Exhibit to Managed Security Services Service Component Provider Master Services Agreement

DIR Contract No. DIR-MSS-SCP-001

Between

The State of Texas, acting by and through the Texas Department of Information Resources

and

AT&T Corp.

Exhibit 2.8.2

Statement of Work

Incident Response Services – Request for Revised Offer

October 26, 2017

Table of Contents

1.0 Managed Security Services – Incident Response

1.1 Services Overview

This **Exhibit 2.8.2 -** Managed Security Services – Incident Response sets forth the roles and responsibilities of the Parties for the Services provided under the Agreement.

DIR is seeking a Service Provider to deliver the following types of services:

1. Incident Response (IR)
    - Services assist agencies in meeting internal needs, as well as state and Federal legal and regulatory requirements for providing effective monitoring and analysis of information security events as well as response to information security and privacy incidents

The type and scope of work will be determined by the Customer and agreed between the Service Provider and Customer.

1.2 Service Strategies and Objectives

Managed Security Services (MSS) is a procurement and service delivery mechanism to be offered by Texas DIR for customers to engage a prequalified service provider to obtain governed security services. Customers request specific solution proposals that assume the responsibilities defined in this Statement of Work that will be applied to a specific scope of work. The service level requirements are described and documented in **Exhibit 3** and its attachments; pricing is described and documented in **Exhibit 4** and its attachments.

2.0 Service Environment

2.1 Scope of the Infrastructure to Be Supported

The following sub-sections and related Appendices further describe and scope the Services to be supported and/or with which Service Provider shall comply. The Service Environment will be specifically defined at the time the Service Provider is engaged by a Customer to propose or deliver Services.

To provide general context across potential Service Environments, the following sections may reference general lists, descriptions or guidance to be considered by the Service Provider in responding to the DIR RFO.

2.1.1 Services and Data

1. All support services must be situated and all agency-related data must reside within the contiguous United States at all times. DIR will not consider any support services situated outside the United States nor will DIR allow any agency-related data to be stored outside the contiguous United States
2. All data or other information generated as a result of services provided by any Service Component Provider must be protected and shared only with relevant stakeholders and may not be shared for the purposes of additional sales opportunities. All data must be protected in accordance with the MSA.

2.1.2 Service Hours and Locations

All services listed below must be offered based on the following service hour options:

1. 24x7x365: all Services to be provided 24 hours a day, 7 days a week, all 365 days per year.
2. 7am-7pm weekdays: all Services to be provided from 7am to 7pm weekdays, with on-call resource support provided during off hours.

All services may be offered remotely, from the Service Provider's facilities. Service Provider must provide Services at Customer locations, if a Customer requests such services through the Request Management system, in accordance with the Service Management Manual. These Customer Requests will be priced at time of request based on the criteria defined in **Exhibit 4**, Pricing.

No off-shoring of resources or services is allowed.

Reference **Attachment 4-A**, Service Provider Pricing Forms, for resource unit pricing models for the Services required in this statement of work.

2.1.3 Personnel

Service Provider will be responsible for providing appropriately skilled staffing to meet the Roles and Responsibilities and service levels set forth in this SOW.

NOTE: Customers may request, through the Request Management process, dedicated resources to provide Services at the Customer's location. Service Provider shall provide dedicated, onsite resources to support Customer's needs in accordance with the Service Management Manual. These Customer Requests will be priced at time of request based on the criteria defined in Exhibit 4, Pricing.

2.1.4 Policies, Procedures and Standards

The general policies, procedures and standards with which Services will comply are provided in **Attachment 6-B** Service Management Manual. Additional requirements will be determined if the Service Provider is engaged by a Customer to propose or deliver services.

2.1.5 Network Connectivity

Service Provider is responsible for providing the necessary network connectivity to DIR Facilities required to support the Services in accordance with the established Service Levels.

