



Appendix C to DIR Contract No. DIR-SDD-779

SERVICE AGREEMENT NO SS-003-2011

THIS SERVICE AGREEMENT NO. SS-003-2011 (the "Service Agreement") is made and entered into this day of August, 2011, between State of Texas Department of Information Resources, ("Customer"), and AT&T Corp. ("Vendor" or "AT&T").

Customer and Vendor hereby agree that Managed Security Services - Security Operations Center shall be provided subject to the following terms and conditions:

1) This Service Agreement by reference incorporates all of the terms of the agreement entered into between the State of Texas Department of Information Resources ("DIR") and AT&T on [DIR Contract No. DIR-SDD-779] ("Contract"). Customer and AT&T agree that: (i) 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").

2) Standard terms for specified Services. The prices and other applicable terms and conditions regarding Managed Security Services / Security Operations Center shall be identified in Attachment B, Scope of Work and Attachment C, Pricing Schedule.

3) Customer specific terms.

AT&T performance of Managed Security Services / Security Operations Center for DIR under this Service Agreement shall be effective as of September 1, 2011, for a term through August 31, 2016 and for such additional term of service to which the parties may agree.

4) Overview of Documents. The terms and conditions governing the Services that AT&T provides to Customer are set forth in the Statement of Work, additional documents, and any other documents executed by the parties and referencing this Service Agreement (which documents together with this Service Agreement are called "this Agreement").

(a) Pricing Schedules. A Pricing Schedule (Attachment A herein), attached to and a part of a Service Agreement, which identifies the Services AT&T may provide to Customer, the price (including discounts, if applicable) for each Service, and the term during which such prices are in effect ("Pricing Schedule Term"). Pricing shall be in accordance with Section 4.B. of the Agreement.

(b) Prepayment of Services. For purposes of the Managed Security Services SOW, AT&T is providing a substantial discount in actual costs of performance in exchange for the prepayment of services which, by saving important and scarce State operating dollars for other needs of the telecommunications system, is a legitimate public purpose and is authorized by Section 2.52 of the State of Texas Procurement Manual.



5) Order of Precedence. In the event of a conflict between this Agreement (including Pricing Schedules, AUP, Service Guides) and the DIR Contract No. DIR-SDD-779, the DIR Contract controls. The Order of Precedence for all documents shall be the DIR Contract No. DIR-SDD-779, Appendix A, Standard Terms and Conditions for Services Contracts; Appendix B, Vendor's Historically Underutilized Businesses Subcontracting Plan; Appendix C, Service Agreement (including Pricing Schedules, AUP, and Service Guides); Exhibit 1, Vendor's Response to RFO DIR-SDD-TMP 091, including all addenda; and Exhibit 2, RFO DIR-SDD-TMP 091, including all addenda. In the event of a conflict within Appendix C the order of precedence shall be Pricing Schedules, AUP, Service Guides, and then the Appendix C Agreement.

6) Revisions to Documents. Subject to Section 8.B.7) (d) (Materially Adverse Change) of the Contract, AT&T may revise Service Guides or the AUP (collectively "Service Publications") at any time.

7) Execution by AT&T Affiliates. An AT&T Affiliate may sign a Pricing Schedule referencing this Service Agreement in its own name and such Affiliate contract will be a separate, but associated, contract incorporating the terms of this Agreement with respect to that Pricing Schedule. AT&T will arrange to its Affiliates comply with this Agreement, regardless of whether an Affiliate has signed a Pricing Schedule.

IN WITNESS WHEREOF the Parties have executed this Service Agreement as of the date of the last signature.

DEPARTMENT OF INFORMATION RESOURCES

AT&T Corp

By: [Signature]

By: [Signature]

Name: Karen Robinson

Name: GABRIELA RATULOWSKI
Contract Management

Title: Executive Director

Title: _____

Date: 8/22/11

Date: 8/17/11

Legal: [Signature]
8/22/11



ATTACHMENT A
TERMS AND CONDITIONS

Terms and Conditions for AT&T SOC SERVICES SOW under DIR - SDD - 779.

Notwithstanding any provisions of DIR - SDD - 779 to the contrary, AT&T Corporation (Vendor) and the Department of Information Resources (DIR) agree that the following terms and conditions shall govern the delivery of Security Operations Center Services (SOC Services) pursuant to that certain Statement Of Work (SOW) No. SS-003-2011, dated 9/1/2011, issued pursuant to DIR - SDD - 779. In the event of conflict between the terms of the SOC Services SOW and DIR - SDD - 779, the terms of the SOC Services SOW shall take precedence. The parties intend to amend the provisions of DIR - SDD - 779 solely for the purposes of the delivery of the SOC Services SOW Attachment B.

Intending to be legally bound, Vendor and DIR agree to the following terms:

1. That the SOC Services SOW shall be delivered and administered in accordance with DIR - SDD - 779, as amended, except to the extent its terms are modified herein.
2. That Appendix A, Section 3 B, of DIR - SDD - 779, as amended in paragraph 8 B of the front end Contract to DIR - SDD - 779, does not apply to the SOC Services SOW.
3. That Appendix A, Section 8.B.5 of DIR - SDD - 779, Customer Rights Under Termination, is hereby amended and replaced in its entirety as follows:

"In the event the Contract expires or is terminated for any reason, a Customer shall retain its rights under the Contract and the Purchase Order issued with respect to all services ordered and accepted prior to the effective termination date. All Purchase Orders issued after expiration of the Contract shall be deemed Amendments to the SOW, such that those Purchase Orders shall run contemporaneous with the SOW."

4. That Appendix A, Section 7 A, 2) of DIR - SDD - 779, as amended in paragraph 8 D of the front end Contract to DIR - SDD - 779, is hereby amended in its entirety for the SOC SERVICES SOW Attachment B to read as follows:

Vendor shall indemnify and hold harmless the State of Texas and Customers, AND/OR THEIR OFFICERS, AGENTS, EMPLOYEES, REPRESENTATIVES, CONTRACTORS, AND/OR PERMITTED ASSIGNEES, FROM ANY AND ALL LIABILITY, ACTIONS, CLAIMS, DEMANDS, OR SUITS, AND ALL RELATED REASONABLE COSTS, ATTORNEY FEES, AND EXPENSES 1) for bodily injury (including death) or physical damage to tangible or real property, and 2) for unauthorized access to DIR or Customer information due to failure to protect such information in accordance with the SOC Services SOW to the extent directly arising out of, or resulting from any negligent acts or omissions



or willful misconduct of the Vendor or its agents, employees or subcontractors, in the execution or performance of the Contract and SOC SERVICES SOW and any Purchase Orders issued under the Contract and SOC SERVICES SOW. VENDOR SHALL PAY ALL COSTS OF DEFENSE INCLUDING ATTORNEYS FEES. THE DEFENSE SHALL BE COORDINATED BY THE OFFICE OF THE ATTORNEY GENERAL FOR TEXAS STATE AGENCIES AND BY CUSTOMER'S LEGAL COUNSEL FOR NON-STATE AGENCY CUSTOMERS.

5. That Appendix A, Section 7 A, 3) of DIR - SDD - 779, as amended in paragraph 8 E of the front end Contract to DIR - SDD - 779, is hereby amended in its entirety for the SOC SERVICES SOW Attachment B to read as follows:

a) Vendor shall indemnify and hold harmless the State of Texas and Customers, AND/OR THEIR EMPLOYEES, AGENTS, REPRESENTATIVES, CONTRACTORS, AND PERMITTED ASSIGNEES from any and all third party claims involving infringement of United States patents, copyrights, trade and service marks, and any other intellectual or intangible property rights in connection with the PERFORMANCES OR ACTIONS OF VENDOR PURSUANT TO THE SOC SERVICES SOW and the CONTRACT, but not in circumstances where the claimed infringement arises out of or results from (a) Customer's, its Affiliates or a User's content; (b) modifications to the Service by Customer, its Affiliates or third parties; or combination of the Service with any services or products not provided by AT&T; or (c) use of the Service in violation of the CONTRACT and SOC SERVICES SOW. VENDOR AND THE CUSTOMER AGREE TO FURNISH TIMELY WRITTEN NOTICE TO EACH OTHER OF ANY SUCH CLAIM. VENDOR SHALL BE LIABLE TO PAY ALL REASONABLE COSTS OF DEFENSE INCLUDING ATTORNEYS' FEES FOR STATE AGENCY CUSTOMERS. THE DEFENSE SHALL BE COORDINATED BY THE OFFICE OF THE ATTORNEY GENERAL FOR TEXAS STATE AGENCY CUSTOMERS AND TO THE EXTENT ALLOWED BY LAW, BY VENDOR'S LEGAL COUNSEL FOR NON-STATE AGENCY CUSTOMERS.

b) If Vendor becomes aware of an actual or potential claim, or Customer provides Vendor with notice of an actual or potential claim, Vendor may (or in the case of an injunction against Customer, shall), at Vendor's sole option and expense (i) procure for the Customer the right to continue to use the affected portion of the product or service; or (ii) modify or replace the affected portion of the product or service with functionally equivalent or superior product or service so that Customer's use is non-infringing. If neither option (i) nor (ii) are reasonably available, Vendor shall provide DIR with prompt written notice and the parties shall agree on how to revise the SOC SERVICES SOW to accommodate the change in the Service, including, but not limited to, amendment of the SOC SERVICES SOW and termination of the affected service.

6. That Appendix A, Section 7 K of DIR - SDD - 779, as amended in paragraph 8 I of the front end Contract to DIR - SDD - 779, is hereby amended in its entirety for the SOC SERVICES SOW Attachment B to read as follows:

1) EXCEPT AS SET FORTH IN SECTIONS 7.A.2 AND 7.A.3, AT&T'S ENTIRE LIABILITY, AND CUSTOMER'S EXCLUSIVE REMEDY, FOR DAMAGES ARISING OUT OF MISTAKES, OMISSIONS, INTERRUPTIONS, DELAYS, ERRORS OR DEFECTS IN THE SERVICES, AND NOT CAUSED BY CUSTOMER'S NEGLIGENCE,



SHALL IN NO EVENT EXCEED THE APPLICABLE CREDITS SPECIFIED IN THE SERVICE LEVEL AGREEMENTS ASSOCIATED WITH THE SOC SERVICES SOW.

