority agency Representative's Name & Address).

D. ACCEPTABILITY OF INSURERS: Insurance is to be placed with insurers duly licensed or authorized to do business in the State and with an "A.M. Best" rating of not less than A-VII. The Utah Transit Authority in no way warrants that the above-required minimum insurer rating is sufficient to protect the Contractor from potential insurer insolvency.

E. VERIFICATION OF COVERAGE: Contractor shall furnish the Utah Transit Authority with certificates of insurance (on standard ACORD form) as required by this Contract. The certificates for each insurance policy are to be signed by a person authorized by that insurer to bind coverage on its behalf.

All certificates and any required endorsements are to be sent to insurancecerts@rideuta.com and received and approved by the Utah Transit Authority before work commences. Each insurance policy required by this Contract must be in effect at or prior to commencement of

work under this Contract and remain in effect for the duration of the project. Failure to maintain the insurance policies as required by this Contract or to provide evidence of renewal is a material breach of contract.

All certificates required by this Contract shall be emailed directly to Utah Transit Authority's insurance email address at insurancecerts@rideuta.com. The Utah Transit Authority project/contract number and project description shall be noted on the certificate of insurance. The Utah Transit Authority reserves the right to require complete, certified copies of all insurance policies required by this Contract at any time. DO NOT SEND CERTIFICATES OF INSURANCE TO THE UTAH TRANSIT AUTHORITY'S CLAIMS AND INSURANCE DEPARTMENT.

F. SUBCONTRACTORS: Contractors' certificate(s) shall include all subcontractors as additional insureds under its policies or subcontractors shall maintain separate insurance as determined by the Contractor, however, subcontractor's limits of liability shall not be less than $1,000,000 per occurrence / $2,000,000 aggregate. Sub-contractors maintaining separate insurance shall name Utah Transit Authority as an additional insured on their policy. Blanket additional insured endorsements are not acceptable from sub-contractors. Utah Transit Authority must be scheduled as an additional insured on any sub-contractor policies.

G. APPROVAL: Any modification or variation from the insurance requirements in this Contract shall be made by Claims and Insurance Department or the UTA Legal Services, whose decision shall be final. Such action will not require a formal Contract amendment, but may be made by administrative action.

16. OTHER INDEMNITIES

a. Contractor shall protect, release, defend, indemnify and hold harmless UTA and the other Indemnitees against and from any and all claims of any kind or nature whatsoever on account of infringement relating to Contractor's performance under the Contract. If notified promptly in writing and given authority, information and assistance, Contractor shall defend, or may settle at its expense, any suit or proceeding against UTA so far as based on a claimed infringement and Contractor shall pay all damages and costs awarded therein against UTA due to such breach. In case any Good or Service is in such suit held to constitute such an infringement or an injunction is filed that interferes with UTA's rights under the Contract, Contractor shall, at its expense and through mutual agreement between UTA and Contractor, either procure for UTA any necessary intellectual property rights, or modify Contractor's Software and Services such that the claimed infringement is eliminated.

b. Contractor shall: (i) protect, release, defend, indemnify and hold harmless UTA and the other Indemnitees against and from any and all liens or claims made or filed against UTA on account of any Software or Services furnished by subcontractors of any tier; and (ii) keep UTA property free and clear of all liens or claims arising in conjunction with any Software or Services furnished under the Contract by Contractor or its subcontractors of any tier. If any lien arising out of the Contract is filed in conjunction with any Software or Services furnished under the Contract, Contractor, within ten (10) calendar days after receiving from UTA written notice of such lien, shall obtain a release of or otherwise satisfy such lien. If Contractor fails to do so, UTA may take such steps and make such expenditures as in its discretion it deems advisable to obtain a release of or

otherwise satisfy any such lien or liens, and Contractor shall upon demand reimburse UTA for all costs incurred and expenditures made by UTA in obtaining such release or satisfaction. If any non-payment claim is made directly against UTA arising out of non-payment to any subcontractor, Contractor shall assume the defense of such claim within ten (10) calendar days after receiving from UTA written notice of such claim. If Contractor fails to do so, Contractor shall upon demand reimburse UTA for all costs incurred and expenditures made by UTA to satisfy such claim.

c. Contractor will defend, indemnify and hold UTA, its officers, agents and employees harmless from liability of any kind or nature, arising from Contractor's use of any copyrighted or un-copyrighted composition, trade secret, patented or un-patented invention, article or appliance furnished or used in the performance of the Contract.

17. INDEPENDENT CONTRACTOR

The parties agree that Contractor, in the carrying out of its duties hereunder, is an independent contractor and that neither Contractor nor any of its employees is or are agents, servants or employees of UTA. Neither Contractor nor any of Contractor's employees shall be eligible for any workers compensation insurance, pension, health coverage, or fringe benefits which apply to UTA's employees. Neither federal, state, nor local income tax nor payroll tax of any kind shall be withheld or paid by UTA on behalf of Contractor or the employees of Contractor. Contractor acknowledges that it shall be solely responsible for payment of all payrolls, income and other taxes generally applicable to independent contractors.

18. STANDARD OF CARE.

Contractor shall perform any Services to be provided under the Contract in a good and workmanlike manner, using at least that standard of care, skill and judgment which can reasonably be expected from similarly situated independent contractors (including, as applicable, professional standards of care).

19. USE OF SUBCONTRACTORS

a. Contractor shall give advance written notification to UTA of any proposed subcontract (not indicated in Contractor's Proposal) negotiated with respect to the Work. UTA shall have the right to approve all subcontractors, such approval not to be withheld unreasonably.
b. No subsequent change, removal or substitution shall be made with respect to any such subcontractor without the prior written approval of UTA.
c. Contractor shall be solely responsible for making payments to subcontractors, and such payments shall be made within thirty (30) days after Contractor receives corresponding payments from UTA.
d. Contractor shall be responsible for and direct all Work performed by subcontractors.
e. Contractor agrees that no subcontracts shall provide for payment on a cost-plus-percentage-of-cost basis. Contractor further agrees that all subcontracts shall comply with all applicable laws

20. CONTRACTOR SAFETY COMPLIANCE

UTA is an ISO 14001 for Environmental Management Systems, ISO 9001 Quality and Performance Management, and OSHAS 18001 safety systems Management Company. Contractor, including its employees, subcontractors, authorized agents, and representatives, shall comply with all UTA and industry safety standards, NATE, OSHA, EPA and all other State and Federal regulations, rules and guidelines pertaining to safety, environmental Management and will be solely responsible for any fines, citations or penalties it may receive or cause UTA to receive pursuant to

this Contract. Each employee, contractor and subcontractor must be trained in UTA EMS and Safety Management principles. Contractor acknowledges that its Software and Services might affect UTA's Environmental Management Systems obligations. A partial list of activities, products or Services deemed as have a potential EMS effect is available at the UTA website www.rideuta.com. Upon request by UTA, Contractor shall complete and return a *Contractor Activity Checklist*. If UTA determines that the Software and/or Services under the Contract has the potential to impact the environment, UTA may require Contractor to submit additional environmental documents. Contractor shall provide one set of the appropriate safety data sheet(s) (SDS) and container label(s) upon delivery of a hazardous material to UTA

21. ASSIGNMENT OF CONTRACT

Contractor shall not assign any of its rights or responsibilities, nor delegate its obligations, under this Contract or any part hereof without the prior written consent of UTA, and any attempted transfer in violation of this restriction shall be void.

22. ENVIRONMENTAL RESPONSIBILITY

UTA is ISO 14001 Environmental Management System (EMS) certified. Contractor UTA is ISO 14001 Environmental Management System (EMS) Certifies acknowledges that its Software and/or Services might affect UTA's ability to maintain the obligation of the EMS. A partial list of activities, products or Services deemed as have a potential EMS effect is available at the UTA website www.rideuta.com. Upon request by UTA, Contractor shall complete and return a *Contractor Activity Checklist*. If UTA determines that the Software and/or Services under the Contract has the potential to impact the environment, UTA may require Contractor to submit additional environmental documents. Contractor shall provide one set of the appropriate safety data sheet(s) (SDS) and container label(s) upon delivery of a hazardous material to UTA.

23. SUSPENSION OF WORK

a. UTA may, at any time, by written order to Contractor, require Contractor to suspend, delay, or interrupt all or any part of the Work called for by this Contract. Any such order shall be specifically identified as a "Suspension of Work Order" issued pursuant to this Article. Upon receipt of such an order, Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of further costs allocable to the Work covered by the order during the period of Work stoppage.
b. If a Suspension of Work Order issued under this Article is canceled, Contractor shall resume Work as mutually agreed to in writing by the parties hereto.
c. If a Suspension of Work Order is not canceled and the Work covered by such order is terminated for the convenience of UTA, reasonable costs incurred as a result of the Suspension of Work Order shall be considered in negotiating the termination settlement.
d. If the Suspension of Work causes an increase in Contractor's cost or time to perform the Work, UTA's Project Manager or designee shall make an equitable adjustment to compensate Contractor for the additional costs or time, and modify this Contract by Change Order.

