

20160606-8386



0232

GBS160752-1

DIR Agreement Number DIR-TSO-1860-SOW4 CTSMA Agreement No.: ~~DIR-SDD-1860~~AT&T Network Integration Tracking ID: **GBS160752-1**Document Version #: **1.0**Date: **06/03/2016**HR ID: **Rx3439**

CUSTOMER Legal Name ("Customer")	AT&T Corp. ("AT&T") (designate other entity if signing entity other than AT&T Corp)	AT&T Branch Sales Contact Name
Texas Department of Information Resources	AT&T	Name: Marcus Montemayor
CUSTOMER Address	AT&T Corp. Address and Contact	AT&T Branch Sales Contact Information
Address: 300 W 15 th St, Suite 1300 City: Austin State: TX Country: USA Zip Code: 78701	One AT&T Way Bedminster NJ 07921-0752 Contact: Master Agreement Support Team Email : mast@att.com	Address: 712 E Huntland Dr Room 313 City: Austin State: TX Zip Code: 78752 Phone: 512-421-5160 Email: mm3894@att.com Sales/Branch Mgr: J. Zimmerman SCVP Name: G. Spencer
CUSTOMER Contact	AT&T Address and Contact (if required)	AT&T NI Contact Information
Name: Sally Ward Title: Dir of Data Ctr Services Telephone: 512-936-0949 Email: sally.ward@dir.texas.gov	Name: Address: City: State / Province: Zip Code: Country: Telephone: Email:	Name: Randy Murray City: Durham State: NC Zip Code: 27703 Telephone: 919-720-2919 Email: rx3439@att.com
CUSTOMER Billing Address		
Address: 300 W 15 th St, Suite 1300 City: Austin State: TX Country: USA Zip: 78701		

This Pricing Schedule for Network Integration Services ("NI Pricing Schedule") is part of the Master Agreement between AT&T and Customer referenced above ("Agreement"). The AT&T Network Integration Services provided under this NI Pricing Schedule shall be governed by the Terms and Conditions contained herein and by the terms of the Agreement. This NI Pricing Schedule is effective, and incorporated in and made part of the Agreement, on the latter of the dates when signed by both Customer and AT&T (the "Effective Date").

AGREED:
CUSTOMER: Texas Department of Information Resources

By: Sally Ward
(Authorized Agent or Representative)

Sally ward
(Typed or Printed Name)

8:57am
(Title)

6/13/2016 | 8:57 AM CDT
(Date)

ATTUID: rx3439

AGREED:
AT&T

By: Patrick J. Gleason
(Authorized Agent or Representative)

Patrick J. Gleason
(Typed or Printed Name)

Sr. Customer Contracts
(Title)

(Date) June 6 2016

MR405Y



Appendix C to DIR Contract No. DIR-SDD-1860

SERVICE AGREEMENT NO. MS-005-2012

THIS SERVICE AGREEMENT NO. : MS-005-2012 (the "Service Agreement") is made and entered into this _____ day of _____, between State of Texas Department of Information Resources, ("Customer"), and AT&T Corp [Name of applicable AT&T entity to be inserted when Service Agreement is developed] ("Vendor" or "AT&T").

This Service Agreement is entered into between Customer and AT&T pursuant to the DIR Contract No. DIR-SDD-1860 ("Contract"). Customer and AT&T agree that: (i) except to the extent expressly provided otherwise in this Service Agreement, all the terms and definitions of the Contract are incorporated by reference into this Service Agreement, (ii) the schedules and exhibits attached hereto are incorporated by this reference, and (iii) in the event of any inconsistent or contradictory terms between the Contract and the Service Agreement, the terms of the Contract shall control. This Service Agreement is effective on the date of last execution ("Effective Date").

Customer and Vendor hereby agree as follows:

1. DEFINITIONS

All defined terms that are used in the Contract will have the same meaning in this Service Agreement. In addition, for purposes of this Service Agreement, the following terms shall have the indicated meanings:

"Service Commencement Date" means the date AT&T and Customer agree specified contracted Services are operational and AT&T begins to take the first help desk calls for Services pursuant to the Operations Plan Outline.