2) SECTION 1) WILL NOT APPLY TO:

- a) BODILY INJURY, DEATH, OR DAMAGE TO REAL OR TANGIBLE PROPERTY OR FOR ANY SUCH CLAIMS DERIVING FROM UNAUTHORIZED ACCESS TO DIR OR CUSTOMER INFORMATION DUE TO FAILURE TO PROTECT SUCH INFORMATION IN ACCORDANCE WITH THE SOC SERVICES SOW DIRECTLY CAUSED BY AT&T'S NEGLIGENCE UNDER APPENDIX A, SECTION 7.A.2;
- b) BREACH OF APPENDIX A, SECTION 7.H (Confidentiality), OR APPENDIX A, SECTIONS 4.C and 4.D (DIR Logo and Vendor Logo);
- c) SETTLEMENT, DEFENSE OR PAYMENT OBLIGATIONS UNDER APPENDIX A, SECTION 7.A.3) (Infringements); OR
- d) DAMAGES ARISING FROM AT&T'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

3) NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR SPECIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, ADVANTAGE, SAVINGS OR REVENUES, OR INCREASED COST OF OPERATIONS.

7. That Appendix A, Section 7. C, as amended in paragraph 8.J. of the front end Contract DIR-SDD-779, is hereby renamed Warranties, and amended in its entirety for the SOC SOW Attachment B to read as follows:

O. Warranties. AT&T WARRANTS THAT IT WILL PERFORM THE SOC SERVICES SOW IN A GOOD AND WORKMANLIKE MANNER. AT&T MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, AND SPECIFICALLY DISCLAIMS ANY OTHER REPRESENTATIONS OR WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, OR ANY WARRANTY ARISING BY USAGE OF TRADE OR COURSE OF DEALING.

8. That Appendix A, Section 7 P of DIR - SDD - 779, as amended in paragraph 8.K. of the front end Contract to DIR - SDD - 779, is hereby amended in its entirety for the SOC SOW Attachment B to read as follows:

AT&T WILL NOT BE LIABLE FOR ANY DAMAGES, EXCEPT TO THE EXTENT CAUSED BY AT&T'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, ARISING OUT OF OR RELATING TO: INTEROPERABILITY, ACCESS OR INTERCONNECTION OF THE SERVICES WITH APPLICATIONS, EQUIPMENT, SERVICES, CONTENT, OR NETWORKS PROVIDED BY CUSTOMER OR THIRD PARTIES, SERVICE DEFECTS, SERVICE LEVELS, DELAYS, OR INTERRUPTIONS



(EXCEPT FOR LIABILITY FOR SUCH EXPLICITLY SET FORTH IN THE SOC SERVICES SOW AND THE AGREEMENT OR SERVICE AGREEMENT) FAILURE TO CORRECTLY ROUTE OR COMPLETE CALLS OR OTHER TRANSMISSIONS (INCLUDING 911 CALLS), OR LOST OR ALTERED MESSAGES OR TRANSMISSIONS.

9. The parties agree that Appendix A, Section 7.J, Background and/or Criminal History Investigation, shall apply to all Vendor employees assigned to deliver the SOC SERVICES SOW, originally and as the employees may change over time. In the event an employee fails to pass the background check customer may notify vendor and vendor must remedy the situation within a reasonable time period, any failure to do so shall be grounds for customer to terminate its purchase order and related service agreement. AT&T will notify DIR in a timely manner prior to removal or change in personnel so that the investigations may be conducted without adversely affecting ongoing operations under the SOC SERVICES SOW.

10. That Appendix A, Section 8.B.7, as amended in the front end Contract DIR - SDD - 779 at Section 8 P., does not apply to the SOC SERVICES SOW; however the following additional suspension and termination of Services provisions apply to such SOC SERVICES SOW:

a) **Misuse or Abuse.** If AT&T suspects misuse or abuse of services provided under the SOC SERVICES SOW, AT&T may terminate or suspend an affected Service by providing DIR with thirty (30) days advance written notice.

b) **Definition of Misuse or Abuse.** The misuse or abuse of, or the intended or attempted misuse or abuse of, services provided under the SOC SERVICES SOW is prohibited. The following activities constitute misuse or abuse: (i) Using Services provided under the SOC SERVICES SOW to transmit a message, locate a person, or otherwise give or obtain information, without payment for the service, (ii) Using or attempting to use services provided under the SOC SERVICES SOW with the intent to avoid the payment, either in whole or in part, of the charges for the services provided under the SOC SERVICES SOW by: (1) Rearranging, tampering with, or making connections not authorized by the SOC SERVICES SOW to any service components used to furnish services under the SOC SERVICES SOW, or (2) Using any unauthorized means or devices, tricks, schemes, false or invalid numbers, false credit devices, or electronic devices to gain access to or use the services provided under the SOC SERVICES SOW.

11. That Appendix A Section 8.B, Termination Charges, of DIR - SDD - 779, as amended in paragraph 8 R of the front end Contract to DIR - SDD - 779, is hereby amended in its entirety for the SOC SERVICES SOW Attachment B to read as follows:

If, on or after Customer's obligation to pay for Services rendered under the SOC SERVICES SOW begins, Customer terminates a Purchase Order or Service Agreement for convenience or Vendor terminates a Purchase Order or Service Agreement for Customer's misuse or abuse, Customer's hazardous materials violations, or Customer's material breach, Customer will pay termination charges as follows:



If termination occurs before the end of the term of the SOC SERVICES SOW Service Agreement, then Customer's termination liability shall be 50% of the monthly recurring charges for the terminated Service or Service Component multiplied by the months remaining in the term, not to exceed \$1,250,000.



Attachment B
STATE OF TEXAS DIR-AT&T

STATEMENT OF WORK
SECURITY OPERATIONS CENTER
SOC SERVICES / Dated 9/1/2011

I. Current Operations

- A. Under the current DIR Network and Security Operations Center (NSOC) operations environment DIR and AT&T have contracted to implement the NSOC that provides a synergistic Network and Security services model. The DIR NSOC offers a managed services solutions model that includes management, monitoring and provisioning of DIR's Internet Gateway multi-ISP model network, Internet facing security infrastructure (Intrusion Prevention Services/Intrusion Detection Services (IPS/IDS), Firewall services), IP Services Gateway (ISG) MPLS network, a full-service Controlled Penetration Testing/Vulnerability Assessment program and SIEM Correlation with Security Analysis services. Additionally, the NSOC operations center is responsible for monitoring external network security events (as described in Texas Government Code (TGC) § 2059) for State of Texas Agencies and other eligible entities as defined by TGC § 2059.
- B. Network and Security tools currently utilized inside the NSOC serve to provide operational views, critical status, trouble ticket tracking and information metrics to both engineers and managers within the DIR NSOC. It is understood that specific operational views, critical status, trouble ticket tracking and information metrics may be presented to State of Texas agencies and other AT&T management entities outside of the NSOC. The NSOC has adopted the ITIL standards for all process methods and workflows administration. [REDACTED]
- [REDACTED] Virtual network accessibility and presentation server capabilities supports technical and managerial access and ensures communication continuity across AT&T functions at the NSOC. Performance data for both network and security functions is provided by standards-based Network Management Systems (NMS), Security Information Event Management (SIEM) platform and other Operations Support Systems (OSS) platforms. Additionally NSOC provides individual customer report capability via a SIEM portal for discrete Agency monitoring of their external facing Internet security infrastructure (Firewalls, IDS/IPS, other security appliances).



II. Proposed Operations

NOTE: All forms of network security data and/or information provided in response to this SOW will be classified and handled as Confidential as required by section 2069.055 Texas Government Code (TGC) and section 552.139 Texas Business and Commerce Code (TB&CC). Additionally, as required by section 2059.055 TGC, AT&T shall only release confidential network security data and/or information to officials responsible for the network, law enforcement officials, the state auditor's office and agency or elected officials designated by DIR.

- A. Since the term of the current TEX-AN agreement expires in August of 2011, AT&T proposes an expanded Security Operations Services offering and agreement utilizing this Scope of Work for a period of five (5) years beginning from time of contract signature or unless otherwise specified.
- B. AT&T will provide all new and existing SOC management services for DIR under this Statement of Work which shall be appended to the DIR-AT&T Security Services agreement Contract No. DIR-SDD-77.9
- C. AT&T agrees to continue to provide specified security operations services to assist the State throughout the duration of this Statement of Work ("SOW"). Additionally, as a part of this SOW, AT&T will migrate from the existing netForensics SIMOne platform to the cloud-based AT&T SETA (Security Event Threat Analysis) platform, which offers increased performance, scalability and features not found in the existing netForensics SIMOne platform. AT&T will furnish the State with performance-based SLAs for AT&T's SETA service.
 - (1) Additionally, AT&T will continue to manage and monitor the two existing State of Texas DIR ISP Gateway IPS devices. Such services will be provided pursuant to this SOW.
- D. Under this SOW AT&T will augment existing AT&T NSOC Help Desk services combining current DIR NSOC Operations Help Desk functions into a new integrated 7X24X365 SOC Help Desk Support model.
- E. Work specific identified strategic asset(s) as listed in Attachment XX to this Appendix C are provided and utilized by AT&T NSOC and located on State of Texas premises. These AT&T assets have been deployed and utilized in providing network and security services for DIR and can convey to the State at a cost of \$1 dollar at the conclusion of the agreement. For the duration of this new agreement AT&T will continue to have use of these existing assets currently utilized by AT&T NSOC to provide network and security services. Should DIR exercise right of conveyance at termination of this agreement, any associated vendor provided hardware and software licensing and/or maintenance associated with conveyed NSOC assets will terminate at the conclusion of this contract and not convey.
- F. DIR's primary role will be to govern and manage the delivery of ongoing SOC services in an arrangement where:

NSOC



- (i) AT&T is responsible for delivering services to the State's eligible customers as defined under the scope of services stated in this agreement. These ongoing services shall be delivered in accordance with documented Service Level Agreements (SLA) as is stated in this contract.
- (ii) AT&T shall continue to employ dedicated SOC resources to be housed on State property in the State NSOC.
- (iii) AT&T shall also employ resources at other AT&T management center back-up facilities. These sites will serve as back-up management capability for Business Continuity and Disaster Recovery functions supporting the State NSOC.