24. TERMINATION

a. **Termination for Cause**. Either Party shall have the right to terminate an Order for Services for cause if (a) the non-breaching Party notifies the other within thirty (30) days of the other's breach, and (b) the breaching Party fails to cure any material breach of the Service Order

within thirty (30) days after its receipt of written notice of such breach. Contractor may cure a material breach of Services, at Contractor's sole option, by either (i) re-performing any defective or non-conforming Services, or (ii) refunding any amount paid by UTA to Contractor for the Services that are deemed to be defective or non-conforming. If UTA terminates the Order for cause for Contractor's failure to cure, Contractor shall refund to UTA the pro-rated portion of any prepaid Services fees, rounded down to the next whole month, corresponding to Services not yet performed. Termination of the Order does not release either Party from any liability which, at the time of termination, has already accrued to the Party. Activation fees and expenses, if any, associated with the establishment of Services will be set forth in the Order and are non-refundable.

b. **Early Cancellation of Services.** If UTA exercises its right to terminate the contract or any portion thereof for convenience , prior to the end of the current term (for any reason other than for an uncured material breach by Contractor), UTA agrees to pay Contractor for the actual services provided to date with a reasonable profit along with reasonable termination expenses. Contractor shall refund any portion of a retainer covering the period no longer covered under a contract due to UTA's early termination.

c. **Cancellation of Product Orders and Return of Products.** Orders for Third-Party Products are non-cancellable and are binding and irrevocable once issued by UTA and accepted by Contractor. Third-Party Product returns may be permitted in limited circumstances where allowed by the Vendor's returns and refunds policy and such return must be approved in writing by the Vendor.

d. **Device Return.** Upon cancellation, termination or expiration of an Order for Services, UTA will return all Contractor-provided equipment and devices ("Devices") in good condition (less normal wear and tear) to a location designated by Contractor within fifteen (15) calendar days after the cancellation, termination or expiration date. If Contractor has not received such Contractor-provided Devices within thirty (30) days after cancellation, termination or expiration of the Order, Contractor shall invoice UTA, and UTA shall promptly pay, for the manufacturer's suggested retail price of such property. For purposes of clarification, "device(s)" do not include any Third-Party Product resold by Contractor and licensed directly to UTA by a Vendor.

25. CHANGES

a. UTA's Project Manager or designee may, at any time, by written order designated or indicated to be a Change Order, direct changes in the Work including, but not limited to, changes:

1. In the Scope of Services;
2. In the method or manner of performance of the Work; or
3. In the schedule or completion dates applicable to the Work.

To the extent that any change in Work directed by UTA causes an actual and demonstrable impact to: (i) Contractor's cost of performing the work; or (ii) the time required for the Work, then (in either case) the Change Order shall include an equitable adjustment to this Contract to make Contractor whole with respect to the impacts of such change.

b. A change in the Work may only be directed by UTA through a written Change Order or (alternatively) UTA's expressed, written authorization directing Contractor to proceed pending

negotiation of a Change Order. Any changes to this Contract undertaken by Contractor without such written authority shall be at Contractor's sole risk. Contractor shall not be entitled to rely on any other manner or method of direction.

c. Contractor shall also be entitled to an equitable adjustment to address the actual and demonstrable impacts of "constructive" changes in the Work if: (i) subsequent to the Effective Date of this Contract, there is a material change with respect to any requirement set forth in this Contract; or (ii) other conditions exist or actions are taken by UTA which materially modify the magnitude, character or complexity of the Work from what should have been reasonably assumed by Contractor based on the information included in (or referenced by) this Contract. In order to be eligible for equitable relief for "constructive" changes in Work, Contractor must give UTA's Project Manager or designee written notice stating:

1. The date, circumstances, and source of the change; and
2. That Contractor regards the identified item as a change in Work giving rise to an adjustment in this Contract.

Contractor must provide notice of a "constructive" change and assert its right to an equitable adjustment under this Section within ten (10) days after Contractor becomes aware (or reasonably should have become aware) of the facts and circumstances giving rise to the "constructive" change. Contractor's failure to provide timely written notice as provided above shall constitute a waiver of Contractor's rights with respect to such claim.

d. As soon as practicable, but in no event longer than 30 days after providing notice, Contractor must provide UTA with information and documentation reasonably demonstrating the actual cost and schedule impacts associated with any change in Work. Equitable adjustments will be made via Change Order. Any dispute regarding the Contractor's entitlement to an equitable adjustment (or the extent of any such equitable adjustment) shall be resolved in accordance with Article 20 of this Contract.

26. INFORMATION, RECORDS and REPORTS; AUDIT RIGHTS

Reserved.

27. FINDINGS CONFIDENTIAL

a. Any documents, reports, information, or other data and materials available to or prepared or assembled by Contractor or subcontractors under this Contract are considered confidential and shall not be made available to any person, organization, or entity by Contractor without consent in writing from UTA.

b. It is hereby agreed that the following information is not considered to be confidential:

1. Information already in the public domain;

2. Information disclosed to Contractor by a third party who is not under a confidentiality obligation;

3. Information developed by or in the custody of Contractor before entering into this Contract;

4. Information developed by Contractor through its work with other UTAs; and

5. Information required to be disclosed by law or regulation including, but not limited to, subpoena, court order or administrative order.

28. CONFIDENTIAL INFORMATION.

a. **Obligations**. The Receiving Party agrees not to disclose or use any Confidential Information of the Disclosing Party in violation hereof and to use Confidential Information of the Disclosing Party solely for the purposes hereof. Upon demand by the Disclosing Party, the Receiving Party shall return to the Disclosing Party all copies of the Disclosing Party's Confidential Information in the Receiving Party's possession or control and destroy all derivatives and other vestiges of the Disclosing Party's Confidential Information; provided that the Receiving Party may retain one archival copy solely for the purpose of administering its obligations under the Order. All Confidential Information of the Disclosing Party shall remain the exclusive property of the Disclosing Party. The Receiving Party may disclose Confidential Information of the Disclosing Party to its employees, officers, directors and representatives who have a reasonable need to know such Confidential Information in connection with the Services. Notwithstanding anything to the contrary, Contractor shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies (including, without limitation, information concerning UTA Data and data derived therefrom), and Contractor will be permitted to: (i) use such information and data to improve and enhance the Services and for other development, diagnostic and corrective purposes solely in connection with the Services and other Contractor offerings and for no other purposes whatsoever; and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business. No rights or licenses are granted except as expressly set forth herein. Notwithstanding the forgoing, both Parties acknowledge that UTA as a public transit district of the State of Utah, is subject to and will comply with the Utah Government Records Access and Management Act (GRAMA) . UTA's good faith compliance with GRAMA will not be deemed as a breach of this Agreement.

b. **Injunction**. Both Parties agree that violation of any provision of this Section would cause the Disclosing Party irreparable injury for which it would have no adequate remedy at law, and that the Disclosing Party will be entitled to seek immediate injunctive relief prohibiting such violation, in addition to any other rights and remedies available to it.

29. PUBLIC INFORMATION.

Contractor acknowledges that the Contract and related materials (invoices, orders, etc.) will be public documents under the Utah Government Records Access and Management Act (GRAMA). Contractor's response to the solicitation for the Contract will also be a public document subject to GRAMA, except for legitimate trade secrets, so long as such trade secrets were properly designated in accordance with terms of the solicitation.

30. PROJECT MANAGER

UTA's Project Manager for the Contract is Matthew Parker, or designee. All questions and correspondence relating to the technical aspects of the Contract should be directed to UTA's Project Manager at UTA offices located at 669 West 200 South, Salt Lake City, Utah 84101, office phone (801) 287-2625.

31. CONTRACT ADMINISTRATOR

UTA's Contract Administrator for the Contract is Amanda Burton, or designee. All questions and correspondence relating to the contractual aspects of the Contract should be directed to UTA's Grants & Contracts Administrator at UTA offices located at 669 West 200 South, Salt Lake City, Utah 84101, office phone (801) 287-3320.

32. CONFLICT OF INTEREST

Contractor represents that it has not offered or given any gift or compensation prohibited by the laws of the State of Utah to any officer or employee of UTA to secure favorable treatment with respect to being awarded the Contract. No member, officer, or employee of UTA during their tenure or one year thereafter shall have any interest, direct or indirect, in the Contract or the proceeds thereof.

33. NOTICES OR DEMANDS

a. Any and all notices, demands or other communications required hereunder to be given by one party to the other shall be given in writing and may be electronically delivered , personally delivered, mailed by US Mail, postage prepaid, or sent by overnight courier service and addressed to such party as follows:

If to UTA:
Utah Transit Authority
ATTN: Contracts Administrator
669 West 200 South
Salt Lake City, UT 84101
Adminstrator@rideuta.com

If to Contractor:
Optiv Security Inc
Attn: Legal Department
1144 15th St Suite 2900
Denver, CO 80202

Either party may change the address at which such party desires to receive written notice of such change to any other party. Any such notice shall be deemed to have been given, and shall be effective, on delivery to the notice address then applicable for the party to which the notice is directed; provided, however, that refusal to accept delivery of a notice or the inability to deliver a notice because of an address change which was not properly communicated shall not defeat or delay the giving of a notice.

