Attachment – A

To Telecommunications Managed Services Agreement HHS000558300001

Statement of Work

This Attachment A covers scope, resources, and cost in reference to Agreement HHS000558300001. Attachment A details the statement of work (SOW) and required services to support the HHSC ENTERPRISE NETWORK OPERATIONS (ENO).

Attachment A - OVERVIEW

HHSC and Insight have agreed that the identified services and resources detailed in this Attachment A are critical to the continuation of the ENO network operations and management.

Statement of Work

1 Enterprise Network Operations Support Services

Introduction and Objectives

The HHS Enterprise Network Services Team primary goal in acquiring vendor network operations support services is to support the Network Division mission to provide secure, scalable, reliable, efficient, affordable and technologically advanced network services to all HHS programs and the constituencies they serve.

The scope contained in this agreement has resulted from a best effort to be representative of each of the key components of required services. However, this scope should not be considered all-inclusive of what the HHS Network Services Team (HNST) may request and expect from Insight in the day to day delivery of services and overall objective to provide complete service excellence to all stakeholders and service consumers.

The HNST through this agreement is contracting for a pool of full time dedicated onsite resources and expects an approach where the vendor resources can be redirected by HNST management to work on any tasks or issues they are qualified to work on based upon then current HHS Network Services Team priorities. The HNST understands that this redirection may from time to time require suspension of one or more SLA measurements while vendor resources have been directed to other agency priorities. In turn HNST expects the vendor resources to assist on any issue as directed by HNST management within their ability independent of if it is clearly defined in the scope section or not. The goal is to always fix the issue, solve the problem, support the customer or do whatever should be considered reasonably necessary to assist. Any ongoing scope or capacity issues or concerns can be dealt with during the monthly governance meetings and change order process if it becomes necessary. HNST will always expect Insight to work as an extension of the HNST and any member of either team needs to be willing and allowed to assist on any issue as may benefit HNST within the allotted resource hours and representative skill sets of the team members.

Insight and HNST will meet monthly to ensure that resource levels and roles are enough and appropriate to meet the HNST service levels for operations. If the operational activities increase or decrease by 15% either party may request a meeting to accelerate a recalibration of provided resource levels/roles to make adjustments to ensure HNST target objectives are met. If a recalibration is required Insight will adjust the monthly operational invoicing as required and agreed upon by HNST. Adjustments that include a cost increase may require an amendment to the agreement.

ENO Network Operations Support Services focuses on network operations at the HHSC Winters Data Center (WDC) and the Department of Information Resources (DIR) Network Security Operations Center (NSOC). The scope for the ENO Network Operations Support Services includes management and maintenance coordination of core, perimeter security, metro, WAN, LAN and numerous other network components as further described within this agreement. Insight will interface with the DIR, AT&T, CenturyLink, Cisco, various other entities, and service providers as necessary to ensure effective delivery and support of network services to HNST and stakeholders.

Insight will support HNST's strategic goal to maintain the networking infrastructure and services that will evolve with the needs of all the HHSC agencies it supports. These contracted services will support HNST in effectively and efficiently managing the infrastructure and resources to meet HNST objectives for the HHS System.

The SOW services are designed to optimize the operation and support of the ENO network infrastructure and are summarized as follows:

- To fully assist HNST in maintaining control of the HHS System Network infrastructure.
- To continue to optimize the operation and support of shared network infrastructure through consolidated network operations and IT support.
- Endeavor to support and fully leverage HNST service management tools for network and IT infrastructure support.
- Continually strive to increase the efficiency of network and IT infrastructure operations for HHSC agencies.
- Maintain an enterprise network and IT infrastructure that is secure, reliable, scalable, and enables agencies to achieve their business objectives.
- To operationally support the deployed redundant architecture for shared agency use of an enterprise-grade, centrally operated and highly secure infrastructure that has been implemented to protect HNST communications with external networks including the Internet, and to provide agencies with high-capacity, high-availability, virtual private network (VPN) services.
- To continue to provide and improve visibility into operational characteristics such as fault, performance, and capacity management as well as network monitoring functions.

Strategic Objectives include the architectural design and new network technology assessments that would enhance ENO performance, scalability and availability in future years.

Operational Objectives focus on the day to day availability of the network in support of ENO users and stakeholders. This includes proactive monitoring, and the use of HHSC Change and Incident processes to manage incidents and required changes to the network infrastructure.

Management Reporting Objectives include the collection of metrics that provide data for key reports; capacity trends, performance, asset management, and other reports that document the health of the ENO network. Reporting on Service Level Agreements (SLAs) and Service Level Objectives (SLOs) are required to maintain agreed upon contractual objectives.

Security Objectives include the effective management of intrusion protection systems and firewalls, as well as overall compliance with the HHSC Information Security Program policies and guidelines. Objectives also include consistent device security patch management.