III. Security Operations Center – SOC Scope

- A. Continue to provide 7x24x365 management and monitoring of current Internet Gateway IPS devices.
- B. Provide security management, monitoring and maintenance of IDSM-2 modules utilized to protect the HHSC-N. These modules are installed in the ISG-WAN routers and currently owned by AT&T. This service is contingent on AT&T managing the ISG routers via an AT&T Network Operations Center (NOC).
- C. Evaluate a new security architecture to replace the IDSM-2 functionality in the existing ISG-WAN routers as HHSC-N customers migrate. Final design will be subject to AT&T and DIRT approval, with any required equipment and associated managed security service provided as an ICB under a separate addendum.
- D. Maintain all vendor maintenance contracts that pertain to the NSA, Internet Gateway IPS devices, and associated equipment.
- E. Provide an NSOC security monitoring service with AT&T's Internet Protect alerts and other critical security information to DIRT and State of Texas Agency ISCs via the DIR portal.
- F. Migrate from the existing netForensics SIMOne platform to the cloud-based AT&T SETA (Security Event Threat Analysis) platform, which offers increased performance, scalability and features not found in the existing netForensics SIMOne platform. The SETA platform has 90 days of raw security log storage and one year of historical archive storage. There is no limit to the numbers of events per second with the AT&T SETA platform, and SETA can be implemented in phases upon mutual agreement by both parties.
- G. Provide 7x24x365 security alerts and analysis of information received via AT&T SETA, as well as other in-scope sources/devices (such as the NSA).
[REDACTED]
- H. Provide support to DIRT on an as-needed basis for security matters and incident response (CSIRT) in support of State Agencies and Customers. AT&T response capabilities include network engineering, security engineering, security analysis, and in-scope project management. To shorten incident response times and effectuate faster remediation capability AT&T will utilize both Network and Security engineers in a synergistic fashion to mitigate incidents. Network engineering resources are contingent on AT&T managing the ISG routers and Internet Gateway routers via an AT&T Network Operations Center services agreement.
- I. Provide monthly performance (i.e. metrics, numbers of critical events, etc.) and SLA reports for all AT&T SOC-managed security devices and associated equipment per the SLA guidelines listed below.
- J. Modify existing GPT program to provide 48 controlled penetration test (CPT) engagements per fiscal year (averaging 4 per month for each fiscal year). Completing



more than 4 scheduled CPT engagements per month will be conducted by AT&T on a best effort basis.

- K. Standard tools utilized as part of the penetration testing are those that have historically been available to AT&T CPT personnel or those provided by DIR at no cost to AT&T during FY 2011 under the Eighteenth Amendment of SBC Contract # TEXAN2000 - SBC - MA1. These standard tools have included ISS Internet Scanner (no longer in use), NMap, Nessus, Core Impact (no longer in use), and Rational AppScan. Other tools that DIR may specify that require additional costs for software, licensing, AT&T personnel or training may require a change order if deemed necessary by AT&T.
- L. AT&T will utilize the existing DIR-owned and DIR-maintained tool (Critical Watch) for performing Vulnerability Assessments, and will perform an external vulnerability assessment as part of each CPT engagement. Additional external vulnerability assessments may be performed based on State Agency and/or DIR requirements, depending on availability of appropriate resources.
- M. Assistance will be provided by AT&T to State Agencies that have had a Controlled Penetration Test performed to remediate the vulnerabilities discovered. Such assistance will be provided after testing activities have concluded, and will be limited in duration to 1800 hours per fiscal year. Remediation activities will encompass remediation recommendations, suggested methods of remediation, and post-remediation testing. All remediation activities are assumed to take place via email, conference call or on-site in the Greater Austin Texas area. A defined Scope of Work will be co-developed by AT&T and DIR for each remediation engagement with each State Agency.
- N. In order to insure technology refresh and address any new DIR requirement to provide enhanced security, additional equipment, hardware, software and related managed services may be proposed and implemented at any time upon mutual agreement and subsequent addendum between AT&T and DIR. Any additional security services provided by AT&T will be considered on an Individual Case Basis (ICB). AT&T reserves the right to modify any hardware, software, associated equipment and related services pending further testing and/or upon mutual agreement with DIR.
- O. AT&T will provide DIR security recommendations at least once a year, in order to address new security technologies, security issues, or compliance requirements.
- P. All existing and new equipment provided by AT&T will be installed and maintained by AT&T.
- Q. AT&T, in cooperation with DIR, has designed and engineered a Next Generation Security Architecture (NGSA) for DIR's Enterprise customer networks, AMAN, ESSMN, and ISG networks.
- R. Implementation of any portion of the NGSA phases as outlined below will be contingent upon the completion of an additional mutual contract agreement or addendum between DIR and AT&T:

(1) Phase 1 - Internet Gateways

1. Implement and manage NGSA integrated security analysis and decoding appliances. Estimated time to implement is no later than 90 days from new equipment delivery.

2. Implement and manage NGSA content analysis security appliances. Estimated time to implement is no later than 90 days from new equipment delivery.
3. Implement and manage NGSA Malware Detection System devices. Estimated time to implement is no later than 90 days from new equipment delivery.
4. Modifications to the architecture, associated equipment and related services may be presented to DIR upon further testing and/or upon mutual agreement with DIR.
5. SLAs specific to NGSA devices will be developed and presented to DIR within 90 days of equipment implementation.

(2) Phase 2 – ESSMN/AMAN – To Be Determined

1. Implement and manage NGSA IPS appliances (2 located off of the [redacted] router and 2 located off of the [redacted] router to protect the network interconnects to the AMAN; 2 located on the network interconnects between the Area 6 (ISG) and Area 61 (ESSMN) routers; and 2 located on the network interconnects to be added between Area 61 (ESSMN) routers and the Pebble and Augusta routers. Estimated time to implement is no later than 90 days from new equipment delivery.
2. Implement and manage NGSA content analysis security appliances (2 located off of the [redacted] routers; and 2 located off of the links between the Area 6 (ISG) and Area 61 (ESSMN) routers). Estimated time to implement is no later than 90 days from new equipment delivery.

(3) Phase 3 – To Be Determined

1. Phase 3 involves long-term planning and architecture design work. For this phase, based on DIR requirements, AT&T can design and implement security technologies on both the AMAN and ISG networks for inter- and intra-agency traffic. Due to the complexity of the networks involved, at this time it is difficult to determine which security technologies will be appropriate and useful for the State. Any additional security technologies that might be implemented on the AMAN and ISG networks could require extensive network engineering changes.

IV. AT&T Roles and Responsibilities:

- A. Management and Monitoring of NGSA Security Devices - AT&T will provide all services within this SOW associated with AT&T provided NGSA security devices, software,

hardware and their respective maintenance to deliver the services as required. AT&T will provide qualified and trained security engineers to fulfill this support.

- B. Management and Monitoring of Internet IPS Devices - AT&T will provide all services within this agreement associated with existing Internet IPS security devices, software, hardware and their respective maintenance to deliver the services as required. AT&T will provide qualified and trained security engineers to fulfill this support.
- C. Management and Monitoring of IDSM-2 Security Devices - AT&T will provide all services within this agreement associated with the existing IDSM-2 security devices (located within the ISG routers), software, hardware and their respective maintenance to deliver the services as required. AT&T will provide qualified and trained security engineers to fulfill this support.
- D. Management and Monitoring of the SETA platform - AT&T will provide all services within this SOW associated with the SETA platform, software, hardware and their respective maintenance to deliver the services as required. AT&T will provide qualified and trained security engineers to fulfill this support.
- E. DIR NSOC Security Engineering - AT&T will furnish qualified and trained Security Engineering personnel.
This service includes trouble ticket creation via DIR provided Trouble Ticket system; tracking, escalation and integrated trouble resolution; security device management, and security event escalation related to AT&T SETA and DIR Customers.
- F. Business Continuity and Disaster Recovery (BCDR) - AT&T will provide a backup SOC services capability for analysis of the SETA platform. This backup AT&T SOC services arrangement consists of a primary AT&T SOC in New Jersey and an alternate secondary AT&T SOC in Virginia.
- G. AT&T Personnel - AT&T will furnish qualified and trained AT&T personnel to successfully support SOC functions. All in-scope AT&T SOC personnel (including AT&T SETA security analysts) and third party AT&T vendors will successfully pass DIR documented background check processes, CJS background check processes and have physical access capability to all appropriate State of Texas facilities as required to fulfill and support all AT&T SOC SLAs.
- H. Compliance - In cooperation with DIR, all services delivered by AT&T will be in accordance with 1. Texas Administrative Code ("TAC") 202, and other designated Federal and State regulations.

V. DIR Responsibilities

- A. DIR will be responsible for providing AT&T personnel 7X24X365 physical work space at the DIR NSOC, including adequate furnishings to support security engineering functions; telecommunications voice/data infrastructure and access; sufficient rack space, power and cooling for all equipment located in State owned facilities; and a safe and secure working environment.
- B. To facilitate AT&T's support of Security Operations, DIR will provide AT&T personnel sufficient access and system permissions for trouble ticketing (i.e. BMC On-Demand Remedy), Network Management System(s) (i.e. CA and NOC Tools) and any other

monitored devices or systems in order to enable AT&T service fulfillment capabilities as specified in this agreement.

- C. DIF will maintain sufficient hardware and software maintenance for all ticketing systems, Network Management Systems, monitoring tools, AMAN, ESSMN, DNS equipment and other in-scope DIF owned and maintained equipment in order to enable AT&T service fulfillment capabilities as specified in this agreement.
- D. DIF will furnish AT&T updated escalation, incident/call treatment, contact lists, process procedures and other appropriate information in order to enable AT&T to provide required Security Operations fulfillment as specified in this agreement.
- E. DIF will provide AT&T a fully documented background check process that addresses physical access requirements to all appropriate State of Texas facilities in support of this SOW.
- F. DIF will maintain the Critical Watch hardware, software, licensing and maintenance, and all CPT-related hardware, software and licensing (except for Nessus and Burp Suite, which will be maintained by AT&T).
- G. DIF is responsible for complete program management of the CPT/Remediation program and the Security Event monitoring program (SETA) as relates to on boarding and scheduling of State Agency/ Political Subdivisions or customers. This includes establishing initial service participation with Agency/Political Subdivision, customer outreach/fulfillment, and DIF Inter-Agency contract management where applicable.

VI. Personnel

Tier 3 Security Engineer Candidate Description:

The Tier 3 Security Engineers have specialized in one or more vertical security technology disciplines, but will also be versed in other IT service delivery technologies supported by the NSOC. The Tier 3 Security Engineers perform testing, analysis and restoration of failed production services to customers and users. When new technologies and/or IT Services are added to the environment, the engineers are responsible for creating acceptance criteria and testing new service/technology supported by the NSOC. A primary function of this position is to monitor and sustain the SLAs (Service Level Agreements) as well as the growth and capacity planning aspects of the IT services.

NSOC Engineers are responsible for:

- Resolving service-impacting events/incidents.
- Escalating incidents to the NSOC Director.
- Engaging support of the CSIRT (Computer Security Incident Response Team) when necessary.

Responsibilities:

- Monitor ongoing operations and IT service infrastructure performance with applications set to anticipate IT service problems.
- Interpret console messages and perform required actions.
- Perform IT service problem isolation and determination.
- Initiate corrective action within scope of knowledge and authority.
- Assist with network / security troubleshooting.
- Implement network bypass/recovery/backup procedures as required.