34. CLAIMS/DISPUTE RESOLUTION

a. "Claim" means any disputes between UTA and the Contractor arising out of or relating to the Contract Documents including any disputed claims for Contract adjustments that cannot be resolved in accordance with the Change Order negotiation process set forth in Article 20. Claims must be made by written notice. The responsibility to substantiate claims rests with the party making the claim.

b. Unless otherwise directed by UTA in writing, Contractor shall proceed diligently with performance of the Work pending final resolution of a Claim, including litigation. UTA shall continue to pay any undisputed payments related to such Claim.

c. The parties shall attempt to informally resolve all claims, counterclaims and other disputes through the escalation process described below. No party may bring a legal action to enforce any term of this Contract without first having exhausted such process.

d. The time schedule for escalation of disputes, including disputed requests for change order, shall be as follows:

Level of Authority	Time Limit
UTA's Project Manager/Contractor's Project Manager	Five calendar days
UTA's Kyle Brimley /Contractor's Jacquelyn Wayne	Five calendar days
UTA's Contractor's Alisha Garrett [THIRD LEVEL]	Five calendar days

Unless otherwise directed by UTA's Project Manager, Contractor shall diligently continue performance under this Contract while matters in dispute are being resolved.
If the dispute cannot be resolved informally in accordance with the escalation procedures set forth above, then either party may commence formal mediation under the Juris Arbitration and Mediation (JAMS) process using a mutually agreed upon JAMS mediator. If resolution does not occur through Mediation, then legal action may be commenced in accordance the venue and governing law provisions of this contract.

35. GOVERNING LAW

The validity, interpretation and performance of the Contract shall be governed by the laws of the State of Utah, without regard to its law on the conflict of laws. Any dispute arising out of the Contract that cannot be solved to the mutual agreement of the parties shall be brought in a court of competent jurisdiction in Salt Lake County, State of Utah. Contractor consents to the jurisdiction of such courts.

36. COSTS AND ATTORNEY FEES.

If any party to this Agreement brings an action to enforce or defend its rights or obligations hereunder, the prevailing party shall be entitled to recover its costs and expenses, including mediation, arbitration, litigation, court costs and attorneys' fees, if any, incurred in connection with such suit, including on appeal

37. UTAH ANTI-BOYCOTT OF ISRAEL ACT

Contractor agrees that will be not engage in any type of boycott against the State of Israel for the duration of this contract.

38. SEVERABILITY

Any provision of the Contract prohibited or rendered unenforceable by operation of law shall be ineffective only to the extent of such prohibition or unenforceability without invalidating the remaining provisions of the Contract.

39. AMENDMENTS

Any amendment to the Contract must be in writing and executed by the authorized representatives of each party.

40. FORCE MAJEURE

Neither Party shall be liable for delays, failure to meet its obligations under these Terms, or damages of any kind due to events, circumstances, or causes beyond its reasonable control or otherwise related to war, terrorism, riots, acts of God, floods, fire, earthquakes, hacking attempts or attacks, systems or data not within Contractor's control, viruses, malware, and similar software

programs, and denial of service attacks and other malicious conduct. The nonperforming Party must promptly notify the other Party of such event, circumstance, or cause and take all reasonable steps to recommence performance promptly. Notwithstanding the foregoing, no such events, circumstances, or causes shall excuse UTA's obligation to pay undisputed amounts when due hereunder.

41. NO THIRD PARTY BENEFICIARIES

Reserved.

42. NON-SOLICITATION

UTA agrees that it and its Affiliates, and their employees, will not, either during or for a period of twelve (12) months after termination or expiration of the Order, solicit to hire as an employee or contractor any of Optiv's and/or Optiv's Affiliates' employees who directly provided Services under this Agreement. Publication of open positions in media of general circulation (e.g., Internet website job postings) will not constitute solicitation of employees.

43. STAFFING AND LOCATION Contractor intends to utilize personnel who are employees of Contractor in provision of Services. However, Contractor may utilize, in performance of the Services, staff augmentation Contractors who are used by Contractor in its normal course of business and subcontractor personnel. Unless otherwise expressly stated in the Order, the Services may be rendered at UTA's facilities, Contractor's facilities or at other suitable locations within Contractor's discretion.

44. CONTRACTOR'S AFFILIATES Contractor's Affiliates and/or employees or Contractors of Contractor's Affiliates may provide Services under the Order. Such Affiliates and/or their employees or Contractors who provide Services will be subject to this Contract. Only the entity who provides Services will be liable under this Contract with respect to such Services. There shall be no joint and several liability with respect to entities that do not provide Services under this Contract.

45. THIRD PARTY BENEFICIARIES Notwithstanding anything to the contrary herein, UTA hereby agrees that for any software, hardware or service sublicensed by Contractor to UTA hereunder, the developer or Vendor of such software, hardware or service will be deemed a third party beneficiary of this Contract.

46. ASSIGNMENT Except as otherwise set forth in this Contract, neither Party may assign the Order or this Contract without the prior written consent of the other Party. Notwithstanding the foregoing, either Party may assign the Order or this Contract without consent to any parent, subsidiary or other Affiliate, in connection with a merger involving any of its Affiliates or in connection with an acquisition of all or substantially all of such Party's assets or equity interests. In addition, Contractor may assign the Work Order or this Contract this Agreement to an Affiliate.

47. ENTIRE AGREEMENT

This Contract shall constitute the entire agreement and understanding of the parties with respect to the subject matter hereof, and shall supersede all offers, negotiations and other agreements with respect thereto.

48. COUNTERPARTS

This Contract may be executed in any number of counterparts and by each of the parties hereto on separate counterparts, each of which when so executed and delivered shall be an original, but all such counterparts shall together constitute but one and the same instrument. Any signature page of the Contract may be detached from any counterpart and reattached to any other counterpart hereof. The electronic transmission of a signed original of the Contract or any counterpart hereof and the electronic retransmission of any signed copy hereof shall be the same as delivery of an original.

49. NONWAIVER

No failure or waiver or successive failures or waivers on the part of either party in the enforcement of any condition, covenant, or article of this Contract shall operate as a discharge of any such condition, covenant, or article nor render the same invalid, nor impair the right of either party to enforce the same in the event of any subsequent breaches by the other party.

50. INFORMATION, RECORDS and REPORTS; AUDIT RIGHTS

Contractor shall retain all books, papers, documents, accounting records and other evidence to support any cost-based billings allowable under Exhibit B (or any other provision of this Contract). Such records shall include, without limitation, time sheets and other cost documentation related to the performance of labor services, as well as subcontracts, purchase orders, other contract documents, invoices, receipts or other documentation supporting non-labor costs. Consultant shall also retain other books and records related to the performance, quality or management of this Contract and/or Consultant's compliance with this Contract. Records shall be retained by Consultant for a period of at least six (6) years after completion of the Work, or until any audit initiated within that six-year period has been completed (whichever is later). During this six-year period, such records shall be made available at all reasonable times for audit and inspection by UTA and other authorized auditing parties including, but not limited to, the Federal Transit Administration. Copies of requested records shall be furnished to UTA or designated audit parties upon request. Consultant agrees that it shall flow-down (as a matter of written contract) these records requirements to all subcontractors utilized in the performance of the Work at any tier.

51. SALES TAX EXEMPT

Purchases of certain materials are exempt from Utah sales tax. UTA will provide a sales tax exemption certificate to Contractor upon request. UTA will not pay Contractor for sales taxes for exempt purchases, and such taxes should not be included in Contractor's Application for Payment.

52. SURVIVAL

Provisions of this Contract intended by their nature and content to survive termination of this Contract shall so survive including, but not limited to, Articles 6,8, 9, 10, 11, 12, 13, 14, 15, 16, 27, 28, 34, 35, and 50.

IN WITNESS WHEREOF, the parties hereto have caused the Contract to be executed by officers duly authorized to execute the same as of the date of last signature below.

UTAH TRANSIT AUTHORITY:

By_____

By_____

OPTIV SECURITY INC.

DocuSigned by:
By Jacquelyn Wayne
381FC9E99088435...
Name Jacquelyn Wayne
Title VP & Associate General Counsel
4/29/2022

Optiv Opportunity#: 1644710-1

Approved as to Form
DocuSigned by:
Mike Bell
70E33A415BA44F6...
UTA Legal Counsel

This SOW is not intended to be an offer in perpetuity. Optiv reserves the right to invalidate and re-issue this SOW if not signed and returned in its entirety within 60 days of SOW Issue Date.

EXHIBIT A

DESCRIPTION AND STATEMENT OF SERVICES

Co-Managed LogRhythm MSS Statement of Work

SOC with Co-managed SIEM

Co-Managed SIEM Service Overview

Optiv's Co-Managed SIEM, On Premise service offering is a collaborative and consultative experience centered around change management, release management, incident management, and device health performance monitoring. This solution provides preventive and ongoing real-time operational measures for in-scope customer SIEM(s). The service maintains software currency, alerting and reporting, as well as break/fix support when necessary as is integral with the management program. The service also provides for content management and tuning of the SIEM environment as well as Threat Hunting and Alert Triage, Analysis and Investigation based on level of service purchased.

The Optiv Security Operations Center (SOC) staff will work collaboratively with client points of contact to provide the activities and deliverables detailed in this service description

Service Description

Optiv's Co-Managed SIEM On-Premise is separated into three offering types, detailed below.

Core

Core service is designed to provide release and configuration management for the SIEM. Optiv will perform the daily health checks to ensure the platform is operating, perform break-fix, patching, upgrades and work with the vendor where required. Optiv will perform automated alerting on SIEM content.

