

**Amendment Number Seven
to
Contract Number DIR-TEX-AN-NG-CTSA-005
between
State of Texas, acting by and through the Department of Information Resources
and
AT&T Corp on behalf of itself and all of its affiliates**

This Amendment Number Seven to TEX-AN-NG Contract Number DIR-TEX-AN-NG-CTSA-005 ("Contract") is between the Department of Information Resources ("DIR") and AT&T Corp on behalf of itself and all of its affiliates ("Vendor"). DIR and Vendor agree to modify the terms and conditions of the Contract dated July 1, 2011 as follows:

1. TEX-AN NG Communications Technology Services Agreement, Exhibit B. General Terms and Conditions, Section 3.11. Vendor Certifications is hereby appended with the following new subsections:

(p) Represents and warrants that in accordance with Section 2271.002 of the Texas Government Code, by signature hereon, Vendor does not boycott Israel and will not boycott Israel during the term of this Contract; and

(q) Represents and warrants with Section 2155.0061, Government Code, the vendor certifies that the individual or business entity named in this contract is not ineligible to receive the specified contract and acknowledges that this contract may be terminated and payment withheld if this certification is inaccurate.

2. TEX-AN NG Communications Technology Services Agreement, Exhibit B. General Terms and Conditions, Article 4 Vendor Personnel Management is appended with a new **Section 4.09. Cybersecurity Training**, as follows:

Section 4.09 Cybersecurity Training.

In accordance with Section 2054.5192, Texas Government Code, for any contract with a state agency, if Vendor, or a subcontractor, officer, or employee of Vendor, will have access to a state computer system or database, then such officer, employee, or subcontractor shall complete a cybersecurity training program certified under Section 2054.519, Texas Government Code, as selected by Customer state agency. The cybersecurity training program must be completed by such officer, employee, or subcontractor during the term of the contract and during any renewal period. Each such officer, employee, or subcontractor shall verify completion of the program to the Customer state agency.

3. **TEX-AN NG Communications Technology Services Agreement, Exhibit C. Descriptions, Rates to DIR, Prices for direct sale transactions and related telecommunications fees and surcharges for Awarded Services, Article 4. Documents Referenced in *Exhibit C*, Attachment C-1 SERVICES OFFERED UNDER THIS CONTRACT** is hereby amended to add the following:

VII. AT&T Switched Ethernet (ASE)

AT&T Switched Ethernet Service is a transport service that uses industry-standard Ethernet technology to transport traffic among two or more locations. AT&T Switched Ethernet Service uses native Ethernet interfaces to transport data without using protocol conversion or special equipment.

We offer AT&T Switched Ethernet Service in speeds of 2 Mbps to 100 Gbps, and you can choose from multiple options for redundancy as well as Class of Service (CoS). This means that you can match your network's performance to your applications' needs.

How ASE Works

We deliver AT&T Switched Ethernet Service over fiber or copper facilities that connect to the MPLS-based switched Ethernet core network. Ethernet Private Line arrangements (E-Lines) can connect remote locations to a hosting data center and Virtual Private LAN Services (E-LANs) can enable any-to-any converged voice and data networks with Class of Service (CoS) intelligence. Port connections are available at 100 Mbps, 1,000 Mbps (1 Gbps), 10,000 Mbps (10 Gbps), and 100,000 Mbps (100G). Those physical ports offer a range of Committed Information Rates (CIRs), from 2 Mbps to 100 Gbps, to align with your need for a given location. You can create Virtual Local Area Networks (VLANs) to subdivide your network into segments that support different user groups or applications.

VIII. AT&T Dedicated Ethernet (ADE)

AT&T Dedicated Ethernet is a fiber-based, point-to-point solution that connects your data service within the same local access and transport area (intraLATA) and transmits data at speeds up to 100 Gbps as either native Ethernet or Optical Transport Network (OTN) formats. AT&T Dedicated Ethernet supports an unprotected and non-diverse configuration and also offers you optional diversity and data protection features.

Our AT&T Dedicated Ethernet can interface natively to your Ethernet-based equipment. Consequently, it provides you with high capacity and efficient data transport without the need for special equipment or protocol conversion.

How ADE Works

AT&T Dedicated Ethernet transports your data via fiber on a point-to-point circuit that runs on an expansive dense wavelength division multiplexing (DWDM) network. Every circuit passes through at least one central office-based optical multiplexer (OM), which serves as a signal regenerator (also known as a repeater) and is what enables us to monitor your traffic. We connect AT&T Dedicated

Ethernet to the fiber patch panel on your premises, and your Ethernet switch or router then uses the service to send and receive data. The Service is an emergency (9-1-1) call routing solution designed for use in the nationwide transition and adoption of Next Generation 9-1-1 (NG 9-1-1) technology.

IX. AT&T Emergency Service IP Network™ (AT&T ESInet™)

The Service is an emergency (9-1-1) call routing solution designed for use in the nationwide transition and adoption of Next Generation 9-1-1 (NG 9-1-1) technology.

1. Geographic Availability

The Service is available within most of the continental United States of America to State, County, Regional 9-1-1 authority or other government entity responsible for providing 9-1-1 service. AT&T will expand the availability of the Service as resources and contractual commitments allow. The Service is not available to federal agencies, the military or entities that design their own emergency response systems.