- * Maintain knowledge of technology used by the NSOC, as well as new technologies that may be used by the NSOC in the future.
- * Create criteria for acceptance of IT services and/or managed elements, by NSOC, for proactive monitoring and management.
- * Validation of new IT services and/or managed elements in the IT environment.
- * Acceptance/coordination of new IT services and/or managed elements in the IT infrastructure.
- * Use and invoke network diagnostic tools.
- * Use and provide input to database(s) for problem and inventory control.
- * Perform testing and maintenance activities of the network, as required.
- * Serve as the customer interface for scheduling network changes, and the coordination of the Change Management process with the customer.

General Qualifying Experience and Attributes for all Tier 3 Security Engineers:

- * A minimum of three (3) to four (4) years of network management experience.
- * Expertise with network management functions, protocols, and standards.
- * Proficient in IT infrastructure technologies:
 - o Routers, Switches, WAN, LAN, VoIP, Telecomm, and other internetworking technologies.
- * Thorough understanding of TCP/IP—addressing, routing protocols and transport protocols (UDP and TCP).
- * Proficient in the use of network management tools, primarily for fault management purposes.
- * Complete understanding of escalation, incident management and change management processes and procedures of the NSOC.
- * Prior training in concepts of network and systems operations.
- * Understands network performance analysis and capacity planning best practices.
- * Thorough understanding of performance impact of network configuration options.
- * Proficient in the operation and use of management tool set including fault, configuration, performance and security tools.
- * Understanding of vendor and industry standards and procedures for their respective technical specialty.
- * Able to provide technical leadership to less experienced personnel either individually or as part of a team.
- * Possess good communication and interpersonal skills.

Specific Security Qualifying Experience and Attributes for Tier 3 Security Engineers:

- * CISSP (Certified Information Systems Security Professional) or CISA (Certified Information System Auditor) certifications are required.
- * CISM (Certified Information Security Manager) certification desired.
- * Cisco CCIE desired.
- * Extensive Network Intrusion Response and threat analysis experience required.
- * Significant Experience with Intrusion Prevention/Detection Systems (all 4 types preferred: host signature, host behavioral, network signature and network behavioral based).

- Significant experience in network-based Evidence Identification and Preservation.
- Experience with Zero-Day analysis, alerting, and virus consortium submission processes.
- Experience with industry-wide processes (FIRST, Storm Center, etc.).
- Experience with Law Enforcement Reporting (Computer Crime Units, USSS ECTF, FBI CCS, CAAT).
- Working knowledge of SIEM vendors, platforms and technology (netForensics, Intellifacets, Cisco MARS, etc.).
- Network and Host system troubleshooting experience.
- Knowledge of network protocols and experience analyzing network traffic with network sniffers (ethereal, netcat, etc.).
- Experience with IPS/IDS: TippingPoint, Cisco, Juniper, etc.
- Working knowledge of network-based threats (various malware attack strategies, common weaknesses, virus vs. worm, DoS & DDoS theory, network attacks such as land, teardrop, Back, Buffer Overflow, etc., back doors [back office, sub seven, netbus], common virus recognition).
- Intrusion Response experience in the form of day-to-day network traffic analysis and threat assessment/impact analysis.
- Possess some knowledge of one of the key areas of data communications (networks, servers and applications), telecommunications and the various interconnecting technologies.

Security Analyst Candidate Description:

Security Analysts are responsible for the day-to-day proactive security analysis. They interface with customers and engineering teams (as needed) to ensure expedient handling of potential security incidents. The primary role of the NSOC Security Analyst is to provide analysis of security events and incidents from multiple sources. They are responsible for proactive security monitoring and performing initial triage for incidents across all layers of the network/security architecture.

Responsibilities:

- Security analysis; watch for any events affecting the IT security infrastructure and proactively contact the Help Desk or Customer and initiate resolution.
- Monitor the security information management system screens for alarms indicating potential SLA (Service Level Agreement) violations, security issues and act proactively to avoid those incidents/violations.
- Perform regular IT security infrastructure surveillance by physically watching security information management system screens and reviewing reports.
- Ensure that all problems are logged by following the trouble ticket procedure.
- Prioritize problems.
- Respond to customer and vendor calls regarding faults.
- Perform problem tracking and initiate escalation procedures as required.
- Follow and understand the automated notification procedures to notify affected parties when problems are identified.
- Track resolution efforts to ensure achievement of SLA resolution.
- Inform customers/helpdesk of any problems or scheduled down times according to established notification guidelines and Change Management procedures.



- Perform additional tasks when NSOC activity is low, such as vulnerability assessment scanning, assisting controlled penetration testing analysts, generating management and technical reports and generating summaries of active problems/incidents.

Qualifying Experience and Attributes for all Security Analysts:

- Possess some knowledge of one of the key areas of data security (networks, servers and applications), telecommunications and the various internetworking technologies.
- CISSP desired.
- Security certification for net forensics desired.
- Understand networking protocols (TCP/IP, etc.) at an entry level.
- Possess basic UNIX and/or Windows NT/Win2K knowledge.
- Demonstrate eagerness to expand knowledge base and ability to learn quickly.
- React quickly to major/critical problems.
- Alert, intelligent, articulate and efficient.
- Possess good communication and interpersonal skills.
- Desire to provide the highest quality of service.
- Sensitive to customers' needs.

VII. SLAs

Uptime

The Service will be provided 24 hours a day, seven (7) days a week, with 99.9% uptime. The uptime guarantee includes all security devices & security management servers and their associated devices and applications owned by AT&T. The 99.9% uptime guarantee excludes any time that is accumulated while replacement hardware is being delivered, during hardware replacement activities, software upgrades, repair or other scheduled maintenance is being performed by AT&T or the manufacturer of the device in question.

Exceptions

The following list of standard exceptions applies to all SLAs. Additional exceptions may apply and are stated within each of the SLAs.

- Interruptions, degradations, deficiencies or delays caused by DIR/State Agency or a User.
- The failure or deficient performance of power, equipment, services or systems not provided by AT&T.
- Service interruptions, degradations, deficiencies, or delays during any period in which AT&T or its agents are not afforded access to the premises where access lines associated with the services are terminated.
- Service interruptions, degradations, deficiencies, or delays during any period when a Service Component is removed from service for maintenance or rearrangement purposes or for the implementation of a DIR/State Agency order.
- DIR/State Agency ejection not to release a Service Component for testing and/or repair and continued use of the Service Component.

- **Remedy Timestamps:** If the actual "closed/resolved" time is not captured due to lack of ability to enter data into Remedy, a comment will be entered into the ticket system to note both the correct or actual time of resolution (i.e. time a managed device was online and available and the fact that this constitutes a need for an exception review).
- **Force Majeure Conditions**

Service Level Summary:

| SERVICE LEVEL DETAIL | |
|-----------------------------|---|
| Objective | To ensure acceptable levels of continuous availability of security devices |
| Service Level | The aggregated total uptime all network security devices will be at least 99.9% of total available time within a month, measured on a per device scale. |
| Service Owner | ATT NSOC Director |
| Measurement Period | Monthly |
| Hours of Support | 7 x 24 x 365 |
| Data Capture | DIR ticketing system will record the uptime/downtime parameters. Trigger points are: <ul style="list-style-type: none"> • Downtime Begins - Failure Detection (timestamp in Remedy), either automatically generated by monitoring system or generated by opening of an incident ticket • Downtime Ends - Failure Resolution (timestamp in Remedy), the point at which the incident is resolved |
| Reports | Monthly report detailing the percentage of Uptime recorded. |
| Reporting Period | Calendar Month |
| Service Credit | \$1000 per device per month, not to exceed \$10,000 in any calendar month. |



Critical Event Notification

A Critical Security Event is defined as an event received in the SIEM and interpreted by a human or human designed rule as critical.

Within fifteen (15) minutes of verification of a security device failure or critical security event from a security device, AT&T will contact DIR/State Agency either by e-mail or telephone or both in accordance with DIR Policy.

Service Level Summary

| SERVICE LEVEL DETAIL | |
|---------------------------|---|
| Objective | To ensure acceptable levels of awareness and communications between AT&T and DIR/State Agency when major alarms are encountered. |
| Service Level | DIR/State Agency will be notified within 15 minutes of all security device failures or critical security events, on an average of 98% of incidents. |
| Service Owner | ATT NSOC Director |
| Measurement Period | Monthly |
| Hours of Support | 7 x 24 x 365. |
| Data Capture | DIR ticketing system will record the event detection time and time a notification was sent to customer. Trigger points are: <ul style="list-style-type: none">• Critical Event/Major Alarm Begins - Failure Detection (timestamp in Remedy, either automatically generated by monitoring system or generated by opening of an incident ticket).• Notification Sent - Time of notification to customer (timestamp in Remedy, the point at which the notification indicator is time stamped). |
| Reports | Monthly report detailing the average time of events when notification should have been sent. |
| Reporting Period | Calendar Month. |
| Service Credit | \$2000 in any one calendar month in which less than 98% of critical incidents are communicated to DIR within 15 minutes. |

**Mean-Time-To-Restore (MTTR)**

AT&T will provide engineering support and restoration attempts in case of security service failure. If needed, an AT&T engineer or manufacturer engineer may be dispatched to the site to complete the restoration.

Service Impacting:

AT&T guarantees that the mean time to restore (MTTR) after a security service failure will not exceed Four (4) hours from the time of trouble isolation.

The MTTR guarantee excludes any time that is accumulated while replacement hardware/software is being delivered, scheduled hardware/software software upgrades, engineer dispatch time or other scheduled maintenance is being performed by AT&T or the manufacturer of the device in question.

Service Level Summary

| Service Level Detail | |
|------------------------------|--|
| Objective | To ensure acceptable levels of responsiveness and resolution to security device failures |
| Service Level | Service Impacting Failures on production security services will be resolved within 4 hours of isolation on an average of 99% of incidents |
| Service Owner | ATT NSOC Director |
| Measurement Period | Monthly |
| Hours of Support | 7 x 24 x 365 |
| Time to Meet Metric | Effective for entire timetable defined in Scope |
| Additional Exceptions | In addition, MTTR calculations do not include time spent waiting for delivery of replacement hardware, software, or associated equipment. |
| Data Capture | DIR ticketing system (Remedy) will record the incident resolution steps. Trigger points are: Failure Notification + Service Impacting/Non-Impact Flag (timestamp in Remedy, either automatically generated by monitoring system or generated by opening of an incident ticket) Fault Isolation (timestamp in Remedy) Failure Resolution (timestamp in Remedy, the point at which the incident record is moved to resolved) |
| Reports | Monthly report detailing the percentage of service failure incidents that were resolved within 4 hours of isolation. |
| Service Credit | \$1000 per service element per month, not to exceed \$10,000 in any calendar month. |

Controlled Penetration Tests (CPTs)

AT&T will provide 48 CPTs per year

Scoping Assumptions

- The CPT program is scoped and priced based on an expectation that the CPTs being delivered are time-bound with an average not-to-exceed duration of three (3) weeks, and that reconnaissance activities only require the use of NMAP and Nessus (and/or Critical Watch).