Total

Total service includes all aspects of Core services. In addition, Optiv will install and optimize all eligible rules documented in the Optiv Content Catalog within the client environment, including the Optiv Threat Intelligence Content Indicator Feed. Any client requested use cases not covered in the Optiv Content Catalog can be requested through a Custom Use Case request process. Clients can request up to 3 custom use cases per quarter, any additional use cases can be requested as a separate Optiv Technology Management engagement. Total Service is designed to execute on the Detect & Respond phases of the NIST Security Framework. Continuous Security monitoring will be performed on all actionable anomalies & events detected from pre-determined use cases. Optiv's Detection and Response team will work with the client regarding response planning, communications, and triage of detected threats, offer mitigation recommendations and improvements to strengthen the client security posture. Remediation recommendations with our Total service are based on the category of alert. All monitored rules will be reviewed by the Optiv Detection and Response team using analysis, enrichment & automation. Optiv's Detection and Response team will triage and categorize a correlated security event as an actionable or non-actionable event. Optiv is responsible for the detection and escalation of correlated security events. The client is responsible for mitigation and remediation of any security events detected by Optiv.

Advanced

Advanced service includes all aspects of Core and Total services plus Threat Hunting, an additional 6 custom use cases per quarter and 10 weeks of additional Client Success activities. In addition, where our Total services offer analysis of the events and associated logs, Advanced offers a deeper investigation that reviews pertinent data surrounding the security event. Analysts will review events and look for alternate events that may have occurred similar to or in addition to the event that was triggered within the client environment. Alerts that are escalated will have specific remediation recommendations if pertinent. This service will also look for monthly trends being seen in both the client environment and our overall client base, allowing for more thorough recommendations, tuning, and increased security posture. Optiv Threat Analysts will conduct hunts based on Optiv's intelligence information to identify outliers not detected by security tools in the environment. Internal analysis will come from both specific events identified in the environment as well as trends and anomalies detect. External threat data will come from Optiv's Global Threat Intelligence Center and vendor provided data.

Service Components

Component	Sub-Component	Core	Total	Advanced
Client Success	Service integration and acceptance	x	x	x
	Dedicated Client Success Manager	x	x	x
	SIEM dashboard/reporting Use Case requests and implementation	x	x	x
	Executive Summary and Client Status Reports		x	x
	Optiv Continuous Improvement		x	x
	10 Weeks per Year of Client Selected Continuous Improvement Activities			x
Cybersecurity Education	Access to Optiv LMS and Designated Role-Based Content	x	x	x
	Completion Reports	x	x	x
SIEM Engineering	24x7x365 SOC Monitoring of Device Health and Performance	x	x	x
	Break/Fix, Patching, Upgrades (8x5)	x	x	x
	Incident Management	x	x	x
	Change Management	x	x	x
	Release Management	x	x	x
	Log Source Management	x	x	x
	SIEM Health Checks (daily)	x	x	x
	SIEM Health Checks (quarterly and semi-annually)		x	x
Detection and Response	Rule/Alert Tuning	x	x	x
	Content and Rule Management		x	x
	24 x 7 Alert Triage		x	x
	Quarterly Trending review		x	x
	General Remediation recommendations		x	x
	24 x 7 Alert Analysis		x	x
	Monthly Trending reports		x	x
	24 x 7 Alert Investigation			x
	Attack Specific Remediation Recommendations			x
	Monthly Environment alert trending			x
Threat Intelligence Services	gTIC Threat Intelligence Report	x	x	x
	gTIC Content Indicator Feed		x	x
	Reactive Threat Hunting • Daily Review of IOCs triggered in the past 24 hrs within the client environment			x
	Proactive Threat Hunting • Weekly Review of Optiv identified IOCs not triggered in the client environment			x

Service Roles and Responsibilities

Client Success and General Technology Management

The Client Success activities include administrative and service support functions needed to support the service engagement. The table below outlines the roles and responsibilities:

#	Client Success and General Technology Management Roles & Responsibilities	Owner
1	Define and submit requirements based on Client's desired security state, corporate policies, regulatory compliance, industry standards and global business needs	Client
2	Document existing configurations and procedures including network architecture	Client
3	Deploy, rack and stack new and/or replacement systems addressing physical installation and integration	Client
4	Deploy, manage and repair software agents and packages on user endpoints and servers related to in-scope managed technologies	Client
5	Provide Optiv list of up to 25 users to be added to Optiv's LMS and whitelist Optiv LMS IP addresses to ensure users receive account email notifications.	Client
6	Document requests/actions with required fields in ticketing system, follow documented change processes and implement changes in alignment with Client standards/policies	Optiv
7	Partner with client to manage and implement changes with client to implement changes to the platform within the boundaries of scope	Optiv
8	Work across teams and stakeholders within Client to integrate complex changes and provide awareness	Optiv
9	Update Optiv utilized access passwords regularly in alignment with Client standards and policies	Optiv
10	Securely vault privileged credentials and other authentication data within Optiv access control systems	Optiv
11	Review configurations in a regular cadence to identify opportunities for optimization, based on level of service purchased	Optiv
12	Provide client access to the Optiv Portal and client information contained within	Optiv
13	Configure user access to Optiv's LMS. Provide reports to client when service requests are submitted for such.	Optiv

SIEM Engineering

SIEM Engineering includes engineering and operational activities for data source management, logging infrastructure, tuning and collection of logs, correlation and identification of security events, and other management activities of the SIEM platform. The table below outlines the roles and responsibilities:

#	SIEM Engineering Roles and Responsibilities	Owner
1	Define SIEM and Log Management requirements based on client's desired security state, corporate policies, regulatory compliance, industry standards and global business needs	Client
2	Review vendor / client design	Optiv
3	Determine, design and document any ongoing logical access requirements	Optiv
4	Review physical / logical topology	Optiv
5	Review client security policies and any applicable regulatory or contractual requirements	Optiv
6	Determine, design and document any ongoing logical access requirements	Optiv
7	Provide Optiv necessary credentials for accessing client environment	Client
8	Configure Client managed data sources (Endpoints, Networking Devices,) to capture and forward log data to SIEM infrastructure.	Client
9	Manage collectors installed directly on applications and infrastructure	Client
10	Configure vendor supported log sources to SIEM supported standards for ingestion, parsing, correlation, and log analysis from various Client data sources.	Client
11	Discovery and documentation of log sources	Optiv
12	Work with Optiv to identify unsupported data sources and provide necessary support (provide logs, etc.) to allow product vendor to develop necessary parsers	Client
13	Provide best practices for the integration of data sources to ensure maximum visibility in security device logs	Optiv
14	Perform device health incident monitoring and troubleshooting on managed in-scope platforms	Optiv
15	Actively perform device health and performance monitoring (DHPM) to identify and proactively service impacting issues	Optiv
16	Perform daily, monthly and quarterly heath checks based on tier of client service	Optiv
17	Monitor the status of cloud platform availability and outages for cloud-based technologies for outages, performance issues and scheduled maintenance	Optiv
11	Identify "silent log sources" and other device health performance monitoring related issues.	Optiv
12	Perform configuration backups on a regular basis within technology parameters	Optiv
13	Audit searches to identify inefficient searches (long query executions) and implement improvements	Optiv
14	Manage cloud-based collector agents as applicable	Optiv
15	Design, create, and implement SIEM dashboards, searches, alerts, and reports based on client Use Case requirements that can be provided by the sources fed into Client's SIEM production instance	Optiv
16	Upgrade platforms on mutually agreed schedule. Optiv generally following a certified version model for most platforms unless otherwise recommended by the vendor	Optiv

Detection and Response Services

Detection and Response uses human analysis, automation, enrichment and additional investigation needed to determine the outcome of the security event. Actionable malicious activity is escalated to the client. The table below outlines the roles and responsibilities for Detection and Response services:

#	Detection and Response Roles & Responsibilities	Owner
1	Develop and maintain standard operating procedures (SOP) for security monitoring and incident response that support Client's operating entities	Optiv
2	Deploy the Optiv Essential Content use cases using industry best practices (such as SANS, CSC, PCI-DSS etc.) and tune for available log sources within the client environment.	Optiv
3	Work with Client staff to prioritize a list of predefined scenario-based rules to identify the most critical and actionable security events for Client	Optiv
4	Optimize SIEM to identify anomalies, reduce false positives and create actionable security alerts	Optiv
5	Integrate automated intelligence to reduce false positives and identify active or potential threats	Optiv
6	Provide Tier 1 support to continuously monitor security alerts and provide basic triage of correlated security alerts.	Optiv
7	Provide Tier 2 support to perform deep-dive incident analysis by correlating data from various sources, determine whether critical system or data set has been impacted, advise on remediation, execute containment actions when available and provide support for new analytic methods of detecting threats	Optiv
8	Provide remediation recommendations for Client for identified security incident either through in-scope managed and/or monitored technology platforms or actions to be taken by Client	Optiv
9	Identify and recommend countermeasures for cyber security threats occurring within Client environment through in scope managed and/or monitored technology platforms	Optiv
10	Continuously establish and refine operational security standards and procedures based on security incident lessons learned	Optiv
11	Work with stakeholders to identify security monitoring use cases for in-scope technologies	Optiv and Client
12	Define critical assets and data sets to support classification and prioritization of security incidents	Client
13	Provide Client environment context to rule out false positives, provide necessary tuning and confirm anomalous behavior	Client
14	Apply mitigations with sense of urgency for systems not under Optiv control	Client
15	Provide feedback and results of incident escalations	Client
16	Provide necessary support and technical expertise in response to security incidents for Client's IT Environment in scope for management and support	Client
17	Approve, apply, socialize, and enforce operational security standards and procedures based on: security incident lessons learned and change drivers	Client

Threat Intelligence Services

Operationalized threat intelligence is the activation of tactical and strategic data to drive overall decision advantage. Optiv leverages research of new security threats, trends, private and open source intelligence (OSINT) to improve the efficiency, and proactively mitigate threats and reduce overall response time.