2.1.6 Dashboard

Service Provider shall provide a dashboard for use by DIR and each Customer as defined in **Exhibit 2.1.2**, Cross-Functional Services. The dashboard shall provide a real-time user interface, showing a graphical presentation of the current status and historical trends of DIR's, the Customer's, or computer appliances key performance indicators necessary to enable instantaneous and informed decisions to be made at a glance.

Customers will require a single tenant dashboard. However, DIR will require a multi-tenant dashboard allowing DIR to access the dashboard for any of the Customers.

2.1.7 Centralized Data Repository

Service Provider shall provide an on-line and secure Centralized Data Repository to store, at a minimum, all DIR Data, log files, and documentation generated as part of and required to

perform the Services. All DIR Data shall be kept in accordance with the Customer's applicable record retention requirements. The Centralized Data Repository shall be single tenant for each Customer. DIR requires a multi-tenant Centralized Data Repository allowing access to the repository for other Customers. Service Provider is responsible per **Exhibit 2.1.2**, Cross-Functional Services, and **Exhibit 13**, Reports, to provide timely and integrated data feeds to the MSI for reports placed on the DCS Portal, including Configuration Management.

2.1.8 Systems and Tools

Service Provider is required to provide any tools (both hardware and software) necessary for the execution of the Services. Service Provider shall maintain tools to meet performance standards, processes and policies requirements, to maximize efficiency, and to minimize outages, as necessary.

Customers may request, through the Request Management process, that the Service Provider use the Customer's tools to provide the Services. These Customer Requests will be priced at time of request based on the criteria defined in **Exhibit 4**, Pricing.

Service Provider shall use the systems and tools provided by the MSI in delivering Services.

2.1.9 Operational Support

Service Provider is responsible for managing the technical operations that support the delivery of the services according to best practices, including regular backups, capacity management, availability management, and Service Provider's own disaster recovery and business continuity. Operational support must be provided for any systems, services, or components on a 24x7x365 basis, in accordance with DIR published processes in the Service Management Manual, including but not limited to maintaining current Hardware and Software version levels on all Systems, Services, and Components in compliance with 1 TAC 202, Customer published standards and processes, and DIR governance board. Reference **Exhibit 4B** for hardware and software version requirements.

2.1.10 Transition Status Meetings

As directed by DIR, Status meetings will be held at DIR offices to update progress made, seek input from DIR, and to ensure that work is proceeding in the desired direction. Any issues affecting this project shall be addressed at these meetings. Initially, it is intended that these meetings will be held at least weekly. The frequency of these meetings may be altered to fit the then current need. At a minimum, the Status Meetings shall include:

1. Agenda – Service Provider shall provide a written agenda to DIR Project Manager at least 24 hours prior to meeting. This will allow DIR Project Manager the opportunity to include any additional topics.

2. Minutes - Service Provider shall keep minutes of each meeting and provide a written copy to DIR Project Manager within two business days of the meeting. As a minimum, minutes shall address topics discussed, issues raised, and intended resolution of those issues.

3. Status Reports - Service Provider shall provide weekly written status reports to the DIR Project Manager. The written status reports shall address Tasks Completed, Tasks in Progress, Work to be Initiated During the Next Period,

identified Risks with Risk Management approach, and Issues Requiring Management Attention. Issues Requiring Management Attention shall include, but not be limited to, any problems that may delay performance along with proposed corrective action, any failure of Service Provider or DIR to perform, any delay of Service Provider or DIR in performing, and any inadequacy in the performance of Service Provider or DIR.

In the event the Service Provider fails to timely specify in writing, within the applicable weekly reporting period, an Issue Requiring Management Attention for the Weekly Status Report, Service Provider shall not be entitled to rely upon such Issue as a purported justification for either (1) claiming Service Provider is entitled to receive any amount (including, without limitation, damages or additional charges arising out of a breach by DIR or Customer of a DIR or Customer obligation) with respect to Service Provider's obligations hereunder in excess of those previously agreed to; (2) failing to complete any of Service Provider's obligations hereunder or (3) requesting any reduction in or avoidance of damages or penalties. Submission of the above referenced status reports shall not alter, amend or modify Service Provider's or DIR's rights or obligations pursuant to any provision of the Contract.