Scheduling Assumptions

- AT&T expects DIR to schedule 4 CPTs per month, so that the CPT delivery team has a steady workflow of CPTs scheduled.
- The DIR Remedy ticketing system will be used to request, schedule, and report CPT tasks.
- DIR will provide complete CPT engagement details, including agency name, testing schedule, IP address range, and any special instructions at least four (4) weeks prior to the scheduled start date.

Delivery Assumptions

- DIR is responsible to ensure agency cooperation during testing.
- All CPT reports will be delivered based on the DIR approved report template.
- In addition to a completed CPT report, AT&T will provide DIR with the following:
 - Port scanning data from NMAP
 - Vulnerability scanning data from Nessus and/or Critical Watch (as determined by mutual agreement)
 - All screen captures and other work data obtained during CPT activities.

Service Level Summary

| SERVICE LEVEL DETAIL | |
|---------------------------|--|
| Objective | To ensure completion of Controlled Penetration Tests of State Agencies or other customers as agreed upon by AT&T and DIR. |
| Service Level | CPT reports for each test session will be delivered to appropriate DIR/State Agency contact |
| Service Owner | ATT NSOC Director |
| Measurement Period | Monthly |
| Hours of Support | 7 x 24 x 365 |
| Data Capture | DIR ticketing system will record the CPT task execution Proposed trigger points are: <ul style="list-style-type: none"> CPT Request Received -- individual CPT requests are entered into Remedy (timestamp) CPT Scheduled -- Individual CPT is scheduled per coordination with State Agency (timestamp) CPT Completed -- individual CPT has been completed (timestamp) |
| Reports | Monthly report detailing the number of requests received/scheduled/completed. |
| Service Credit | \$2000 in any one calendar month in which less than 4 CPTs are completed as scheduled within that calendar month. |

Managed Security Device Configuration Change Requests



As part of the SOC Service, security engineers will perform configuration changes on the security devices. Emergency, Standard (Urgent) and Standard (Normal) configuration changes are offered. Emergency configuration changes are handled within 15 minutes of approval to proceed on AT&T recommended changes. Standard (Urgent) configuration change requests will be taken on a 24 hours a day, seven days a week basis and initiated within ten (10) hours of receipt of request. Standard (Normal) configuration change requests are taken on a 24 hours a day, seven days a week basis and will be initiated within twenty-four (24) hours of receipt of request. When DIR/State Agency authentication is required or when AT&T determines that requested changes create potential security risk, AT&T will contact the appropriate DIR/State Agency representative.

NOTE: These Configuration changes will only be accepted from identified Security Contact personnel for DIR and/or State Agencies. Request for Change (RFC) for configuration changes will be entered in Remedy.

Definition of Priority and Standard Changes

Emergency Configuration Changes are any critical security event observed on a managed security device. This event will be monitored and DIR will be notified within 15 minutes. The appropriate required changes will be communicated to DIR upon completion.

Standard (Urgent) Configuration Changes normally carries a sense of urgency (such as opening a designated firewall port to allow out-of-the-ordinary incoming or outgoing customer traffic) and can be completed within 10 hours of receipt of the request.

Standard (Normal) Configuration Changes are not time-constrained and can be completed within 24 hours of receipt of the request.

Service Level Summary

| SERVICE LEVEL DETAIL | |
|------------------------------|---|
| Objective | To ensure acceptable levels of responsiveness and resolution to Security Device Changes |
| Service Level | Changes will be successfully implemented to the following parameters, on an average of 95% of all changes <ul style="list-style-type: none"> * Emergency Configuration Changes or Change Requests resulting from security incidents - Within 15 minutes of approval to proceed on recommended changes. * Standard (Urgent) Configuration Changes - Within 10 hours of receipt of RFC. * Standard (Normal) Configuration Changes - Within 24 hours of receipt of RFC. |
| Service Owner | ATT NSOC Director |
| Measurement Period | Monthly |
| Hours of Support | 7 x 24 x 365 |
| Additional Exceptions | Some RFCs (Request for Change) may, by design, have implementation times/dates specified. When a specific date or time is stated in an RFC that time will be used as the Start Time trigger. |
| Data Capture | AT&T ticketing system will record the incident and/or change resolution steps. Trigger points are: FOR INCIDENT RELATED CHANGES: <ul style="list-style-type: none"> * Event Detection (timestamp in Remedy, either |

| | |
|-----------------------|--|
| | <p>automatically generated by monitoring system or generated by opening of an Incident ticket)</p> <ul style="list-style-type: none"> Start Time: Solution Recommendation Approved by Customer (timestamp in Remedy) End Time: Solution Implementation (timestamp in Remedy) <p>NOTE: A Change Record may be created record the configuration change details after the Incident is resolved.</p> <p>FOR NON-INCIDENT RELATED CHANGES Standard (Urgent) and Standard (Normal) Changes:</p> <p>Approved or Pre-Approved Change Request received in Change Request system (Characterization of a Pre-Approved Change Request is a request that follows specific requirements and does not demand an Engineering Review in order to implement)</p> <ul style="list-style-type: none"> Start Time: Approved RFC by DIR/State Agency received (timestamp in Remedy) End Time: Change Request Closed (timestamp in Remedy) |
| Reports | Monthly report detailing the percentage of Change Implementations that were resolved within 15 minute, 2 hour, & 10 hour windows. |
| Service Credit | \$2000 in any one calendar month in which less than 95% of all changes in each category are implemented on time. |

SETA Log Feeds, Monitoring, and Analysis (LFMA) SLA

The performance objective for the SETA LFMA SLA is that the Log Feeds, Monitoring, and Analysis portion of SETA operations management will commence within 60 days after completion of the discovery phase and environment stabilization.

Service Level Summary

| SERVICE LEVEL DETAIL | |
|---------------------------|--|
| Objective | To ensure timely and acceptable levels of SETA operational readiness |
| Service Level | SETA Log Feeds, Monitoring and Analysis will commence within 60 days of discovery and environment stabilization. |
| Service Owner | ATT NSOC Director |
| Measurement Period | Monthly |
| Hours of Support | 7 x 24 x 365. |
| Data Capture | AT&T ticketing system will record the incident and/or change resolution steps that pertain to SETA LFMA enablement and operations. |
| Reports | Monthly report detailing the numbers of incidents and duration of each incident. |
| Service Credit | Credit equal to 1/30th of a single monthly charge for each day's delay. |



ATTACHMENT C
PRICING SCHEDULE

SOC: (Maintain security operations / SETA / CPT Remediation)

| | |
|---|--------------|
| One Time Charge (Prepayment for Year 1) | \$ 2,528,301 |
| Monthly (Years 2 - 5) | \$ 223,115 |
| Annual (Years 2 - 5) | \$ 2,677,380 |
| Total | \$13,237,821 |
| Prepayment Savings | \$ 149,079 |

**Attachment 1 – Network Security Monitoring Analysis and Alerting Service Description
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW04-CTS**

Introduction/Background

Texas Government Code Chapter 2059 authorized creation of a network and security operations center (NSOC) and the provision of network security services by State of Texas Department of Information Resources (DIR) for state agencies and others. The broad scope of the legislation places DIR in the position to provide information and defend against external threats. The Communications Technology Services (CTS) Division follows a scope based in Texas Government Code 2059 and places its primary focus on the enterprise infrastructure that DIR maintains on behalf of the state.

The dynamic nature of the cyber-threat, the continuously changing nature of technology and the evolving needs of the organizations that the NSOC protects, all create challenges for CTS/NSOC management. To provide the security necessary, the NSOC must:

- Consistently execute secure operation of existing capabilities;
- continually improve existing capabilities
- deploy tools to detect threats in the environment, and
- maintain trained operators who understand the technologies deployed as well as the DIR environment and customers.

And most importantly, the NSOC operation must be flexible enough to change as needed to address the ever-changing risks and threats to the State of Texas.

Scope of Work

The scope of work for this Network Security Monitoring, Analysis and Alerting Services agreement is to order, install and configure equipment and related infrastructure necessary to maintain current security monitoring capabilities through the expansion of the shared network to 10Gb capacity.

Period of Performance

The period of performance for this agreement is 36 months (calendar) from September 1, 2014. All work requirements described below will be performed from the date this SOW is accepted by both parties until this SOW expires or is otherwise terminated.

Place of Performance

AT&T may perform a majority of the work at DIR's NSOC facility. The project team members will be required to meet with DIR's management once per week (day and time TBD) either in-person or via teleconference for a weekly status meeting. DIR will provide and arrange for meeting spaces within its facility for all required meetings.

**Attachment 1 – Network Security Monitoring Analysis and Alerting Service Description
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW04-CTS**

Work Requirements

AT&T will provide the appropriate level of engineering resources to perform the work listed below:

- a) Order, install and configure equipment and related infrastructure necessary to maintain current security monitoring capabilities through the expansion of the shared network to 10Gb capacity. Specifically, this effort covers the equipment purchase, install and configuration for an Intrusion Prevention System (IPS) and a Network Aggregation system needed to provide the Monitoring Service, as outlined in Attachment B of Services Agreement NO SS-003-2011, attached hereto as Attachment B, as well as completing requisite infrastructure tasks (installing rack(s), power and telecomm cabling).

Schedule/Milestones

The below list consists of the initial milestones identified for the Installation effort within 10Gb Network Security Upgrade project:

| | |
|---|----------------------|
| SOW Approval | Day 0 |
| Project Kickoff | Day 1 |
| Order equipment and infrastructure needs | Day 2 |
| Complete upgrade of network devices | Day 14 |
| Receive Network Aggregation system components | Day 21 |
| Upgrade Network Aggregation system complete | Day 30 |
| Receive IPS Devices | Day 45 |
| IPS device Installation complete | Day 60 |
| IPS device configuration and testing complete | Day 90 |
| 10Gb router interface testing complete | Day 90 |
| Activation of new 10Gb Circuits | Day 90 (approximate) |
| Delivery of Operational System | Day 90 (approximate) |
| Annual Review #1 | Month 12 |
| Annual Review #2 | Month 24 |
| Project Completion Review | Month 36 |
| Project Closure/Archives Complete | Month 36 |

**Attachment 1 – Network Security Monitoring Analysis and Alerting Service Description
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW04-CTS**

Acceptance Criteria

Prior to each annual review, DIR Management will receive a supporting documentation package that will include a report on work completed, a report of the activity and effectiveness of the current system and recommendations for changes to equipment and processes to be implemented in the next period. DIR will also review the deliverables including the recommendations for the next period and if acceptable will approve and authorize the execution of work to implement the recommendations provided.

Security Operations Center Services (SOC Services)

In addition to the Work Requirements listed above, AT&T will perform the work outlined in Attachment B of Service Agreement NO SS-003-2011 as amended from time to time, attached hereto as Attachment B.