2. TERM

The term for Service provided under this Service Agreement (the "Term") shall begin on June 1, 2016 and shall terminate on July 31, 2016, unless earlier terminated or renewed in accordance with the provisions of this Service Agreement or Section 8.B. of the Contract.

3. TERMINATION

3.1 TERMINATION. Customer may terminate this Service Agreement in accordance with Section 10.B of Appendix A of the Contract and this Section 3.

3.2 CONVENIENCE TERMINATION FEE. If Customer terminates this Service Agreement for convenience in accordance with Section 10B3 of the Appendix A of the Contract, the following termination charges shall apply: [Termination fee formula will be referenced as agreed upon in the DIR contract.]



4. SERVICE ELEMENTS

The Service Elements to be delivered as part of this agreement are detailed in Exhibit A attached.

5. PRICING

Applicable AT&T MIPS Level 3 Services for <i>two-month term include:</i>	Monthly	Extended
<ul style="list-style-type: none"> • Existing Customer deployed McAfee M-8000XC sensors • Operations - IPS Tuning • Management - MSS Firewall Operations and Platform • Management - MSS MIPS Level 3 Operations and Platform 	\$20,818.00	\$41,636.00
<ul style="list-style-type: none"> • Monthly recurring support and operation charge • Includes support for 28 individual virtual IPS profile 		
TOTAL CHARGES:		\$41,636.00

5.1 INVOICES FOR CHARGES AND EXPENSES.

Invoice submission and payment shall be in accordance with the Contract.

6. PERFORMANCE STANDARDS

The Performance Standards pertaining to this agreement are detailed in Exhibit A below.

7. CUSTOMER SITES

Detailed in Exhibit A attached.

8. TRANSITION PLAN

Detailed in Exhibit A attached.

9. CUSTOMER HISTORICAL SERVICE BASELINE

Not applicable

10. AFFECTED EMPLOYEES

Not applicable

11. THIRD PARTY AGREEMENTS

Not applicable

12. PURCHASED EQUIPMENT

Not applicable

13. OPERATIONS PLAN OUTLINE

Any operations plan will be developed and mutually agreeable by all parties as part of the delivery of the service.



EXHIBIT A: STATEMENT OF WORK

Introduction

This Statement of Work ("SOW") is attached to Service Agreement MS-005-2012 (Appendix C of DIR-SDD-1860) as Exhibit A and made a part thereof upon execution. The Parties to this SOW are **AT&T Corp.** ("AT&T") and the **Texas Department of Information Resources** ("Customer"). Services and/or Equipment not specifically provided for hereunder are outside the scope of this SOW. Change Control will be processed by the Parties pursuant to procedures detailed herein. Change Control will be handled by the Parties pursuant to the documented Change Control Process.

AT&T reserves the right to withdraw this SOW or modify the prices and any other terms and conditions, including, but not limited to, any section of this SOW if the SOW is not signed by Customer and AT&T within thirty (30) days of 06/03/2016.

1. Scope of Work for AT&T Managed Security Services

1.1 Managed Intrusion Prevention Level 3 Services Description

AT&T will provide Managed Security Services to include Managed Intrusion Prevention Service ("AT&T MIPS"), Level 3 for two (2) months as described herein this SOW.

Services Overview Description: The AT&T Managed Intrusion Prevention Service is a fully managed, attack recognition and response solution. It provides Host Intrusion Prevention IP attack recognition and response. Intrusion Prevention involves the ongoing monitoring of network traffic for potential misuse or policy violations. Upon recognizing a pattern of misuse (known as a Signature), such as suspicious or unauthorized activity, MIPS responds in a Customer-defined manner to send an alert or to take immediate action.

The following table describes at a high level the applicable capabilities:

Item	Customer Requirements	As Designed: Maximum
Existing Customer Deployed McAfee M-8000XC IPS Devices	Provide Managed Intrusion Prevention/Detection Services within the network to support an initial configuration for 28 state agency end customers	Two (2) State of Texas customer locations in the US: Austin, TX and San Angelo, TX

1.2 Managed Intrusion Prevention Service

MIPS Level 3: A custom service that will meet Customer requirements and provide investigation support. Security Analysts monitor, report, and assist Customers with recommended mitigations.