2.1.11 Key Service Provider Personnel

Service Provider shall designate Key Personnel for the Service Component and each of the service areas in accordance with the MSA, **Section 8.1**, Key Service Provider Personnel. At a minimum, Key personnel shall include:

1. Account Manager
2. Executive Sponsor
3. Transition Manager (TM)
4. Technical Subject Matter Experts or Leads

All proposed personnel shall be immediately available to provide services as required. Key Service Provider Personnel may not be removed from the project without DIR's written permission.

2.1.12 Confidentiality

In providing services under this contract, the Service Provider will have access to confidential information related to each Customer. Therefore, Service Provider may be required to execute a non-disclosure/confidentiality agreement with each Customer.

Information obtained by Service Provider in the performance of this Contract shall be used only for the purposes of carrying out the provisions of this Contract. Inspection by or disclosure of any such information to anyone other than an officer or employee of Service Provider or Customer, other than for the purposes of carrying out, and in accordance with, the provisions of this Contract, shall require prior written approval of the Customer.

Service Provider shall implement and document a comprehensive information security program. Service Provider shall use, implement, and document reasonable and appropriate security practices to make information secure. If the security of any shared data is compromised or breached by Service Provider, subcontractors, or third-party, Service Provider shall notify DIR and Customer immediately, but no later than 12 hours after discovery of the potential compromise or breach. Service Provider shall be liable to Customer for any compromise or breach whatsoever and shall be liable for all reasonable and appropriate costs (as determined

by DIR or the Customer) associated with remediating the compromise or breach, as defined in the Master Services Agreement.

2.1.13 Background Checks

Prior to commencement of any services, Service Provider is required to conduct background and/or criminal history investigation of the Service Provider's employees and subcontractors who will be providing services under the resulting contract in accordance with MSA, **Section 8.6(g)**, Background and/or Criminal History Investigations, and **Exhibit 17**, Safety and Security.

3.0 Service Descriptions – Incident Response

3.1 Incident Response Service Component

Incident Response Services are intended to assist agencies in meeting internal needs, as well as state and Federal legal and regulatory requirements for providing effective monitoring and analysis of information security events as well as response to information security and privacy incidents. Upon discovery of a cybersecurity incident, the Incident Response Service Provider (IR Service Provider) shall coordinate with the Customer's Information Security staff, or designated points of contact, to follow any Incident Response plan that the Customer has in place. At the same time, the IR Service Provider shall provide information on the scope of the incident and recommendations for remediation to Customer's management and work closely with Customer's legal counsel to provide the detailed information necessary to ensure the Customer's understanding of the magnitude of the incident and possible impacts of the situation. Additionally, the IR Service Provider shall look for any evidence in the Customer's network and identify all assets/information that may have been compromised. The IR Service Provider may also be called on to collect information related to a security incident that could be used in a legal action.

The IR Service Component is divided into three (3) Service Areas:

1. Incident Management
2. Digital Forensics
3. Response Preparedness

3.1.1 Incident Management

The IR Service Provider shall develop for the Customer's written approval and execute as required well understood and appropriate responses to damaging events, computer intrusions, service disruption, security compromises, and inadvertent data disclosure or loss. As part of Incident Response, the IR Service Provider shall provide the necessary resources to manage and support the Customer in preparing for and resolving the Security Incident.

3.1.1.1 Incident Management Service Requirements

At a minimum, the IR Service Provider shall meet or exceed the following Incident Management requirements:

1. Provide a technical team of subject matter experts to be available 24 X 7 upon the declaration of a Security Incident to respond to Security Incidents in accordance with Customer's IT security requirements, policies, and processes.
2. Track all Security Incidents in accordance with STC polices as documented in the Service Management Manuals and with Customer's security requirements.