Service Level Agreements

Service Level Agreements will be in accordance with those Service Levels outlined in Attachment B of Service Agreement NO SS-003-2011, attached hereto as Attachment B.

Pricing

Pricing for services is contained in Attachment A to this SOW.

Payment will commence September 1, 2014. Should system delivery exceed September 30th, 2014 the payments will commence the month after system delivery.

Termination Charges

Should AT&T not be selected to provide SOC Services following the expiration of Service Agreement NO SS-003-2011, August 31, 2016, this SOW will also terminate. DIR will pay termination charges for the 10Gb monitoring services. Termination charges will be the monthly rate for the remaining months of service for the 10Gp monitoring services.

Any discrepancies involving completion of project tasks or disagreement between DIR and AT&T will be referred to both organizations' contracting offices for review and discussion.

Other Requirements

All AT&T project team members will submit security forms to DIR for clearance and access badges to the facility.

Attachment 1 – Network Security Monitoring Analysis and Alerting Service Description
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW04-CTS

IN WITNESS WHEREOF the Parties have executed this SOW04 as of the last day of the signature shown below.

TEXAS DEPARTMENT OF INFORMATION RESOURCES

By: Karen Robinson

Name: KAREN ROBINSON

Title: Executive Director

Date: 8-12-14

Legal: MZ/pjrb 8/12/14

AT&T Corp.

By: Eva P. Smith

Name: Eva Smith

Title: Lead Customer Contracts

Date: 22 Aug 2014

Attachment A Pricing
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW04-CTS

| Deliverable | Monthly Price | Annual Price | Extended Price (3yr) |
|------------------------------------|----------------------|---------------------|-----------------------------|
| 10 Gp Monitoring Service | \$25,000 | \$300,000 | \$900,000 |
| | | | |
| Total for 10 Gp Monitoring Service | | | \$900,000 |
| | | | |
| | | | |

**Attachment 1 – Network Security Monitoring Analysis and Alerting Service Description
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW05-CTS**

Introduction/Background

Texas Government Code Chapter 2059 authorized creation of a network and security operations center (NSOC) and the provision of network security services by State of Texas Department of Information Resources (DIR) for state agencies and others. The broad scope of the legislation places DIR in the position to provide information and defend against external threats. The Communications Technology Services (CTS) Division follows a scope based in Texas Government Code 2059 and places its primary focus on the enterprise infrastructure that DIR maintains on behalf of the state.

The dynamic nature of the cyber-threat, the continuously changing nature of technology and the evolving needs of the organizations that the NSOC protects, all create challenges for CTS/NSOC management. To provide the security necessary, the NSOC must:

- Consistently execute secure operation of existing capabilities;
- continually improve existing capabilities
- deploy tools to detect threats in the environment, and
- maintain trained operators who understand the technologies deployed as well as the DIR environment and customers.

And most importantly, the NSOC operation must be flexible enough to change as needed to address the ever-changing risks and threats to the State of Texas.

Scope of Work

The scope of work for this Network Security Monitoring, Analysis and Alerting Services agreement is to expand network security monitoring capabilities by implementing a Malware Detection System (MDS) and related infrastructure necessary to operate a Malware Detection System within the DIR Shared Network.

Period of Performance

The period of performance for this agreement is 36 months (calendar) from September 1, 2014. All work requirements described below will be performed from the date this SOW is accepted by both parties until this SOW expires or is otherwise terminated.

Place of Performance

AT&T may perform a majority of the work at DIR's NSOC facility. The project team members will be required to meet with DIR's management once per week (day and time TBD) either in-person or via teleconference for a weekly status meeting. DIR will provide and arrange for meeting spaces within its facility for all required meetings.

**Attachment 1 – Network Security Monitoring Analysis and Alerting Service Description
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW05-CTS**

Work Requirements

AT&T will provide the appropriate level of engineering resources to perform the work listed below:

- a) Expand network security monitoring capabilities, as outlined in Attachment B of Service Agreement NO SS-003-2011, attached hereto as Attachment B, by implementing a Malware Detection System (MDS) and related infrastructure necessary to operate a Malware Detection System within the DIR Shared Network. Specifically, this includes the effort to order, install and configure equipment of the MDS needed to provide the Malware Detection Service, as well as completing requisite infrastructure tasks (installing rack(s), power and telecomm cabling).

Schedule/Milestones

The below list consists of the initial milestones identified for the Installation effort within 10Gb Network Security Upgrade project:

| | |
|---|----------|
| SOW Approval | Day 0 |
| Project Kickoff | Day 1 |
| Order equipment and infrastructure needs | Day 2 |
| Complete upgrade of network devices | Day 14 |
| Receive MDS Devices | Day 30 |
| MDS Installation complete | Day 45 |
| MDS device configuration and testing complete | Day 60 |
| MDS System Operational | Day 90 |
| Annual Review #1 | Month 12 |
| Annual Review #2 | Month 24 |
| Project Completion Review | Month 36 |
| Project Closure/Archives Complete | Month 36 |

Acceptance Criteria

Prior to each annual review, DIR Management will receive a supporting documentation package that will include a report on work completed, a report of the activity and effectiveness of the current system and recommendations for changes to equipment and processes to be implemented in the next period. DIR will also review the deliverables including the recommendations for the next period and if acceptable will approve and authorize the execution of work to implement the recommendations provided.

**Attachment 1 – Network Security Monitoring Analysis and Alerting Service Description
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW05-CTS**

Security Operations Center Services (SOC Services)

In addition to the Work Requirements listed above, AT&T will perform the work outlined in Attachment B of Service Agreement NO SS-003-2011 as amended from time to time, attached hereto as Attachment B.

Service Level Agreements

Service Level Agreements will be in accordance with those Service Levels outlined in Attachment B of Service Agreement NO SS-003-2011, attached hereto as Attachment B.

Pricing

Pricing for services is contained in Attachment A to this SOW.

Payment will commence September 1, 2014. Should system delivery exceed September 30th, 2014 the payments will commence the month after system delivery.

Termination Charges

Should AT&T not be selected to provide SOC Services following the expiration of Service Agreement NO SS-003-2011, August 31, 2016, this SOW will also terminate. DIR will pay termination charges for the MDS services. Termination charges will be the monthly rate for the remaining months of service for the MDS services.

Any discrepancies involving completion of project tasks or disagreement between DIR and AT&T will be referred to both organizations' contracting offices for review and discussion.

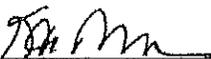
Other Requirements

All AT&T project team members will submit security forms to DIR for clearance and access badges to the facility.

Attachment 1 – Network Security Monitoring Analysis and Alerting Service Description
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW05-CTS

IN WITNESS WHEREOF the Parties have executed this SOW05 as of the last day of the signature shown below.

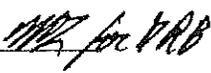
TEXAS DEPARTMENT OF INFORMATION RESOURCES

By: 

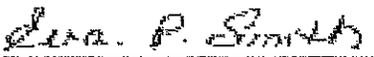
Name: Karen Robinson

Title: Executive Director

Date: 8-12-14

Legal:  for TDR 8/12/14

AT&T Corp.

By: 

Name: Eva Smith

Title: Lead Customer Contracts

Date: 22 Aug 2014

Attachment A Pricing
for Appendix D to DIR-SDD-1860
Service Agreement No. DIR-SDD-1860-SOW05-CTS

| Deliverable | Monthly Price | Annual Price | Extended Price (3yr) |
|--|----------------------|---------------------|-----------------------------|
| Malware Detection System - HW&SW | \$27,207.26 | \$326,487.13 | \$979,461.39 |
| Malware Detection System - Maintenance | \$7,652.99 | \$91,835.93 | \$275,507.79 |
| | | | |
| Total for Malware Detection System E&M | | | \$1,254,969.18 |
| | | | |

DIR Statement of Work (SOW) Change Order Request

Change Order One to DIR-SDD-779-SOW1-CTS

SDD-779-SOW1-CTS

This Statement of Work (SOW) Change Order Number One to SOW DIR- ("SOW") 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 SOW dated August 22, 2011 as follows:

I. Section 4.(b) Prepayment of Services is hereby revised and restated in its entirety:

For purposes of the Managed Security Services SOW, AT&T is providing a substantial discount in actual costs of performance in exchange for the prepayment of services which, by saving important and scarce State operating dollars for other needs of the telecommunications system, is a legitimate public purpose and is authorized under the State of Texas Procurement Manual.

III. Attachment C Pricing Schedule is hereby updated and restated as follows:

SOC: (Maintain security operations / SETA / CPT Remediation)

| | |
|--|-----------------------|
| One Time Charge (Prepayment for Year 1) | \$2,528,301 |
| Monthly (Years 2-5) | \$223,115* |
| Annual (Years 2-5) | \$2,677,380* |
| Total | \$13,237,821** |
| | |
| Prepayment Savings | \$149,079 |

*Monthly and Annual amounts due may be lower than the above stated year to year amounts due to prepayments negotiated at time payment is due.

**Total overall payments may be lower than the above stated amounts due to prepayments made throughout the life of the SOW.

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 Change Order One, then the Statement of Work, then the Contract.

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: *Maribel Salgado*
Name: *Maribel Salgado*
Title: *Contract Specialist*
Date: *12/6/2013*

The State of Texas, acting by and through

the Department of Information Resources

Authorized By: *John Hoffman*
Name: *John Hoffman*
Title: *Director of Communications Technology Services*
Date: *12/19/2013*

RR/zone, Assistant General Counsel 12-17-13

20140904-7785

DIR-SDD-779-SOW01 – CO2
to
APPENDIX C SERVICE AGREEMENT NO. SS-003-2011
to
DIR CONTRACT NUMBER DIR-SDD-779
between
the State of Texas, acting by and through the Department of Information Resources
and
AT&T Corp.

This SOW Change Order, (CO), 02 to Appendix C, Service Agreement No. SS-003-2011 to DIR Contract Number DIR-SDD-779 ("Contract") is between the State of Texas, acting by and through the Department of Information Resources ("DIR") and AT&T Corp. ("Vendor"). DIR and Vendor agree to modify the terms and conditions of the Service Agreement as follows:

1. Attachment C, Section 5.1. Pricing is hereby amended as follows:

Attachment C, Pricing Schedule, is hereby amended and replaced in its entirety, with a revised Attachment C dated September 1, 2014 to reflect a prepayment amount of \$1,000,000 for year 4 and reduce the year 4 monthly payments.

All other terms and conditions of the Service Agreement No. SS-003-2011, 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 CO2 to Service Agreement No. SS-003-2011, then CO1 to Service Agreement No. SS-003-2011, then Service Agreement No. SS-003-2011, and then the Contract.