#	Threat Intelligence Services Roles and Responsibilities	Owner
1	Incorporate threat intelligence feeds into Optiv managed devices to improve visibility and provide proactive mitigation	Optiv
2	Daily review of threat intelligence for proactive measures	Optiv
3	Implement proactive controls based on strategic and tactical intelligence	Optiv
4	Incorporate threat intelligence feeds into client managed devices to improve visibility and provide proactive mitigation	Client
5	Provide access to machine consumable threat intelligence feeds	Optiv
6	Provide daily/weekly reports and quarterly briefings	Optiv
7	Provide insight into patterns and techniques being leveraged by attackers along with accompanying recommendations (i.e. block uncommon TLDs)	Optiv
8	Onboard client team members to receive intelligence products	Optiv
9	Provide a secure mechanism for requesting and receiving intelligence	Optiv
10	Respond to formal request for information submissions and provide available information based on traffic-light protocol (TLP) handling and sensitivity	Optiv

Service Integration

A Technical Project Manager (TPM) will be assigned to manage and track the service integration process. Service integration is a collaborative effort requiring close coordination with the client to ensure all required information is gathered and a complete knowledge transfer occurs between the client points of contact and Optiv SOC staff. Depending on level of service, a Client Success Manager (CSM) will be assigned to support the Continuous Improvement activities at the conclusion of service integration.

Below are the phases that occur during the service integration process. Some steps may occur in parallel.

Initiation and Planning

- Optiv delivers Security Operations Services welcome packet to client project contact
- Pre-Kick-Off Call scheduled and conducted to discuss Client Workbook
- Technical Project Manager schedules and conducts Kick-Off call
- Completion and Optiv review of Client Workbook
- Discussion of the Optiv Content Catalog and what is included. Working through the security value provided in the rules and discuss of what specific risks.

Connectivity and Access

- Setup Client Portal Access for authorized Points of Contact for the service
- Configure network connectivity and/or logical access
- Validation and confirmation of connectivity and access

Service Configuration

- Configure solutions for service delivery
- Work with Optiv SOC personnel to fine tune rules that were discussed during initiation and planning.
    - Depending on the complexity of the client environment, this can take several weeks for some rules.
- Add client escalation sequence to Optiv SOC workflows
- Apply Optiv Content Use Cases
- Deliver and validate Optiv SOC Portal credentials

Continuous Improvement

The Core service level does not include a Continuous Improvement component. Total and Advanced service offerings continuous improvement components are as follows.

Total

- Quarterly Optiv Content updates for use cases that are operable with the client's available log sources.
- Custom use case request management
- Maintain currency with client workbook, SIEM log sources and changes to network architecture
- Tuning Service Request management

Advanced

- The Client Success resource will work collaboratively with the client point of contact to define and perform SIEM assessments, Threat Hunting assessments, project support or technology summit, time limited to 10 weeks per year for planning, delivery and associated artifact creation.

Service Deliverables

Optiv will provide the Client with the following Deliverables as part of the Total and Advanced service offerings. All items designated as a Deliverable will be provided as-is and not subject to any acceptance process.

Client Status Report (CSR)

Weekly report of case summaries and other available data points summarizing service performance.

Executive Summary Report (ESR)

Monthly report of case summaries and other available data points summarizing service performance.

Quarterly Business Review (QBR)

Quarterly review of content evolution pack, alert trending reports, client security roadmap and overall program health.

gTIC Threat Intelligence Reports

Optiv's threat intelligence team publishes daily and weekly threat intelligence summaries for information they have gathered on current threats in the wild. For Advanced clients, Optiv will provide weekly pro-active investigation reports based investigate client alerting to see if we have any clients affected with current attacks.

Service Considerations

The following considerations are applied to the delivery of the defined service.

Log Source Availability

Any missed heartbeat and or silent log source alarms will be sent to the Optiv SOC if the log source is considered critical and directly connected to the security monitoring solution. Log sources under a Device Management service contract are also monitored by the Optiv SOC to ensure general device health and availability (unless client has opted out). When log sources are connected to the security solution via a log aggregation device, missed heartbeat and/or silent log source alarms will only be generated for the log aggregation device.

Runaway Log Sources

Log sources that exhibit excessive logging or anomalous activity may be classified as runaway log sources. Runaway log sources can jeopardize Optiv SOC's ability to provide real-time monitoring of log sources. Optiv SOC staff will recommend log filtering countermeasures, including disabling errant log source signatures and dropping suspect log traffic. Placing a log source in a temporary off-line status is considered a last-resort option and is employed only when the log source in question is impacting the client's real-time analysis service.

Silent Log Sources

The security solution must ingest logs directly from the log source device to properly monitor for alerts from silent log sources.

Native Rules and Alert Templates

Optiv supports rules, alert templates and report templates consisting of vendor prebuilt rules and rules created specifically by the Optiv SOC and intended to address common use cases.

- Rules must be related to actionable security events and cannot impose unacceptable negative impacts on the performance of security solutions. Low fidelity rules will be directed to the client via a report rather than an alert to the Optiv SOC. Rules, alert and report templates altered from the vendor's or Optiv's original design and purpose may not be supported.

- Optiv will support in the configuration and maintenance of vendor-built items as requested, but these will not be monitored by the SOC unless both Optiv and the client agree during the tuning process.

Non-Native Rules and Alert Templates

Optiv will support custom and specific client use cases that are not natively available from the vendor. However, they will be handled on a best effort basis. Client requests for non-native rules and alert templates that are not accepted by the Optiv SOC will be referred to Optiv Professional Services.
Optiv SOC triage of non-native rules must be reviewed and accepted by Optiv. If not accepted by Optiv for triage, non-native rules will be configured to alert the client directly

Professional Considerations

Assumptions

Responsibilities that are not specifically identified in the Service Description, Service Considerations and/or Service Roles and Responsibilities table herein are considered Out of Scope for this service. Additional items Out of Scope items are defined in the Service Level Management Agreement located at www.optiv.com/agreements.

Optiv Responsibilities

The following list details Optiv's responsibilities for the service offering:

- Optiv consultants consider all Client information and documentation as sensitive and confidential and will handle appropriately.
- Optiv shall have responsibility only for consultants employed or subcontracted directly by Optiv for performance of these services.
- Optiv shall staff its SOC to meet the in-scope SLAs as defined in the Service Level Management Agreement located at www.optiv.com/agreements.
- Responsibilities as specifically identified in the Service Description and/or Service Roles and Responsibilities tables herein.

Client Responsibilities

The following list details the Client's responsibilities for this service. Failure to meet these responsibilities may result in delay of the service or the need for a Change Order.

- Client will designate one (1) employee to serve as a primary POC for the engagement. The POC will be responsible for items necessary to the success of this engagement including, but not limited to: scheduling Client resources for required meetings, interviews, and/or data gathering activities; participating in status meetings; serving as the first point of escalation for any engagement-related requests or issues; etc.
- Client will provide access to items necessary for the success of this engagement, including but not limited to: knowledgeable and authorized personnel; proprietary information, applications, and/or systems; network diagrams; facility and/or remote access; operational Internet connection; etc.

- If during the course of the engagement the Client provides to Optiv, its vendors, or subcontractors any personally identifiable information (PII) or access to PII, then (a) the Client will inform Optiv regarding the type of PII, and (b) the Client will provide instruction on the applicable handling, storage, cross-border restrictions, and destruction of such PII. Further, if Optiv's services involve performing work at the Client's location outside of the United States, both the Client and Optiv agree that they will abide by all applicable international laws. To the extent that Optiv processes any personal data for the Client in connection with the Services, the Data Processing Terms and Conditions located at www.optiv.com/agreements shall also apply.
- Responsibilities as specifically identified in the Service Description and/or Service Roles and Responsibilities tables herein.

Change Control

In the event that either party requires changes to the scope originally identified herein, a Change Order will be created. Optiv will provide a Change Order for the Client to review and sign before additional work is performed or additional fees are invoiced to the Client.

Optiv shall be entitled to Change Orders for increases in charges and adjustments of service levels due to (a) changes in the Client's environment as its architecture changes and evolves, (b) changes in the Client's environment and volumes due to the any acquisitions, (c) differences between the Client's responses to Optiv's scoping questions and Client's existing conditions, number of end users, number of locations, and matters that could affect the scope and price of the Services.

Incident Response Retainer

Optiv delivers an Incident Response (IR) Retainer ("Retainer") to provide priority support and guaranteed response times to assist UTA in response to and/or investigation of suspected incidents. In the event of a security incident, Optiv will act as an advisory member of the UTA cyber security IR team, providing technical and non-technical assistance where appropriate. Optiv will obtain digital evidence in a manner consistent with industry practices and will protect that information so that it may be properly submitted in the event that UTA wishes to pursue prosecution in a court of law.