- AT&T MIPS will be monitored 24 hours x 7 days a week. Host Intrusion Prevention components will be deployed by the customer or customer representatives at strategic locations within the network. This would either be at the Customer's premises, or within their service components located at an Internet DataCenter. The Intrusion Prevention system will monitor data packet header and payload information to detect possible malicious activity and the AT&T S/NOC responds to pre-defined events and alarms based on the Customer's security posture. The Customer defines the signature policy by accepting the AT&T Design Documentation and Technical Provisioning Document prepared by AT&T for the Customer upon the basis of the Customer's decisions.
- The Service to be provided is subject to a technical assurance review by AT&T, prior to providing a contract to customer. This is to validate that the proposed MIPS implementation is technically feasible and workable under the standard definition of the Service. The Customer retains the responsibility to confirm their decisions for sensor placement and signature profile.
- AT&T applies a signature policy that makes use of the Intrusion Prevention sensor manufacturer-provided signature list, and sets the alarm severity and resulting action. Each Intrusion Prevention sensor will be configured by AT&T, based on the Customer determined signature policy, with



changes to the standard alarm and severity settings determined by the Customer. As part of the service implementation process, AT&T works with the Customer to determine the required settings.

- Procedures will be put in place between the AT&T S/NOC and the Customer identified Security Contact(s) to request configuration changes to the policy and to act as a single contact point for Service issues.
- Customers may request additional technical support, which is separately available at an additional cost, to provide support with any vulnerability assessment or risk evaluation that the Customer may require by signing the relevant agreement with AT&T.

1.3 Features of MIPS Level 3

The following table identifies the features and associated functionality by level for AT&T's MIPS Service offering.

Features of MIDS	
Feature/Functionality	MIDS Level 3
Network IDS	NIDS
7x24 Monitoring	Included
Signature Updates Vendor Updates: Emergency	Included 3-5 business days, 24 hours
Incident notification	Email alert for low correlated, medium, and high events. Phone call will also be placed for critical incident.
Custom Reports	Not Included
SENSOR CONFIGURATION	
Initial Sensor Configuration	Custom Tuning
Continuous Sensor Tuning	Included
Custom Signatures	20 per Agency Profile
SECURITY ANALYSIS	
Alarm Analysis	Included
Event Correlation & Analysis	Included with additional real time analyst support
Root Cause Analysis for High Level Alerts	Included
Investigation Support	Included
Customer Notification based on SLO	Included
Attack Signature Recognition	Included
Dynamic Attack Blocking (Intrusion Prevention)	Included
CPE SOFTWARE	
CPE Installation	Not Included
CPE Maintenance	Not Included
Software Installation	Not Included
Software Maintenance	Not Included
Problem Ticketing/Reporting	Included
Initial Configuration Support	Included
Configuration Maintenance	Included
Network IDS	NIDS

1.4 Service Limitations

The following limitations additionally apply to the Service provided:

- The AT&T MIDPS is not capable of analyzing encrypted data streams and would only be able to perform rudimentary analysis based on the packet header information in this scenario
- AT&T does not provide as part of this service any dissemination of generally available security information, including, but not limited to, instant alerts or security advisories relating to threats and/or abnormalities, such as, virus attacks, which may affect networks and their functionality.



1.5 Standard Components

AT&T provides the following Service features for **MIPS Level 3 Service**:

- Provide 7x24 security event monitoring and equipment management.
- Provide profiling (enhanced tuning and data traffic analysis) and professional services to give a baseline of the network or Host alarm activity, including analysis and verification by AT&T.
- Develop customized alert levels, through use of AT&T's proprietary tools and correlation database, so that alarms from individual sensors are correlated to alerts and categorized for response/reporting.
- Perform in-band correlation. In-band correlation refers to AT&T proprietary analysis of sensor data in a Customer's network, both individually and collectively.
- Provide incident response based on signature policies and traffic profiles of Customer's sensors.
- AT&T periodically updates Customer sensor profiles to minimize false positive alerts or alarm activity not related to cyber intrusions.
- Provide root cause analysis where AT&T will determine the source, destination, and type of attack for alerts and provide Customer with specific information on each incident.
- Provide on-line summary reports on a daily, weekly, or monthly basis. A customized incident report is also provided for each High Level alert.
- Provide technical support related to High Level alerts, where Customers will interface with (Tier III) technical analysts.
- Provide technology updates to support the updating of intrusion signature databases, used to trigger alarms for known attacks.
- Regular vendor signature updates:
 - All new IPS signatures from a sensor manufacturer will be implemented within 5 business days of release by the manufacturer(s) and after appropriate verification and testing process of alarm level settings by the AT&T S/NOC. AT&T reserves the right to take longer than 5 business days to implement the update or not to implement it at all.
 - The AT&T verification process may result in the signature being implemented after the 5 business day target or not being implemented.
 - AT&T will make reasonable efforts to implement emergency updates by sensor manufacturers within 24 hours or earlier based on severity, testing, and verification by AT&T.
 - Customer determined, pre-defined, dynamic incident response (i.e., dynamic attack blocking, dynamic session reset), depending upon incident type and severity, for events as specified by the Customer as part of the Customer-specified signature policy for the manufacturer-supplied signature set or for the AT&T-defined unique signatures.

1.6 Customer Responsibilities

Customer may fulfill its responsibilities through use of third parties, but those responsibilities shall remain Customer responsibilities as between Customer and AT&T. Customer responsibilities for each of the available MIPS Level 3:

- Provisioning of the Service Components, which may include some of the following: Intrusion Prevention/Detection sensors, switches, routers and cables depending upon the configuration
- Installing and maintaining the Customer LAN environment
- Provide a network diagram and Security Policy to assist in the professional services activity of placing and configuring sensors, and base lining "normal" traffic to assist in establishing an IDS profile for each sensor.
- Identifying the placement of the Intrusion Prevention sensor software. A Customer's decision relative to sensor placement may impact the ability of the sensor to detect potential traffic threats and may impact the ability of certain applications to perform properly.
- Providing the necessary information, including network diagram and Security Policy, for the Customer's network and Server environment to AT&T as part of the provisioning process and during the lifecycle phase of the Service.



- Completion of provisioning documentation in a timely manner as appropriate to the requirements of the AT&T MIPS implementation schedule, including confirmation of sensor signature level settings or modification of AT&T-provided standard sensor signature level settings.
- Providing AT&T, or its designated agents, access to Customer premise for the purpose of installation and maintenance of the Service and its components as required.
- Designating primary and secondary contacts to/for:
 - Security, system administration and technical issues.
 - Service reporting
 - Change management requests
- Receive and consult on service alarms and to enable Customer initiated incident response
- Ensuring that Customer security contact information provided to AT&T is up to date and appropriate including timely notification of any changes.
- Customer will make every effort to notify AT&T as soon as possible when a security breach is suspected within Customer's network.
- AT&T is not responsible for issues arising from any delays in Customer notification.
- Notifying AT&T at least five working days in advance of any scheduled maintenance, planned outages, or Service configuration changes that may interfere with device monitoring. Customer must notify AT&T promptly of any unscheduled activities that may interfere with device monitoring.
- Designating a contact that has access to room and space where the equipment at the Customer premises will be held.
- Providing functionality testing assistance during implementation, problem and change management processes.
- Where an AT&T MIPS Intrusion Prevention sensor is connected to a Customers LAN, provide and fully manage the switch the sensor is connected to.
- Customers must ensure compatibility with the Service both initially and throughout the service period. It is essential in this case to make sure the Customers switch will support the functions required for the MIPS.
- Provide network and/or Server, including Firewall, support to allow the flow of MIPS traffic for management purposes.
- Ensuring that the AT&T MIPS does not conflict with any service provided by an agreement between the Customer and a 3rd Party supplier, and the Customer is responsible for any impacts or conflicts that may occur including their satisfactory resolution at the Customers expense to the extent they prevent the provision of the AT&T MIPS. The Customer remains liable for the charges due to AT&T during such period. .
- Ensuring that the AT&T MIPS supplied has adequate capacity to support the communication link(s) to be monitored. Customers must inform AT&T of any bandwidth upgrades or increased traffic flows on the network segment to which the sensors are attached.
- Complete required AT&T MIPS Level 3 pre-deployment worksheet.
- Cooperate with AT&T in identifying severity levels for specific groups of attack signatures.
- Cooperate with AT&T in identifying escalation policies and procedures.
- Provide an IPSEC termination point for the AT&T management tunnel
- Provide updated escalation contacts and reach numbers as they change.
- It is recommended that the Customer implement an event response process to use when Customer's receive security event notifications from the Managed Intrusion Prevention Service. Due to the diverse nature of security events, international regulations and Customer environments, the Customer is solely responsible to establish any such events response processes for their use.
- Provide servers as required in each data center that is appropriate.