THIS SECTION INTENTIONALLY LEFT BLANK

IN WITNESS WHEREOF, the parties hereby execute this CO2 to be effective September 1, 2014.

AT&T Corp.

By: *Lisa Casey-Gutshall*

Name: Lisa Casey-Gutshall
Contracts Specialist

Title: _____

Date: 9-11-14

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

By: *Karen Robinson*

Name: Karen Robinson

Title: Executive Director

Date: 9-10-14

Office of General Counsel: *K Robinson 9-10-14*



ATTACHMENT C

PRICING SCHEDULE

September 1, 2014

SOC: (Maintain security operations / SETA / CPT Remediation)

| | |
|---|--------------|
| Annual (Year 1) | \$ 2,677,380 |
| One Time Charge (Prepayment for Year 1) | \$ 2,528,301 |
| Monthly (Year 1) | \$ 0 |
| Prepayment Savings (Year1) | \$ 149,079 |
| Annual (Year 2) | \$ 2,677,380 |
| One Time Charge (Prepayment for Year 2) | \$ 644,713 |
| Monthly (Years 2) | \$ 166,167 |
| Prepayment Savings (Year 2) | \$ 38,664 |
| Annual (Years 3) | \$ 2,677,380 |
| One Time Charge (Prepayment for Year 3) | \$ 2,080,304 |
| Monthly (3/1/14 – 8/1/14) | \$ 86,679.33 |
| Prepayment Savings (Year 3) | \$ 77,000 |
| Annual (Year 4) | \$ 2,677,380 |
| One Time Charge (Prepayment for Year 4) | \$ 1,000,000 |
| Monthly (Year 4) | \$ 136,865 |
| Prepayment Savings (Year 4) | \$ 35,000 |
| Annual (Year 5) | \$ 2,677,380 |
| Monthly (Year5) | \$ 223,115 |
| Total | \$13,087,157 |
| Prepayment Savings | \$ 299,743 |

Change Order No. 3
to
SERVICE AGREEMENT NO. SS-003-2011,
DIR SOW No. DIR-SDD-779-SOW01-CTS
between
the State of Texas, acting by and through the Department of Information Resources
and
AT&T Corp.

THIS CHANGE ORDER, ("CO") 3 TO APPENDIX C, SERVICE AGREEMENT NO. SS-003-2011, DIR SOW NO. DIR-SDD-779-SOW1-CTS (the "CO") to DIR Contract Number DIR-SDD-779 and its successor Contract Number DIR-SDD-1860 is between the State of Texas, acting by and through the Department of Information Resources ("DIR") and AT&T Corp. ("Vendor"). As of the effective date of this CO 3, DIR and Vendor agree to modify the terms and conditions of the Service Agreement and its Attachments as follows:

1. DIR and Vendor acknowledge that the original contract from which the above-referenced Service Agreement and Statement of Work (SOW) was derived, Contract No. DIR-SDD-779, has expired and been replaced by Contract No. DIR-SDD-1860.
2. Pursuant to Section 3. Customer specific terms, of Appendix C Service Agreement No. SS-003-2011, as amended (hereinafter "Service Agreement"), DIR and Vendor agree to extend the term of the Service Agreement through August 31, 2017 under the terms and conditions of the successor Contract No. DIR-SDD-1860, as amended ("DIR Contract No. DIR-SDD-1860" or "Contract").
3. The effective date of this CO 3 will be August 31, 2015.
4. All references to Contract No. DIR-SDD-779 within the Service Agreement and its Attachments will be replaced with DIR Contract No. DIR-SDD-1860.
5. The parties also agree to amend the Service Agreement and Attachment A Terms and Conditions as follows:

a) **Appendix C, Service Agreement No. SS-003-2011, Section 3. Customer specific terms**, is hereby amended as follows:

"AT&T performance of Managed Security Services / Security Operations Center for DIR under this Service Agreement shall continue until August 31, 2017, unless earlier terminated or renewed in accordance with the provisions of this Service Agreement or Appendix A, Standard Terms and Conditions for Services Contracts dated 02/04/15 ("Appendix A"), Section 11. Contract Enforcement, B Termination as amended by paragraphs 7. W through BB) of Amendment 2 to Contract No. DIR-SDD-1860".

b) **Appendix C, Service Agreement No. SS-003-2011, Section 4(a) Pricing Schedules**, is hereby deleted and replaced with the following:

"(a) Pricing Schedules. A Pricing Schedule (Attachment C herein), attached to and a part of a Service Agreement, which identifies the Services AT&T may provide to Customer, the price (including discounts, if applicable) for each Service, and the term during which such prices are in effect ("Pricing Schedule Term"). Pricing shall be in accordance with Section 8 of the Appendix A, Standard Terms and Conditions for Product Related Services Contracts, dated 02/04/2015 ("Appendix A"), as amended by 7. H of Amendment 2 to the Contract No. DIR-SDD-1860.

- c) Appendix C., **Service Agreement No. SS-003-2011**, Section 6) **Revisions to Documents** is hereby deleted and replaced with the following:

"6) Revisions to Documents. Subject to Appendix A, Section 11. Contract Enforcement, B.7) (b_) **Materially Adverse Change**, as amended by Section BB of Amendment 2 to DIR Contract No. DIR-SDD-1860, AT&T may revise Service Guides or the AUP (collectively "Service Publications") at any time."

- d) Attachment A to **Service Agreement No. SS-003-2011**, Terms and Conditions, Section 2 is hereby deleted and replaced with the following:

"2. . That Appendix A, Standard Terms and Conditions for Services Contracts dated 02/04/15 to Contract No. DIR-SDD-1860 ("Appendix A"), Section 4. General Provisions, B. Modification of Contract Terms and/or Amendments, as amended in part in paragraph 7. B. of Amendment 2 to Contract No. DIR-SDD- 1860, does not apply to the SOC Services SOW."

- e) Attachment A to **Service Agreement No. SS-003-2011** , Terms and Conditions, Section 3 is hereby deleted and replaced with the following:

"3. That Appendix A, Section 11. Contract Enforcement, B.5) **Customer Rights Under Termination**, as amended in paragraph 7. Z of Amendment 2 to the DIR Contract No. DIR-SD-1860, is hereby amended and replaced in its entirety as follows:

"In the event the Contract expires or is terminated for any reason, a Customer shall retain its rights under the Contract and the Purchase Order issued with respect to all services ordered and accepted prior to the effective termination date. All Purchase Orders issued after expiration of the Contract shall be deemed Amendments to the SOW, such that those Purchase Orders shall run conterminous with the SOW."

- f) Attachment A to **Service Agreement No. SS-003-2011** , Terms and Conditions, Section 4 is hereby deleted and replaced with the following:

"4. That Appendix A, Section 10 **Vendor Responsibilities**, A. 2) **Acts or Omissions**, is hereby amended in its entirety for the SOC SERVICES SOW Attachment B to read as follows:

Vendor shall indemnify and hold harmless the State of Texas and

Customers, AND/OR THEIR OFFICERS, AGENTS, EMPLOYEES, REPRESENTATIVES, CONTRACTORS, AND/OR PERMITTED ASSIGNEES, FROM ANY AND ALL LIABILITY, ACTIONS, CLAIMS, DEMANDS, OR SUITS, AND ALL RELATED REASONABLE COSTS, ATTORNEY FEES, AND EXPENSES 1) for bodily injury (including death) or physical damage to tangible or real property, and 2) for unauthorized access to DIR or Customer information due to failure to protect such information in accordance with the SOC Services SOW to the extent directly arising out of, or resulting from any negligent acts or omissions or willful misconduct of the Vendor or its agents, employees or subcontractors, in the execution or performance of the Contract and SOC SERVICES SOW and any Purchase Orders issued under the Contract and SOC SERVICES SOW. VENDOR SHALL PAY ALL COSTS OF DEFENSE INCLUDING ATTORNEYS FEES THE DEFENSE SHALL BE COORDINATED BY THE OFFICE OF THE ATTORNEY GENERAL FOR TEXAS STATE AGENCIES AND BY CUSTOMER'S LEGAL COUNSEL FOR NON-STATE AGENCY CUSTOMERS."

- g) Attachment A to Service Agreement No. SS-003-2011, Terms and Conditions, the first full paragraph of Section 5 is deleted and replaced with the following:

"5. That Appendix A, Section 10. Vendor Responsibilities. A. 3) Infringement-, as amended in paragraph 7.0 of Amendment 2 to Contract No. DIR- SDD- 1860, is hereby amended in its entirety for the SOC SERVICES SOW Attachment B to read as follows:"

a) Vendor shall indemnify and hold harmless the State of Texas and Customers, AND/OR THEIR EMPLOYEES, AGENTS, REPRESENTATIVES, CONTRACTORS, AND PERMITTED ASSIGNEES from any and all third party claims involving infringement of United States patents, copyrights, trade and service marks, and any other intellectual or intangible property rights in connection with the PERFORMANCES OR ACTIONS OF VENDOR PURSUANT TO THE SOC SERVICES SOW and the CONTRACT, but not in circumstances where the claimed infringement arises out of or results from (a) Customer's, its Affiliates or a User's content; (b) modifications to the Service by Customer, its Affiliates or third parties, or combination of the Service with any services or products not provided by AT&T; or (c) use of the Service in violation of the CONTRACT and SOC SERVICES SOW

. VENDOR AND THE CUSTOMER AGREE TO FURNISH TIMELY WRITTEN NOTICE TO EACH OTHER OF ANY SUCH CLAIM. VENDOR SHALL BE LIABLE TO PAY

ALL REASONABLE COSTS OF DEFENSE INCLUDING ATTORNEYS' FEES FOR STATE AGENCY CUSTOMERS. THE DEFENSE SHALL BE COORDINATED BY THE OFFICE OF THE ATTORNEY GENERAL FOR TEXAS STATE AGENCY CUSTOMERS

AND TO THE EXTENT ALLOWED BY LAW, BY VENDOR'S LEGAL COUNSEL FOR NON-STATE AGENCY CUSTOMERS.

b) If Vendor becomes aware of an actual or potential claim, or Customer provides Vendor with notice of an actual or potential claim, Vendor may (or in

the case of an injunction against Customer, shall), at Vendor's sole option and expense: (i) procure for the Customer the right to continue to use the affected portion of the product or service, or (ii) modify or replace the affected portion of the product or service with functionally equivalent or superior product or service so that Customer's use is non-infringing. If neither option (i) nor (ii) are reasonably available, Vendor shall provide DIR with prompt written notice and the parties shall agree on how to revise the SOC SERVICES SOW to accommodate the change in the Service, including, but not limited to, amendment of the SOC SERVICES SOW and termination of the affected service.