2. General Description

The Service is a resilient call routing service utilizing AT&T's nationwide IP network and 9-1-1 services to route and deliver 9-1-1 calls from any Originating Service Provider (OSP) to a designated Public Safety Answering Point (PSAP). The originating call received from AT&T's wireline or mobility networks and from OSPs' networks is routed through AT&T's network to IP-based 9-1-1 application systems that identify the PSAP to which the call should be delivered. The call is then routed over a fully redundant AVPN network to the Network Terminating Equipment (NTE) located at the appropriate PSAP. The Service is designed to handle call routing and delivery of IP-based 9-1-1 voice calls and data. In addition to supporting VoIP calls from mobility and land lines, the Service also supports SMS to 9-1-1 text messaging, location-based services such as Automatic Location Identification (ALI) and Automatic Number Identification (ANI) and GIS-based routing over a managed IP network.

The Service is designed to support the applicable functional elements to the National Emergency Number Association (NENA) i3 Standards, NENA Technical Standard 08-003. The Service supports call delivery to both IP-enabled NENA i3 PSAP CPE hosts as well as legacy PSAP CPE hosts that are not yet IP-capable.

The Service includes management of incoming 9-1-1 calls from Originating Service Provider (OSP) networks. Collectively, these capabilities are referred to as the "Service". Additional information can be found in the AT&T Business Service Guide - AT&T Emergency Service IP Network™ (AT&T ESInet™)

3. AT&T ESInet™ Security Overview

AT&T ESInet™ is a highly secure, privately managed IP network providing IP based call routing services for next generation 9-1-1 call delivery. All inbound and outbound traffic interactions are with pre-authorized entities, utilize agreed upon protocols and traverse controlled access points. Call processing and real-time data delivery are protected through both physical and logical controls.

AT&T's ESInet cyber security policies, standards, and guidelines are consistent with industry best practices as defined by International Organization for Standardization and Control Objectives for Information and related Technology. The AT&T ESInet™ solution network architecture follows the guidelines and recommendations of the NENA ESIND (ESInet Network Design) and meets the security criteria as defined in the NENA NG-SEC specifications for NG9-1-1 security.

4. AT&T ESInet™ Security Features

Specific elements built into AT&T ESInet™ that help secure the network include:

- **Defense-in-Depth.** The AT&T ESInet™ infrastructure is designed to withstand sophisticated attacks by means of a defense in depth strategy. The AT&T ESInet employs high availability systems with geographic diversity and component redundancy at the physical, network, platform and application layers that are wrapped up into a “single pane of glass” end-to-end monitoring. The security architecture employs best in class mechanisms such as, stateful packet inspection firewalls, Intrusion Detection Systems (IDS), multi-factor authentication, strong encryption, encrypted data at rest, anti-virus/anti-malware, vulnerability and patch management solutions.
- **Physical Security.** All Core sites and Aggregation Centers are located in AT&T owned and maintained secure facilities and are only accessible to authorized personnel.
- **Encryption.** Highly secure IP SEC VPN tunnels are established between PSAPs and the core sites to encrypt data in transit
- **Least Privilege.** Infrastructure routers and Provider Edge (PE) interfaces are hardened by turning off, or severely restricting, unnecessary protocols and ports.
- **Industry Standard Security M&Ps.** Control of operational security in AT&T's network is strictly enforced to maintain high levels of reliability and availability. To accomplish this, AT&T operations follow mature and proven Methods & Procedures and are certified, wherever appropriate, to the highest industry standards. Additionally, all incidents are subject to comprehensive Root Cause Analysis to ensure that processes are improved.

- **Proactive Network Security Probes.** AT&T Network Security continually probes its networks, both internally and externally, for security vulnerabilities using the same techniques as a potential intruder. AT&T compiles and analyzes test results, reports their findings to the organization that requested testing, and recommends measures to close the vulnerabilities that testing uncovered.
 - **Disaster Recovery.** The 24x7 operations center employs an Incident Handling process modeled on FEMA's Incident Command System, with notifications built into this process.
 - **AT&T Labs.** All hardware and software elements deployed in a production environment go through stringent release management processes that incorporate thorough penetration scan testing.
- Collectively, including the AT&T Business Service Guide – AT&T Emergency Service IP Network (AT&T ESInet), these capabilities are the AT&T ESInet service.

All other terms and conditions of the Contract as amended, not specifically modified herein, shall remain in full force and effect. In the event of conflict among the provisions, the order of precedence shall be this Amendment Number Seven, then Amendment Number Six, then Amendment Number Five, then Amendment Number Four, then Amendment Number Three, then Amendment Number Two, then Amendment Number One, and then the Contract.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

IN WITNESS WHEREOF, the parties hereby execute this amendment to be effective as of the date of last signature.

AT&T Corp on behalf of itself and all of its affiliates.

Authorized By: /signature on file/

Name: Brandon Trotter

Title: Contract Specialist CGI

Date: 08/21/2019

HD091V

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

Authorized By: /signature on file/

Name: wayne Ege1er

Title: Director CTS

Date: 9/9/2019 | 12:37 PM CDT

Legal: /initials on file/