AT&T Security will require two virtual server (VM) instances, on managed and one un-managed by Atos.



The first server owned and managed by Atos will be a Windows 2008 terminal server supporting up to 5 simultaneous users. The only application to be installed will be Firefox. AT&T MSS Threat Management personnel do not need special privileges on this server.

The second server will be a Linux based tools server that AT&T Threat Management will have Atos with AT&T Security performing subsequent configuration, and ongoing management. This server will run a web server and contain scripts to allow the analysts access to the detailed capture information from the McAfee NSP. Minimum specs for this server are: 2x CPUs, 4 GB RAM, 60 GB disk space.

1.7 Service Availability

The AT&T MIPS will be available 24 hours a day, 7 days a week, except for the following instances:

- During scheduled/unscheduled maintenance windows
- During systems upgrades/sensor tuning
- During connectivity or network outages
- Note that during any of these instances, alarm notification to the Customer may be delayed.

1.8 Support and Management

A. Support

AT&T will provide the following support as part of the AT&T MIPS as determined by the service level selected by the Customer:

- Provisioning of the Service Components, which may include some of the following: intrusion Prevention sensors, switches, out-of-band access and remote power equipment, router and cables depending on the configuration.
- Registration of Customer information and security configuration in AT&T's databases that is required by AT&T to deliver the Service.
- Project management.
- Configuration of the Customer IDS according to the agreed signature profile defined by the Customer.
- 7x24 Customer support.
- Proactive monitoring and emergency procedures.
- Problem management: logging, tracking and escalation of reported problems based on pre-determined severity levels set by Customer.
- Communication with the Customer designated security contact(s) on service related issues including:
 - Security, system administration and technical issues.
 - Service reporting.
 - Change management requests.
 - MACD (Move, Add, Change, and Delete) Change Request can be submitted through the Business Direct Web Portal at <http://www.businessdirect.att.com> Additionally, we support direct calls. The Business Direct access requires a Business Direct ID and password.
- Receive and consult on service alarms and to enable Customer initiated incident response
- Work with AT&T on all matters related to this service.
- Management and implementation of Customer-requested signature changes.
- Provision of defined Service reports and facilities via the AT&T web portal or other web-based portal mutually agreed upon by both customer and AT&T



- Event Data (IP addresses and Signature Name) will need to flow to the AT&T MSS management center. Packet capture data will remain in the customer datacenter and local NSP.

All AT&T Threat Management Security Analysts supporting State of Texas Data Center will maintain appropriate State of Texas Data Center security background investigation compliance, as mutually agreed upon by AT&T and the State of Texas Department of Information Resources.

B. MIPS Level 3 Event Response

The following event response process will apply for MIPS Level 3:

1. An automated correlation of intrusion events, adding AT&T proprietary analysis tools and trained security analysts to respond to alerts in accordance with a Customer's individual Security Policy.
2. Technical support personnel will work with Customers in establishing the specific signatures and their associated severity level alerts and any service level objectives that may be available. This process will take place during the initial sensor tuning period to ensure that the alerts and severity levels are tailored to meet the Customers requirements.