IR Retainer Services Definitions

Response Start Time

The Response Start Time is the point in time when an authorized representative of UTA is on the phone with a qualified Optiv IR representative contacted through the Security Operations Center (SOC) to collect the details regarding UTA's incident.

Service Level Agreement Response Time

The Service Level Agreement (SLA) Response Time is the amount of time between the Response Start Time and when Optiv will respond to UTA's request for assistance under the Retainer. Committed response times are shown in the Service Scope section below.

Remote Response Time

Optiv will use commercially reasonable efforts to provide at least one (1) qualified IR consultant remotely within the Remote Response Time specified in the Service Scope section below to address the incident.

Onsite Response Time

Optiv will use commercially reasonable efforts to have at least one (1) qualified IR consultant onsite within the Onsite Response Time specified in the Service Scope section below for locations within the continental United States. For locations in Alaska, Hawaii, Canada, Mexico, Central America, and South America, Optiv will use commercially reasonable efforts to have at least one (1) qualified IR consultant en route within the specified start time. Operationally, response times often are faster, but in rare instances, Optiv's onsite response times may be impacted by multiple elements out of Optiv's control (such as geography of the incident, flight schedules/availability, and inclement weather). Optiv will also provide at least one (1) qualified IR consultant within the Remote Response Time specified within this Retainer to assist UTA with its incident while Optiv's onsite resource is en route.

NOTE: Response Time(s) do not apply within the first 14 days after signature of SOW. If the SOW is a renewal of an existing Optiv IR Retainer, this restriction does not apply.

Reactive Services

In the event of an incident requiring Optiv's response, UTA should contact the SOC. A lead IR consultant will be engaged, and the incident will be triaged with a Project Manager engaged in parallel.

The Project Manager will set up a call to review the incident, supply guidance about containment, and initiate all project activity. If appropriate, the Project Manager will initiate travel plans, and identify other critical expertise required to respond to the incident. Optiv will establish a secure file transfer capability to facilitate quick transfer of suspect files and evidence, following the preparatory guidance on evidence collection and handling procedures that UTA receives as part of the Onboarding Exercise. Optiv will then triage evidence received in the Incident Management lab in accordance with applicable response times.

In parallel, the Project Manager will send an email requiring approval from UTA that details the task(s) to be completed, the estimated hours needed to complete each task, the associated deliverables, and the estimated additional cost (if applicable) for each initiative. Once the email is approved by authorized personnel at UTA, the Project Manager then will assign resources accordingly.

Logistics documentation and contact information will be provided following signatures of this Retainer.

Proactive Services

Upon Retainer expiration, Retainer hours may be applied toward proactive Threat Management security services (See Expiration). This includes Enterprise Incident Management, Attack and Penetration, Application Security, and Threat and Vulnerability Remediation consulting services ("Proactive Services").

To utilize Retainer hours for Proactive Services, UTA will contact its Optiv Account Manager. Optiv will create a Task Order (TO) detailing the work to be completed, the methodology used to execute the project, and the associated deliverables for the initiative. Optiv and UTA will sign the agreed-upon TO and the Project Manager will assign resources accordingly. Where applicable, the Project Manager will provide a summary of hours utilized to date and hours remaining at the conclusion of each project.

The following represents examples of Proactive Services available when applying unused retainer hours prior to retainer expiration:

- **Incident Management Services:**
  - Incident Discovery/Threat Hunting
  - Incident Management Program Development
    - IR Readiness
    - IR Plan Dev
    - IR Playbook Dev
    - IR Tabletops
- **Application Security Services:**
  - App Architecture/Design Review
  - Threat Modeling
  - Secure SDLC
  - AppSec Program Management
  - Application Assessments:
    - Web
    - Mobile
    - Thick UTA
    - API
  - Secure Code Review
  - Tool Implementation/Tuning/Integration/Automation
  - Internet of Things (IoT) Product Assessment
- **Attack and Penetration Services:**
  - Assessments and Penetration Tests:
    - Network
    - Wireless
    - Physical Security
    - IoT
    - Endpoint
    - Cloud
    - Embedded Devices
  - Social Engineering
  - Red Teaming/Breach Simulation
- **Threat and Vulnerability Management – Remediation:**
  - Continuous Remediation
  - Dedicated Remediation
  - Post Assessment Remediation

This Incident Response Retainer is a renewal of Optiv Op. #. This renewal includes a one-time exception that allows for consulting hours remaining upon Retainer expiration to be used for Proactive Services.

Travel Time

The time required for an onsite Optiv IR consultant to travel to an onsite location to assist UTA with its incident will not be deducted from UTA's Retainer hours. UTA will be billed for any concurrent remote work that is performed while the onsite resource is in transit.

Deliverables Documentation

Optiv will provide UTA with the following deliverable documents ("Deliverables") electronically in standard Optiv format.

Incident-Related Documentation

Deliverables associated with additional services that utilize hours from this Retainer will be detailed in subsequent emails exchanged between UTA and the Project Manager or in the TO if applicable.

Incident Report

Upon UTA's request, a detailed report of all digital evidence will be provided to UTA upon the completion of any examination. This report will detail the evidence collected and any significant findings regarding the data that is relevant to the incident. Information such as Chain of Custody and detailed findings analysis will be included in this report as appropriate.

Deliverable Acceptance

Deliverables defined in this SOW are subject to inspection and acceptance by the designated UTA Point of Contact (POC):

- There will be one (1) round of Deliverable review.
- UTA is responsible for consolidating its stakeholder feedback into a single view for Optiv within ten (10) business days.
- If UTA does not accept or reject the draft within this period, the Deliverable(s) shall be considered accepted by UTA.
- If the draft is rejected, Optiv will update the draft within a mutually agreeable timeframe. Optiv will then provide the updated, finalized Deliverable to UTA.

Service Scope

Scoping Considerations

Scoping details listed below were provided by UTA through documents and/or interviews; and some assumptions may have been made based upon industry best practices.

Retainer Package and SLA

Billed Item	Description and Terms
IR Retainer Package	• 100 Retainer Hours (annual) • Four (4)-Hour Remote Response Time • 48-Hour Onsite Response Time • Onboarding <u>Purchase of Additional Hours</u> Additional hours can be purchased via a mutually executed Change Order at the hourly rates below during the term of each annual Retainer. • Additional Retainer Hours: ○ $375.00/hr

Incident Response Retainer Assumptions

- **Conflict of Interest:** If it is determined that the third party who is a target of this investigation is also a current customer of Optiv, Optiv may, at its sole discretion, immediately terminate its performance of Services under the Retainer SOW and credit the retainer any hours already worked for the Services. In the event of such termination, Optiv is not liable to UTA for any loss of profits, or any indirect, incidental, exemplary, consequential, or special damages relating to or arising out of the Retainer SOW.
- **Expiration**: Annual retainer hours must be used within twelve (12) calendar months from date of (Year 1) or anniversary of (Years 2 and 3) Retainer SOW signature for reactive incident response services.
    - **Proactive Services Credit:** Within one (1) month after annual Retainer expiration, unused Retainer hours can be leveraged as a dollar-based credit towards the scope of Proactive Services. SLA pre-paid fees cannot be applied to Proactive Services.
    - **Proactive Services Scheduling:** Proactive Services must commence within four (4) months after annual Retainer expiration.
    - **Unused Hours:** Any unused hours not leveraged for Proactive Services will be forfeit, and no refunds for any pre-paid fees will be provided. **Usage Restrictions**: Unused Hours cannot be applied to Training, Subscription Services, Authorized Support Provider (ASP) Services, purchase of products, or services outside of Threat Management's portfolio.
- **Holiday Work:** Any work performed during a scheduled holiday will be performed at a rate of two (2) hours per hour worked [equivalent to two (2) times the project bill rate]. Optiv holidays may be provided by the Optiv Project Manager.
- **Weekend Work**: Any work performed during a weekend will be performed at a rate of one and a half (1.5) hours per hour worked (equivalent to time-and-a-half of the project bill rate). Weekend times are defined as 7:00 P.M. Friday through 7:00 A.M. Monday (UTA local time).
- **Overtime Hours:** Any work beyond 10 consecutive hours per day from a single individual will be deducted at a rate of one and a half (1.5) hours per hour worked (equivalent to time-and-a-half of the project bill rate).
- **Excessive Hours: Optiv** incident responders are limited to no more than 15 consecutive hours of work. If additional hours are required, the Project Manager may utilize additional resources (with UTA's approval).
- **Minimum Usage:** Please note the following minimum deductions will apply for all projects pulling from the block: eight (8) hour minimum for any onsite billable work and two (2) hour minimum for any remote consulting.