- h) Attachment A to **Service Agreement No. SS-003-2011**, Terms and Conditions, Section 6 is hereby deleted and replaced with the following:

"6. That Appendix A, Section 10. Vendor Responsibilities, K Limitation of Liability is hereby amended in its entirety for the SOC SERVICES SOW Attachment B to read as follows:

1) EXCEPT AS SET FORTH IN SECTIONS 10. VENDOR RESPONSIBILITIES, A.2 ACTS OR OMISSIONS AND SECTION 10. VENDOR RESPONSIBILITIES, A.3 INFRINGEMENT, AS AMENDED BY PARAGRAPH 7.0 OF CONTRACT NO. DIR-SDD-1860, AT&T'S ENTIRE LIABILITY, AND CUSTOMER'S EXCLUSIVE REMEDY, FOR DAMAGES ARISING OUT OF MISTAKES, OMISSIONS, INTERRUPTIONS, DELAYS, ERRORS OR DEFECTS IN THE SERVICES, AND NOT CAUSED BY CUSTOMER'S NEGLIGENCE, SHALL IN NO EVENT EXCEED THE APPLICABLE CREDITS SPECIFIED IN THE SERVICE LEVEL AGREEMENTS ASSOCIATED WITH THE SOC SERVICES SOW.

2) SECTION 1) WILL NOT APPLY TO:

A) BODILY INJURY, DEATH, OR DAMAGE TO REAL OR TANGIBLE PROPERTY OR FOR ANY SUCH CLAIMS DERIVING FROM UNAUTHORIZED ACCESS TO DIR OR CUSTOMER INFORMATION DUE TO FAILURE TO PROTECT SUCH INFORMATION IN ACCORDANCE WITH THE SOC SERVICES SOW DIRECTLY CAUSED BY AT&T'S NEGLIGENCE UNDER APPENDIX A, SECTION 10 VENDOR RESPONSIBILITIES, A.2 ACTS OR OMISSIONS;

B) BREACH OF APPENDIX A, SECTION 10. VENDOR RESPONSIBILITIES, H CONFIDENTIALITY. AS AMENDED IN PARAGRAPH 7.R OF CONTRACT NO. DIR-SDD-1860, OR APPENDIX A, SECTIONS 7. CONTRACT FULFILLMENT AND PROMOTION, F DIR LOGO AND SECTION 7. CONTRACT FULFILLMENT AND PROMOTION, G VENDOR AND ORDER FILLER LOGO;

C) SETTLEMENT, DEFENSE OR PAYMENT OBLIGATIONS UNDER APPENDIX A, SECTION 10. VENDOR RESPONSIBILITIES, A.3) INFRINGEMENTS, AS AMENDED IN PARAGRAPH 7 O OF CONTRACT NO. DIR-SDD-1860. ; OR

D) DAMAGES ARISING FROM AT&T'S GROSS NEGLIGENCE OR WILLFUL

MISCONDUCT.

3) NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR SPECIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, ADVANTAGE, SAVINGS OR REVENUES, OR INCREASED COST OF OPERATIONS."

- i) Attachment A to **Service Agreement No. SS-003-2011**, Terms and Conditions, Section 7 is hereby deleted and replaced with the following:

"7. That Appendix A, Section 10 **Vendor Responsibilities** is hereby amended to add the following for the SOC SOW Attachment B:

X. Warranties. AT&T WARRANTS THAT IT WILL PERFORM THE SOC SERVICES SOW IN A GOOD AND WORKMANLIKE MANNER. AT&T MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, AND SPECIFICALLY DISCLAIMS ANY OTHER REPRESENTATIONS OR WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON INFRINGEMENT, OR ANY WARRANTY ARISING BY USAGE OF TRADE OR COURSE OF DEALING."

- j) Attachment A to **Service Agreement No. SS-003-2011**, Terms and Conditions, Section 8 is hereby deleted and replaced with the following:

" 8. That Appendix A, Section 10. **Vendor Responsibilities**, is hereby amended to add the following for the SOC SOW Attachment B:

Y. Disclaimer of Liabilities. AT&T WILL NOT BE LIABLE FOR ANY DAMAGES, EXCEPT TO THE EXTENT CAUSED BY AT&T'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, ARISING OUT OF OR RELATING TO: INTEROPERABILITY, ACCESS OR INTERCONNECTION OF THE SERVICES WITH APPLICATIONS, EQUIPMENT, SERVICES, CONTENT, OR NETWORKS PROVIDED BY CUSTOMER OR THIRD PARTIES, SERVICE DEFECTS, SERVICE LEVELS, DELAYS, OR INTERRUPTIONS EXCEPT FOR LIABILITY FOR SUCH EXPLICITLY SET FORTH IN THE SOC SERVICES SOW AND THE AGREEMENT OR SERVICE AGREEMENT) FAILURE TO CORRECTLY ROUTE OR COMPLETE CALLS OR OTHER TRANSMISSIONS (INCLUDING 911 CALLS), OR LOST OR ALTERED MESSAGES OR TRANSMISSIONS.

- k) Attachment A to **Service Agreement No. SS-003-2011**, Terms and Conditions, Section 9 is hereby deleted and replaced with the following:

"9. The parties agree that Appendix A, Section 10. **Vendor Responsibilities**, .J., **Background** and/or **Criminal History**

Investigation, shall apply to all Vendor employees assigned to deliver the SOC SERVICES SOW, originally and as the employees may change over time. In the event an employee fails to pass the background check customer may notify vendor and vendor must remedy the situation within a reasonable time period, any failure to do so shall be grounds for customer to terminate its purchase order and related service agreement. AT&T will notify DIR in a timely manner prior to removal or change in personnel so that the investigations may be conducted without adversely affecting ongoing operations under the SOC SERVICES SOW.

- l) Attachment A to **Service Agreement No. SS-003-2011** . Terms and Conditions, Section 10 is hereby deleted and replaced with the following:

"10. That Appendix A, Section 11, Contract Enforcement, .B. Termination, as amended in paragraph 7 BB. 7) Suspension and Termination of Services, a) Fraud or Abuse, of Amendment 2 to Contract No. DIR- SDD- 1860 does not apply to the SOC SERVICES SOW; however the following additional suspension and termination of Services provisions apply to such SOC SERVICES SOW:

a) Misuse or Abuse. If AT&T suspects misuse or abuse of services provided under the SOC SERVICES SOW, AT&T may terminate or suspend an affected Service by providing DIR with thirty (30) days advance written notice.

Definition of Misuse or Abuse. The misuse or abuse of, or the intended or attempted misuse or abuse of, services provided under the SOC SERVICES SOW is prohibited. The following activities constitute misuse or abuse: (i) Using Services provided under the SOC SERVICES SOW to transmit a message, locate a person, or otherwise give or obtain information, without payment for the service, (ii) Using or attempting to use services provided under the SOC SERVICES SOW with the intent to avoid the payment, either in whole or in part, of the charges for the services provided under the SOC SERVICES SOW by: (1) Rearranging, tampering with, or making connections not authorized by the SOC SERVICES SOW to any service components used to furnish services under the SOC SERVICES SOW, or (2) Using any unauthorized means or devices, tricks, schemes, false or invalid numbers, false credit devices, or electronic devices to gain access to or use the services provided under the SOC SERVICES SOW."

- m) Attachment A to **Service Agreement No. SS-003-2011**, Terms and Conditions, Section 11 is hereby deleted and replaced with the following:

"11. That Appendix A, Section 11. Contract Enforcement, .B.7 (and 8) through 9)) Termination, as amended in paragraph 7. BB. 9) Termination Charges of Amendment 2 to Contract No. DIR- SDD-1860, is hereby amended in its entirety for the SOC SERVICES SOW Attachment B to read as follows:

9) Termination Charges.

If, on or after Customer's obligation to pay for Services rendered under the SOC SERVICES SOW begins, Customer terminates a Purchase Order or Service Agreement for convenience or Vendor terminates a Purchase Order or Service Agreement for Customer's misuse or abuse, Customer's hazardous materials violations, or Customer's material breach, Customer will pay termination charges as follows:

If termination occurs before the end of the term of the SOC SERVICES SOW Service Agreement, then Customer's termination liability shall be 50% of the monthly recurring charges for the terminated Service or Service Component multiplied by the months remaining in the term, not to exceed \$1,260,000."

6. Attachment C, to Service Agreement No. SS-003-2011, Pricing Schedule is hereby amended and replaced in its entirety, with the revised Attachment C Pricing Schedule attached hereto.

All other terms and conditions of the Service Agreement No. SS-003-2011, 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 CO No. 3 to Service Agreement No. SS-003-2011, then CO No. 2 to Service Agreement No. SS-003-2011, then CO No. 1 to Service Agreement No. SS-003-2011, then Service Agreement No. SS-003-2011, and finally the DIR Contract No. DIR-SDD-1860.

The Remainder of This Page Intentionally Left Blank

IN WITNESS WHEREOF, the parties hereby execute this Change Order No. 3 to be effective August 31, 2015.

AT&T Corp.

By: 

Name: _____

Title: PATRICK GLEASON
ASSOC DIR CUSTOMER CONTRACTS

Date: 8-11-15

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

By: 

Name: TODD Kimball

Title: Interim Executive Director

Date: 8/26/15

Office of General Counsel: JPB MAR 8-24-15

ATTACHMENT C
 PRICING SCHEDULE
 August 31, 2015

SOC: (Maintain security operations / SETA / CPT Remediation)

| | |
|---|---------------------|
| Annual (Year 1) | \$ 2,677,380 |
| One Time Charge (Prepayment for Year 1) | \$ 2,528,301 |
| Monthly (Year 1) | \$ 0 |
| Prepayment Savings (Year1) | \$ 149,079 |
| | |
| Annual (Year 2) | \$ 2,677,380 |
| One Time Charge (Prepayment for Year 2) | \$ 644,713 |
| Monthly (Years 2) | \$ 166,167 |
| Prepayment Savings (Year 2) | \$ 38,664 |
| | |
| Annual (Years 3) | \$ 2,677,380 |
| One Time Charge (Prepayment for Year 3) | \$ 2,080,304 |
| Monthly (3/1/14 – 8/1/14) | \$ 86,679.33 |
| Prepayment Savings (Year 3) | \$ 77,000 |
| | |
| Annual (Year 4) | \$ 2,677,380 |
| One Time Charge (Prepayment for Year 4) | \$ 1,000,000 |
| Monthly (Year 4) | \$ 136,865 |
| Prepayment Savings (Year 4) | \$ 35,000 |
| | |
| Annual (Year 5) | \$ 2,677,380 |
| Monthly (Year5) | \$ 223,115 |
| | |
| Monthly (Year 6 per CO 3) | \$ 223,115 |
| | |
| Total | \$13,087,157 |
| | |
| New Total with CO 3 | \$15,764,537 |