C. Severity Alert Definitions:

The following definitions clarify each of the MIPS severity levels:

1. High Severity Security Alerts

High severity alerts constitute an alert or combination of alerts that define a security threat or breach against critical business/service/systems. Examples of possible high severity alerts are denial of service attacks which consume enough bandwidth or CPU cycles to impact the Customers service; or an identified attempt to gain root privilege on a Customer device through a monitored network or on a monitored device; or a non-severe attack that is escalating at such a rate that it is likely to eventually breach the system or render service inoperable.

2. Medium Severity Security Alerts

Medium severity alerts, or combination of alerts, are those that do not place the business /service/system in immediate risk of compromise, but may pose severe risks if not dealt with in a timely fashion. Examples of alerts at this level are attacks that are persistent and may degrade the system without impacting it significantly; or any attack that displays a strong understanding of the systems involved as this could indicate an attack using inside information.

3. Low Severity Alerts

These are alerts or combinations of alerts that do not pose severe risks but may indicate trends or patterns that might suggest future impact. Examples of alerts at this level are port scans originating from the Internet that may indicate reconnaissance for a future attack, or any unusual traffic patterns.

D. Transition – End of Contract Term

Upon termination of this contract with the State of Texas, AT&T will perform the following transition:

- De-install the Linux VM server and all associated AT&T Proprietary software that is placed in the Atos datacenter for AT&T's management purposes.
- Remove all AT&T best practices signature set from the IPS sensors
- Ensure that the vendors default Signature set is enabled.
- AT&T will document the customer's specific tuning parameters.
- Customer must submit a MACD prior to contract termination to request this action.
- AT&T will provide list of tuning parameters for the customer to reapply to the sensor after transition
- Prior to decommissioning, Customer should submit a MACD request to have AT&T document the customer specific tuning parameters so that the customer can reapply the parameters after the transfer of control of the asset has occurred.



1.9 Help Desk Support

- All problems, questions or requests for assistance related to the MIPS should be made to the designated AT&T help desk support. Problems may be reported by telephone or electronically, where available as specified by AT&T. The time an incident starts is when a Customer speaks to the help desk, or when a Customer submits an electronic notification, or when an AT&T generated ticket is opened, as the case may be.
- US Centralized Customer Help Centers provide 7x24 problem assistance

1.10 Service Reporting

MIPS Level 3:

AT&T will provide the following standard reports, which will be available via an AT&T managed services portal. The Customer will be provided with secure User-IDs and passwords to enable access to the portal and are fully responsible for the use and management of these User-IDs. Each customer Agency will have an individual report view consistent with their Agency service profile.

- **IDS/IPS Directions & Severities**
 - **IDS Events By Destination IP** - This report summarizes IDS Events. The report can be broken down by Top 10, 20, 30, 40 or 50 by Date, Site Name, Event Type and Destination IP
 - **IDS Events By Protocol/Port** - This report summarizes IDS Events. The report can be broken down by Top 10, 20, 30, 40 or 50 by Date, Site Name, Event Type, Protocol and Port
 - **IDS Events By Source IP** - This report summarizes IDS Events. The report can be broken down by Top 10, 20, 30, 40 or 50 by Date, Site Name, Event Type and Source IP
 - **IDS Events By Source/Destination IP** - This report summarizes IDS Events. The report can be broken down by Top 10, 20, 30, 40 or 50 by Date, Site Name, Event Type and Source/Destination IP
 - **IDS Activity By Event Type** - This report summarizes IDS Activity by ranking through Event Type. The report can be broken down by Date, Site Name, Host, Event Type
 - As part of the data gathering that takes place during enablement of the Service, AT&T will gather Customer contact details for the reporting system.
 - Reports are available on a daily, weekly and monthly basis.
 - Reporting will be provided on an individual virtual IPS profile.