Onboarding

#	Onboarding Roles and Responsibilities	Owner
1	Enumerate the IR posture of UTA, including corporate computing environment, critical assets, network configuration, security devices, and overall IR capabilities	Both
2	Discuss current policies, procedures, personnel, training, and communication plans	UTA

#	Onboarding Roles and Responsibilities	Owner
3	Review network design, infrastructure, threat identification mechanisms, and security/investigative technologies and devices currently in place in UTA's environment	Optiv
4	Discuss the programs that control where sensitive data (e.g., CHD, SSNs, CCNs, PII, IP) is kept, how it moves through the organization, and the potential risk of compromise	Both
5	Provide primary and secondary points of contact for UTA, should Optiv Services be needed	UTA
6	Identify alternate technologies within the UTA's environment that may contain key pieces of evidence for an IR	Both
7	Establish secure file transfer capability	Optiv
8	Provide preparatory guidance on evidence collection and handling procedures	Optiv

Reactive Services

#	Reactive Services Roles and Responsibilities	Owner
1	Contact Optiv SOC in the event of an incident requiring response	UTA
2	Triage of incident upon receipt of call	Optiv
3	Provide guidance about containment	Optiv
4	Initiate project activity, including travel plans and identification of critical expertise required to respond to incident	Optiv
5	Confirm file transfer capability to rapidly transfer suspect files and evidence	Both
6	Triage evidence in Incident Management Lab	Optiv
7	Send approval email that details tasks to be completed, estimated hours, any additional deliverables, and estimated additional costs (if applicable)	Optiv
8	Authorize work to be performed by Optiv	UTA

LogRhythm Health Check and Optimization

The LogRhythm Health Check consists of a review of the target environment at every level, including hardware, network architecture, software, configurations, integrations, and overall effectiveness to determine a prioritized set of actionable recommendations on improving the overall health of the LogRhythm. Optiv recognizes that the following are UTA' key objectives:

- Review of UTA's LogRhythm with recommendations for improvement
- Optimization and fine-tuning of UTA's LogRhythm solution in preparation for onboarding to Optiv Managed Security Service (MSS)
- Knowledge transfer

Service Activities and Approach

The following phases and list of activities provide an overview into the work and processes required to complete the services included as a part of this offering. However, this list should not

be taken as a complete list of tasks. Each phase may change based on the information gathered during the project.

Project Planning Phase

Kick-Off Call

This Kick-Off Call consists of project planning and coordination and helps to identify the following items:

- UTA and Optiv resources and roles
- Agreement on project timeline and resource availability

Health Check Phase

Data Collection

Optiv will collect configuration data regarding LogRhythm and its network environment including, but not limited to the following:

- Design and network diagrams
- Hardware and software specifications
- Configuration standards and settings
- Performance and run state information

Review and Analysis

Optiv will review LogRhythm across the key areas below, then document any issues that are discovered and make recommendations for suggested improvements.

Architecture and Network

Optiv will verify that LogRhythm's design and architecture adhere to Optiv's standards as well as the vendor's best practices for the version that the UTA is running. The review will include:

- Architecture
- Performance, resiliency, and stability

Hardware and Operating System

Optiv will verify that the in-scope hardware and Operating Systems are performing within acceptable parameters and conforming to LogRhythm's best practices for the configuration and version running in production. Suggested improvements to the hardware and operating system are determined to increase performance. The review will include the following (as applicable):

- Sizing: LogRhythm agents, appliances, collectors, receivers, forwarders, and managers
- Performance: CPU, RAM, Disk, I/O, EPS
- Security: Hardening, security roles, and authentication
- Networking and services: IP addresses, time servers, and email
- Monitoring: Heartbeats, health alerts, alarms, logs, and logging
- Virtualized environments: Verification that the virtualized environment is operating well and not blocking due to IO contention

Application and Database

Optiv will review the configurations and operating state for the LogRhythm applications as well as the in-scope database against LogRhythm's best practices for the version running in production. The review will include the following (as applicable):

- Database jobs: verify that they are configured and functioning properly
- Version
- Security
- Performance and stability
- Content and use cases

Inputs, Parsing and Archiving

Verify LogRhythm's inputs, parsing configurations, and archiving strategy against Optiv standards as well as the vendor's best practices. The review and verification will include:

- Sizing and caching
- Performance and stability
- Aggregation and filtering
- Parsing: Verify that data sources are being parsed correctly
- Transformation: Verify that data sources are being transformed and enriched
- Entity Structures and Lists: Review structures and lists against best practices and verify that Lists are populated
- Verify all Global Log Processing Rules (GLPR) are documented and adheres to best practices:
- Review disabled GLPRs
- Review LogRhythm Service Account tuning adhere to best practices
- Verify proper alarm tuning is in place using GLPRs
- Verify Local log source collection is properly configured for all System Monitor Agents
- Optiv will assist creating a process to parse archived logs to meet data retention requirements

Correlation and Management

Optiv will review LogRhythm's correlation and management systems against Optiv standards as well as the vendor's best practices:

- Review performance and stability
- Verify backups and cleanup task are being performed
- Verify a sampling of content is functioning efficiently by reviewing a sampling of the following:
    - Firing rules and partial match rules
    - Longest running trends and queries
    - Dashboards and query viewers
- Verify Knowledge Base is properly configured and updating
- Verify a sampling of content is functioning efficiently:
    - Review a sampling of the following:

        - Triggered rules
        - Investigations
        - Unidentified Log Sources
        - Reports
    - Log Volume Reports:
        - Verify report email delivery (if applicable)

Operations

Optiv will verify that the hardware is operating within acceptable parameters, and conforms to the solution's best practices for the version that the UTA is running:

- Triage Procedures
- Basic Workflow
- Knowledge Assessment

Optimization Phase

Following completion of the Health Check review, Optiv will provide up to 40 Hours of log source tuning and optimization services.

- Critical remediation of the LogRhythm environment to ensure preparedness for onboarding to Optiv MSS. Critical Remediation needs shall be noted by the Optiv consultant and discussed with the UTA. Critical Remediation or additional tuning requests by the UTA may be performed at the discretion of the Optiv Consultant within the hours allotted and scoped in this SOW. Critical remediation that materially affects the success of this engagement or that results in the need for additional hours will require a Change Order
- Optiv will assist UTA with onboarding additional log sources to provide gaps in security monitoring,
- Tuning and Optimization services will be focused on Optiv recommendations and vendor best practices
- Optiv will put forth commercially reasonable efforts to complete remediation of identified issues, but due to the time limited nature of the engagement, Optiv makes no guarantee of full resolution of the problems. If additional time is required to address issues, time can be added via the completion of a mutually agreed on Change Order

Final Documentation Creation

- Create the Project Summary Report
- UTA Workbook

Deliverables Documentation

Optiv will provide UTA with the following deliverable documents ("Deliverables") electronically in standard Optiv format.

Project Summary Report

The Project Summary Report contains a high-level description of the work performed and details

of the SIEM solutions Health Check and includes the following sections:

- Executive Summary
- Summary of work performed
    - Including remaining remediation efforts
- Architecture diagram
- Configuration settings
- Findings and recommendations
    - Critical issues and remediation steps
    - New use cases
    - Use cases to retire, adjust or augment
    - Current log sources
    - New log sources
    - Log sources to retire, adjust and or augment
    - Gaps in detective controls (sensors)
    - Improvements in maintenance processes
- Future state recommendations

UTA Workbook

The UTA Workbook contains a detailed description of the LogRhythm environment and will be transitioned to Managed Security Services.

- Network Data
- List Data
- Co-Managed SIEM Content

Deliverable Acceptance

Deliverables defined in this SOW are subject to inspection and acceptance by the designated UTA Point of Contact (POC):

- There will be one (1) round of Deliverable review.
- UTA is responsible for consolidating its stakeholder feedback into a single view for Optiv within ten (10) business days.
- If UTA does not accept or reject the draft within this period, the Deliverable(s) shall be considered accepted by UTA.
- If the draft is rejected, Optiv will update the draft within a mutually agreeable timeframe. Optiv will then provide the updated, finalized Deliverable to UTA.

Service Scope

Scoping Considerations

Scoping details listed below were provided by UTA through documents and/or interviews; and some assumptions may have been made based upon industry best practices.

Scope Item	Metrics
LogRhythm Environment	• Existing LogRhythm deployment
Additional Notes	• UTA looking for future state recommendations regarding LogRhythm architecture • UTA will be on-boarded to Optiv MSS • UTA will provide sufficient access to the LogRhythm solution to allow successful completion of the above tasks
Consulting Hours	• Up to 80

Out of Scope

All activities listed below, and any unspecified activities not stipulated above are out of scope for the services defined in this SOW. Inclusion of any of the following items will require additional scoping to provide sufficient Level of Effort (LOE) and associated costs.

- Integration of custom log sources or log sources not fully supported by LogRhythm
- Implementation of additional products or services not listed in the activities above
- Integration with third-party ticketing systems not listed in the activities above
- Integration with third-party software not listed in the activities above
- Creation of procedural or process documentation
- Creation of run books
- Creation of custom queries, rules, notifications, dashboards and reports other than those listed above
- Creation of instructional deployment handbooks enabling the complete rebuild of all settings and configurations

Professional Services Considerations

Professional Services Considerations are limited to Incident Response Retainer and LogRhythm Health Check and Optimization Services provided under this SOW and do not apply to SecOps Services.

Services Assumptions

- Significant variance from the scope stated herein or to the terms and conditions of this SOW will result in a written, mutually executed Change Order.
- "Business Hours" are Monday through Friday 8:00 A.M. to 5:00 P.M. (UTA local US time). “Non-Standard Hours” include hours/testing windows/maintenance windows outside of Business Hours (“After Hours”) or any hours that fall on Optiv-recognized holidays (“Holiday Hours”).