3. Provide Customer with a dedicated investigative liaison, who will serve as an alternate escalation point to any 'hotline' service the IR Service Provider provides, and will directly contribute to the delivery of Customer's emergency Incident Response.
4. Determine root cause of Security Incident.

3.1.2 Digital Forensics

IR Service Provider shall take part in the recovery and investigation of material or artifacts found in Customer's digital devices as part of the Incident Response services.

3.1.2.1 Digital Forensics Service Requirements

At a minimum, the IR Service Provider shall meet or exceed the following Digital Forensics requirements:

1. Provide Digital Forensics services, as requested by DIR or the Customer, to collect, examine, investigate, and report on authorized access and use of DIR and Customer computer systems.
2. If applicable, coordinate services to capture and analyze forensic evidence with Customer's forensics team, whether internal or a third-party provider.
3. Document and manage processes that provide a chain of custody for all materials collected.
    a. These processes shall be mutually determined by DIR and the Customer and the IR Service Provider.
    b. Provide controls that manage any change in materials being collected.
    c. Uniquely track and report on all collected materials.
4. Provide reverse engineering and systems analysis capabilities.
5. Provide assistance to Customer's Investigation Team with any investigations (e.g., employee misconduct, fraud, embezzlement).
6. Provide forensic evidence acquisition services, including but not limited to log data collection.
7. Analyze forensic data, images, or related logs whether captured by IR Service Provider, Customer, or a third-party.

NOTE: In order to provide timely Digital Forensics services, IR Service Provider must have available staff resources who have successfully completed the Background Check requirements in accordance with MSA, **Section 8.6(g)** Background and/or Criminal History Investigations, and **Exhibit 17**, Safety and Security.

3.1.3 Response Preparedness

The intent of Response Preparedness is to produce a Security Response Plan and provide verification, through regularly scheduled test exercises, that the Customer can respond to major security incidents within the required and agreed upon business timeframes.

3.1.3.1 Response Preparedness Service Requirements

At a minimum, the IR Service Provider shall meet or exceed the following Response Preparedness requirements:

1. Identify and document for Customer's written approval the required business time frames for responding to security incidents based on Severity Level, policy, and state statutes.
2. Develop for Customer's written approval and maintain a Security Response Plan

that defines the activities and responses that are required to verify the Customer is able to satisfactorily respond to a security incident within any required and agreed upon time frames. The contents of the Security Response Plan will be mutually determined by DIR and the Customer and the IR Service Provider.

3. Develop for Customer's written approval a Security Response Test Plan designed to validate the proposed responses of the Security Response Plan.
    a. The contents of the Security Response Test Plan will be mutually determined by DIR and the Customer and the IR Service Provider.
    b. IR Service Provider shall conduct an annual Security Response Test Plan exercise. Based on the results of the exercise, the Customer may require an additional Security Response Test Plan exercise(s).
    c. IR Service Provider shall develop, in coordination with the Customer and for Customer's written approval, test objectives and success criteria designed to verify that Customer's IT organization, security organization, other Service Providers and designated third-party vendors can respond to a major security incident.
    d. IR Service Provider shall identify and document all the required IT technical and services operations (including computer systems, networks, Applications, data repositories, telecommunications, environment, technical support and Service Desk) for test execution.
    e. IR Service Provider shall coordinate with Customer, other applicable Service Providers, and any of the Customer's designated Third Party vendors to establish a schedule and calendar of test activities.
4. IR Service Provider shall schedule testing dates in coordination with the Customer, its designees, other Service Providers, and other third-party vendors.
5. IR Service Provider shall facilitate the Security Response Test Plan exercise, capture all results, and prepare a written report for the approval of the Customer.
6. Based on results of exercise, IR Service Provider shall appropriately update the Security Plan for the Customer's written approval.
7. At Customer's request, participate in and conduct annual Incident Response management exercises in accordance with guidance set forth in 1 TAC 202 and provide recommendations for improvements based on the lessons learned.
    a. The IR Service Provider shall coordinate with the Customer regarding the scope and timing of the Incident Response exercise.