1.11 Service Features:

- Implementation of up to twenty-eight (28) individual virtual IPS profiles
- Additional individual virtual IPS profiles can be supported at a charge. (This will be based on any increment above 28)
- An individual virtual IPS profile is based on a single VLAN. (1 VLAN per customer)
- **Regular Vendor Signature updates:**
 - AT&T being the Customer's subcontractor, Customer is solely responsible for **informing AT&T of the parameters to be used in programming and implementing the Intrusion**



Prevention functions of the MIPS Service, and obtaining, as required by applicable laws, all consents of all persons whose data, of whatsoever kind, would be processed, or rights would be affected, at the occasion of, or for each of the purposes of this AT&T MIPS service, including the latter's activities performed by AT&T or the Customer as described in this Service Guide or the Agreement.

- For pursuing any other purpose, not mentioned under this Service Guide or Agreement, the Customer acknowledges to be solely responsible for such purposes and warrants to act in accordance with applicable laws.
- **SLO – Service Level Objectives:**
In the event the SLOs are not met, Customer and Vendor will work together to identify solutions. In the event of ongoing noncompliance with the stated SLOs, Customer and Vendor will work together to develop and implement corrective action plans to ensure compliance.
- **AT&T Managed IDS/IPS – Mean Time to Implement MACD Orders SLO**
The performance objective for Managed IDS/IPS Service – Mean Time to Implement MACD Orders SLA is that on average during a month AT&T will complete the stated percentage of MACD orders within the time frame in the Managed IDS/IPS Mean Time to Implement MADC Orders Performance Objective Table.

Managed IDS/IPS - Mean Time to Implement MACD Orders Performance Objective Table	
	Performance Objective
Mean Time to Implement MACD Orders within next Business Day	99.0%

- **AT&T Managed IDS/IPS - Mean Time to Notify – Incident Notification SLO**
The performance objective for Managed IDS/IPS Mean Time to Notify SLO is that that on average during a month AT&T will provide notice to the Customer of an “auto-detect” Trouble Ticket within the time indicated in the Managed IDS/IPS Time to Notify Performance Objective Table.

Managed IDS/IPS - Time to Notify Performance Objective Table	
	Performance Objective
Time in which AT&T will provide notice to Customer of an “auto-detect” Trouble Ticket within 15 minutes of Trouble Ticket generation for Medium Alerts via email; Critical/High Alerts via generated telephone call	90.0%



- AT&T Managed IDS/IPS–Customer Help Desk Support – AT&T Security Operations Center Availability SLO**
 AT&T Security Help Desk is available 7X24X365. All problems, questions or requests for assistance related to the Managed IDS/IPS should be made to the designated AT&T Security Help desk support. Problems may be reported by telephone or electronically, where available as specified by AT&T.

Managed IDS/IPS – AT&T Security Operations Center Time to Answer Customer generated telephone call - Performance Objective Table	
	Performance Objective
Time in which AT&T Security Help Desk will answer a customer generated telephone call within 30 seconds	99.0%

2. Project Governance

a. Change Control Process

- (a) AT&T and the Customer will manage all changes to this SOW through a written change request process (“Change Control Process”). AT&T manages changes that have cost or schedule impact as contractual changes through a disciplined contracting process.
- (b) Either Party must submit change requests to contractual documents in writing via Appendix B to this SOW.
- (c) The party requesting the change must submit a written request to the other party and the receiving party shall issue a written response within five (5) business days of the receipt of the request, including whether the receiving party accepts or rejects the request and/or any changes to the Terms and Conditions.
- (d) Once agreed upon, both parties must execute the document in Appendix B.

3. Schedule of Fees

See section 5 of Appendix C to DIR Contract No. DIR-SDD-18601 above.

3.1 ADDITIONAL PRICING TERMS AND CONDITIONS

- (a) Fixed pricing is based on the currently defined Scope of Work. Any additions or changes to this Scope of Work will necessitate changes in pricing. It is also assumed that no project delays occur that would require AT&T to stop work. AT&T will not be held financially responsible for project delays outside of its control.
- (b) AT&T MIDPS Supported Access Methods:
 - 1. AT&T Internet access or Internet access provided by an alternate Internet provider
 - 2. Any IPS/IDS sensors located at a Customer location or within an Internet Data Center must be Internet routable to allow management access to the S/NOC
 - 3. IPS/IDS sensors must be placed behind a screening device (i.e., Firewall, etc.).
- (c) Locations: All Services described in this SOW will be provided within the Contiguous United States (excludes Alaska and Hawaii). All pricing is in U.S. dollars (“USD”).
- (d) Two (2) US location in Austin, TX and San Angelo, TX



4. Engagement Assumptions

This SOW, including but not limited to the pricing and charges, is based on the following assumptions. If any of these assumptions are found to be inaccurate or invalid, AT&T shall provide Customer with the changes to the scope, tasks, deliverables or terms and conditions of this SOW via the Change Control Process detailed herein.

