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 17
Safety and Security

October 26, 2017

TABLE OF CONTENTS

1. INTRODUCTION

In performing the Services all Service Providers shall observe and comply with the policies, rules, procedures and regulations set forth or referenced in this Exhibit.

2. SAFETY AND SECURITY

The Service Provider's responsibilities include and the Service Provider, at a minimum, shall do the following:

1. Adhere to the then-current safety and security policies, rules, procedures and regulations established by the State and DIR, and each Customer with respect to Customer's Data and Facilities.
2. Adhere to DIR and Customer's then-current Security Rules, as published in 1 TAC 202, Information Security Standards of the Texas Administrative Code.
3. The Service Provider shall comply with the policies defined by the FBI Criminal Justice Information Services (CJIS) requirements, where applicable.
4. DIR and Customers comply with National Institute of Standards and Technology (NIST) Federal standards and related NIST 800 series Special Publications (SP) and Federal Information Processing Standards (FIPS) standards. Where there is a conflict between NIST, FIPS, and 1 TAC 202 rules and security controls, the 1 TAC 202 takes precedence.
5. Comply with all security incident notification and response procedures as specified in the Service Management Manual.

3. SECURITY ASSESSMENTS

DIR, Customers, Texas State Auditor's Office, and other entities authorized by DIR may conduct security reviews, assessments, forensic analysis and/or audits (e.g., SOC 2, State Audit Office, IRS audits) of locations where service is being provided by the Service Provider. These assessments may include (but are not limited to) physical security, logical security, policies and procedures, network analysis, vulnerability scans and Controlled Penetration Tests.

4. CRIMINAL HISTORY BACKGROUND CHECKS

1. The Service Provider staff are required to successfully complete a background and criminal history investigation prior to performing contract functions or accessing DIR or Customer Facilities, Systems, networks, or Data under this contract. Criminal history background checks are to be conducted per Texas Government Code (TGC) Subchapter F, Section 411.1404 and will be in compliance with the then-current versions of the FBI CJIS Security Policy and the FBI CJIS Security Addendum. In addition, an annual background check re-verification is required. DIR must be notified of the compliance with the initial criminal history background check and the annual re-verification. The Service Provider shall be responsible for any costs associated with this process.
2. Background and criminal history investigations shall be performed by the Texas Department of Public Safety, Texas Department of Criminal Justice, and the Texas Department of Family and Protective Services. Other Customers may require additional levels of compliance as per agency regulations and policies.

3. The MSI will establish a comprehensive security clearance database capable of tracking and reporting on all MSS Service Provider personnel. All persons having been cleared shall be reported to the MSI and documented in the Security Clearance Database. The Service Provider shall establish a process and reporting procedure, approved by DIR, which shall provide timely notifications and updates of the database of personnel who are added to or depart from the contract. Reports shall be provided no later than 24 hours after employee departure from the contract. Documented policies for this requirement will be drafted by the MSI and approved by DIR.

5. REFERENCES

The Service Provider shall perform the Services in compliance with all federal and state laws and industry standards as they may be updated from time-to-time, including but not limited to the following:

- Texas Administrative Code (TAC) 1 Chapter 202. TAC 202 provides the State of Texas security standards policies applicable to all Texas state agencies.
- HIPAA – Health Insurance Portability and Accountability Act Privacy and Security Rules
- HITECH – Health Information Technology for Economic and Clinical Health Act
- FIPS 140-2 Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules
- FISMA – Federal Information Security Management Act
- FERPA – Family Educational Rights and Privacy Act
- FACTA – Fair and Accurate Credit Transactions Act
- IRS Pub 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies
- PCI – Payment Card Industry Security Standards
- ISO/IEC 27001:2005 - Information technology – Security techniques – Information security management
- ISO/IEC 27002 – code of practice for information security management
- NIST 800 – National Institute of Standards and Technology standards and related publications
- CJIS Security Policy - FBI Criminal Justice Information System Security Policy and CJIS Security Addendum
- Cybersecurity Act of 2015