- All work to be performed by Optiv under this SOW will be completed during Business Hours unless Non-Standard Hours are otherwise noted.
- For any un-scoped UTA-requested project holds greater than 30 days, Optiv will invoice for fees and charges accrued using a pro-rated amount for fixed-price services for work performed up to the time of hold requestAny project remaining on un-scoped UTA-requested holds for 90 days will terminate and will be bound to any applicable termination provisions, unless otherwise mutually agreed to in writing.
- UTA may terminate or reschedule this SOW for convenience upon two (2) weeks' written notice; provided, however, termination of this SOW for any reason does not release either party from any liability, which, at the time of termination, has already accrued to the other party. Upon termination, Optiv will invoice for fees and charges accrued but unpaid as of the termination date. For Fixed Fee engagements, charges accrued shall be the pro-rata portion of the services provided.

The following list details Optiv's responsibilities for this project, in addition to performance of Services as described in Approach section:

- Optiv's Project Management Organization will provide project planning, coordination, and governance related to the delivery of security solutions. The level of Project Management activities (project planning, oversight, and governance) is determined during the early planning phases, and may include, but is not limited to, the following:
    - Facilitate UTA-centric planning, coordination, and governance throughout the project lifecycle
    - Provide oversight and support managing the project plan, scope, cost, timelines, personnel logistics and quality assurance
    - Manage project communications, including project status updates, reporting and risk mitigation
- Optiv consultants consider all UTA information and documentation as sensitive and confidential and will handle appropriately.
- Optiv shall have responsibility only for consultants employed or subcontracted directly by Optiv for performance of Services.

The following list details UTA's responsibilities for this project.

- UTA will provide access to items necessary for the success of this project in a commercially reasonable response time, including but not limited to:
    - One (1) primary POC for the project responsible for required meetings, coordination of other key personnel, data gathering, and project-related issues
    - Applicable proprietary information, applications, systems, and/or network diagrams
    - Facility and/or remote access
    - Operational Internet connection
- This paragraph applies only if UTA and Optiv do not have a mutually executed Agreement related to the handling of personal data. If during the course of the project UTA provides to Optiv, its vendors, or subcontractors any personally identifiable information (PII) or access

to PII, then (a) UTA will inform Optiv regarding the type of PII, and (b) UTA will provide instruction on the applicable handling, storage, cross-border restrictions, and destruction of such PII. Further, if Optiv's services involve performing work at a UTA location outside of the United States, both UTA and Optiv agree that they will abide by all applicable international laws. To the extent that Optiv processes any personal data for UTA in connection with the project, the Data Processing Terms and Conditions located at www.optiv.com/agreements shall also apply.

EXHIBIT B
PRICING

SOC with Co-managed SIEM

Fee table for base and option year services

Start-Up & Implementation Services	
One time, all inclusive, set-up and configuration fee(s)	$ 38,855.33
Not-to-exceed travel costs	$0
Other reimbursable expenses	$0
Project Management fee(s),	$0
Other (expand/detail as req'd)	$0
Total ONE-TIME implementation costs	**$ 38,855.33**
SOCaaS Co-managed SIEM Costs	
Annual cost of SOCaaS with co-managed SIEM	$ 175,000.00
Any costs not included in annual SOCaaS service	**$0**
Total non-Inclusive cost related to Co-managed SIEM	***$ 175,000.00***
Cyber Incident Response(IR) Retainer Costs	
Annual Incident Response (IR) Retainer	$47,000
Fixed/blended hourly rate for IR services	$340 (100 prepaid hours included in Retainer) $375 (additional hours as needed)
Travel expense daily rate for IR services (max)	$0
Unused IR hours/dollars max rollover which can be used towards subsequent year IR Retainer (UTA's discretion)	$0
Unused IR hours/dollars max rollover which can be used for other services offered by vendor (UTA's discretion)	$34,000
Total IR Retainer Costs	***$47,000***

Fee table for 2nd year bid services:	
SOCaaS Co-managed SIEM Costs	
Annual cost of SOCaaS with co-managed SIEM	$ 175,000.00
Any costs not included in annual SOCaaS service	$ 0

Total non-Inclusive cost related to Co-managed SIEM	***$ 175,000.00***
Cyber Incident Response(IR) Retainer Costs	
Annual Incident Response (IR) Retainer	$47,000
Fixed/blended hourly rate for IR services	$340 (100 prepaid hours included in Retainer) $375 (additional hours as needed)
Travel expense daily rate for IR services (max)	$
Unused IR hours/dollars max rollover which can be used towards subsequent year IR Retainer (UTA's discretion)	$0
Unused IR hours/dollars max rollover which can be used for other services offered by vendor (UTA's discretion)	$34,000
Total IR Retainer Costs	***$47,000***

Fee table for 3rd year bid services:	
SOCaaS Co-managed SIEM Costs	
Annual cost of SOCaaS with co-managed SIEM	$ 175,000.00
Any costs not included in annual SOCaaS service	$
Total non-Inclusive cost related to Co-managed SIEM	***$ 175,000.00***
Cyber Incident Response(IR) Retainer Costs	
Annual Incident Response (IR) Retainer	$47,000
Fixed/blended hourly rate for IR services	$340 (100 prepaid hours included in Retainer) $375 (additional hours as needed)
Travel expense daily rate for IR services (max)	$
Unused IR hours/dollars max rollover which can be used towards subsequent year IR Retainer (UTA's discretion)	$0
Unused IR hours/dollars max rollover which can be used for other services offered by vendor (UTA's discretion)	$34,000
Total IR Retainer Costs	***$47,000***

- A Credit of $34,000 for any unused retainer will be applied to towards the other vendor services in years 1-3 Options years will be negotiated at time options are exercised.

Invoicing Terms

One-Time Invoicing

Invoice upon signature of SOW for SecOps Start-Up and Implementation Services one-time cost.

Recurring Invoicing

- Upon mutual execution of this SOW, Optiv will schedule a kickoff call with UTA to commence the installation period. Fees for Optiv SecOps Services will commence upon the completion of the installation period or 45 days from the kickoff call, whichever comes first.
- First Year Fee to be invoiced upon SOW signature: $175,000
- Second and Third Year Fees each to be invoiced in advance upon each anniversary date: $175,000

Fee table for 4th year bid services (or 1st option year) :	
SOCaaS Co-managed SIEM Costs	
Annual cost of SOCaaS with co-managed SIEM	$ 175,000.00
Any costs not included in annual SOCaaS service	$ 0
Total non-Inclusive cost related to Co-managed SIEM	***$ 175,000.00***
Cyber Incident Response(IR) Retainer Costs	
Annual Incident Response (IR) Retainer	$50,000
Fixed/blended hourly rate for IR services	$360 (100 prepaid hours included in Retainer) $400 (additional hours as needed)
Travel expense daily rate for IR services (max)	$ 0
Unused IR hours/dollars max rollover which can be used towards subsequent year IR Retainer (UTA's discretion)	$0
Unused IR hours/dollars max rollover which can be used for other services offered by vendor (UTA's discretion)	$36,000
Total IR Retainer Costs	***$50,000***

Fee table for 5th year bid services (or 2nd option year):	
SOCaaS Co-managed SIEM Costs	
Annual cost of SOCaaS with co-managed SIEM	$ 175,000.00
Any costs not included in annual SOCaaS service	$ 0
Total non-Inclusive cost related to Co-managed SIEM	***$ 175,000.00***
Cyber Incident Response(IR) Retainer Costs	
Annual Incident Response (IR) Retainer	$ 52,000
Fixed/blended hourly rate for IR services	$375 (100 prepaid hours included in Retainer) $415 (additional hours as needed)
Travel expense daily rate for IR services (max)	$0
Unused IR hours/dollars max rollover which can be used towards subsequent year IR Retainer (UTA's discretion)	$0
Unused IR hours/dollars max rollover which can be used for other services offered by vendor (UTA's discretion)	$37,500
Total IR Retainer Costs	***$52,000***

Incident Response Retainer

Fixed-Price Services

The Services shall be performed on a fixed-price basis.

Description of Service	Price
Year 1	
IR Retainer SLA	$13,000
IR Retainer Hours	$34,000
Year 2	
IR Retainer SLA	$13,000
IR Retainer Hours	$34,000
Year 3	

IR Retainer SLA	$13,000
IR Retainer Hours	$34,000
Total	$141,000

Invoicing Terms

Invoice based on the milestones listed below:

Payment Milestone	Amount
SOW signature (Year 1 Retainer)	$47,000
Anniversary date of Year 1 signature (Year 2 renewal)	$47,000
Anniversary date of Year 2 signature (Year 3 renewal)	$47,000

Additional Payment Terms

- All pricing is in U.S. Dollars (USD)
- Payment terms: Net 30

Expenses

Travel and expenses are not applicable for this engagement, as all work will be completed remotely.

LogRhythm Health Check & Optimization

Time-and-Materials Services

The Services shall be performed on a time-and-materials basis, as time allows.

Service	Description	Estimated Price
LogRhythm Health Check & Optimization	Estimated cost for Health Check service, including: • Consulting Rate: $284/Hour at an estimated 80 hours • Oversight Rate: $194/Hour at an estimated 8 hours	$24,272

Invoicing Terms

Invoice monthly for hours utilized.

Rates for Non-Standard Hours

- After Hours to be billed at time-and-a-half the standard billing rate
- Holiday Hours to be billed at two (2) times the standard billing rate

Additional Payment Terms

- All pricing is in U.S. Dollars (USD)
- Payment terms: Net 30

Expenses

Travel and expenses are not applicable for this engagement, as all work will be completed remotely.