- (a) The Project Scope is based upon the activities and services listed in this SOW and are valid for sixty (60) days from the date of this document.
- (b) All of the work will be performed in the Contiguous United States (excludes Hawaii and Alaska).
- (c) AT&T shall endeavor to arrange that all information presently known to be necessary for the performance of services as stated in the SOW has been disclosed or provided to the AT&T engagement personnel and shall provide information reasonably requested by them.
- (d) Customer takes full responsibility for the accuracy of all information supplied to AT&T by Customer representatives and which AT&T relies upon in the performance of this Agreement.
- (e) AT&T will document and review specific requirements provided to the Customer and will require final approval by the Customer SPOC prior to starting any work under this SOW.
- (f) Customer will coordinate the project kick-off with the designated AT&T's SPOC, for meeting schedules and confirm all required attendees are present as required.
- (g) During the engagement, AT&T may require ad-hoc access to Customer personnel who participated in the meetings. This ongoing access will allow resolution of any questions or issues as they arise.
- (h) Specific information for individual business units or other groups may be reviewed and additional charges will be applied via the Change Control Process for unique complex areas determined outside of the scope of this SOW.
- (i) All changes or amendments to this SOW will be mutually agreed to in writing per the Change Control Process and signed by the authorized representatives of both parties upon final presentation. AT&T will not perform any out of scope changes without prior written authorization and approval from the Customer authorized contact.

[THE BALANCE OF THIS PAGE INTENTIONALLY LEFT BLANK]



APPENDIX A: EQUIPMENT LIST

Item	Customer Requirement
Existing Customer Deployed McAfee MX-8000XC IPS Devices	Provide Managed Intrusion Prevention/Detection Services within the network to support an initial configuration for 28 state agency end customers

<p>Additional Assumptions:</p> <ul style="list-style-type: none"> ○ MIDS Level 3 service ○ AT&T will support the service with the Atos NSP locally on site at State Data Center(s) ○ Atos will purchase and deploy local tools/server(s) within the appropriate State Data Center location(s) to accommodate custom AT&T support of the MIDS Level III analysis service as required Atos will own the Clustering configuration on the 8000XC and 240-XC ○ Atos will manage the CPE (8000XC and 240XC) ○ Atos will manage the onsite NSP ○ Once the 8000XC's have been turned over to AT&T for management, AT&T will own the IPS policy configuration <ul style="list-style-type: none"> ▪ All configuration changes on the 8000XC sensor and IPS policy will need to be requested to AT&T as a MACD ○ 8000XC sensor will be deployed with sub-interface VLAN policy for agency separation <ul style="list-style-type: none"> ▪ This scope is based on 28 total agencies ▪ Additional scope will incur cost appropriately
--



APPENDIX B: SAMPLE CHANGE REQUEST FORM

Type of Request:	
Initiator (Company):	
Change Request Received by:	
Price Impact:	
AT&T Additional Resources Req'd:	

Task Description:

Other information related to Change:

Impact of Change
Provide a description of the impact of the change (increase in duration, delay in start, cut-over date change, added dependency, additional resources required change to design, change to baseline solution, other).

AGREED and ACCEPTED:
CUSTOMER: Department of Information Resources

AGREED and ACCEPTED:
AT&T

By: _____
 (Authorized Agent or Representative)

By: _____
 (Authorized Agent or Representative)

Sally Ward _____

 (Typed or Printed Name)

Director of Data Center Services _____

 (Title)

 (Date)

 (Date)