1.1 Scope of Work

Each of the services outlined below will be defined by services description and level of support provided by Insight or HNST. The support levels are defined by Levels of Support with Level 1 being the lower or first level for support. The Tiered support model is defined in tables 1.0 and 2.0 below. HNST reserves the sole right to designate an issue or incident as needing Tier 3 support based upon HNST executive level exposure, involvement or direction.

- WAN Routers and Circuit Support (Field Offices)
- Core and Distribution Network Services
- Perimeter Network and Security Services
- Proxy Services
- Active Directory Services
- Network and Security Architecture Services
- IEE/TIRN Call Centers and EB/DPC Network
- Local Area Network Services
- Wireless Local Area Network Services
- Access Control Services
- IP Address Management Services
- Systems Services – UCS, VM, SAN (Telcom)
- Network Tools Support Services
- Video Conferencing Service

The parties agree that future HHS modernization efforts, including future cloud initiatives affecting the requirements of this contract, may be required. Depending on the cost and complexity of such efforts the parties agree to cooperate in the planning and implementation needed for such efforts. Such cooperation may include mutually agreed revisions of the scope and pricing through amendments.

It is understood and agreed that the fixed monthly service fee includes supporting moves, adds, upgrades, changes, refreshes, patches or removals to existing LAN/WAN equipment, site locations or to any other existing in-scope service or technology and shall not require any additional fees.

Support for upgrades is dependent on the skillset and capability of the Insight onsite operations and architecture team members and the team's availability to meet HNST desired upgrade schedule vs. maintaining daily support activities. HNST will work with Insight to prioritize workloads and operational tasks. Should any upgrade be mutually determined to be out of scope of this agreement the parties may develop a separate scope of work at an additional cost to be executed as project services as further defined within this agreement.

Insight shall perform the services at levels of accuracy, quality, completeness, timeliness, responsiveness, productivity, and resource efficiency that are necessary to meet all

requirements of this agreement.

Table 1.0 - Service Area Responsibility Matrix	Level 1	Level 2	Level 3
WAN Routers and Circuit Support (Central and Field Offices)	Insight	Insight	Insight
Core and Distribution Network Services	Insight	Insight	Insight
Perimeter Network and Security Services	Insight	Insight	Insight
AD Engineer Services	Insight	Insight	Insight
Network and Security Architecture Services	Insight	Insight	Insight
LAN/WLAN – Austin Metro	Insight/HNST	Insight/HNST	Insight
LAN/WLAN – Outside Austin Metro Field Offices	HNST	HNST	Insight
Access Control Services	Insight	Insight	Insight
IP Address Management	HNST	HNST	Insight
Systems - UCS, VM, SAN, O/S DOWN	Insight	Insight	Insight
Network Tools Support Services	HNST	HNST	Insight
Video Conferencing	Insight	Insight	Insight
IEE/TIRN Call Centers and EB/DPC Network	Insight	Insight	Insight

Table 2.0	Service Level	Description
Level	**Services Categories**	**Services Tasks**
Level 1	Access Management	Input Incidents into Incident Management System
		Monitor Remedy Ticket Queue
		Maintain Incident Status throughout lifecycle of Incident
		Provide On-call Support
	Request Fulfillment	Provide Network and System Monitoring
		Basic Troubleshooting and Incident Investigation
		Incident Prioritization
	Event Monitoring	Primary Point of Contact for status and communication of Incidents
	Incident Management	Incident Resolution or Escalation to Level 2
		Document Ticket with Required Information
		Update and Maintain Configuration Management System
		Participate in Root Cause Analysis as needed
		Close Resolved Tickets
Level 2	Event Management	Monitor Remedy Ticket Queue
		Provide On-call Support
		Field Escalations from Level 1
	Incident Management	Advanced Troubleshooting
		Incident Resolution or Escalation to Level 3
	Availability Management	Maintain Proactive Maintenance Schedule for Systems
		Perform Scheduled Maintenance
		Perform iOS and Software Upgrades
	Problem Management	Document Ticket with Required Information
		Perform Design and Configuration Changes
		Close Resolved Tickets

	Change Management	
Level 3	Strategy/Design Capacity Management Architecture Consultancy Incident Escalation Change Management	Provide On-call support
		Expert Troubleshooting
		Provide Escalation support for Critical Incidents and Events
		Provide Architecture Design and Guidance
		Provide iOS Version Recommendations
		Provide Hardware and Platform Recommendations
		Participate in Root Cause Analysis as needed
		Provide Support for Sanctioned Operational Initiatives
		Perform Network Maintenance in compliance with change management process
		Provide Support for Sanctioned Projects
		Close Resolved Tickets
		Collect network data and perform analysis to identify issues, patterns, or trends
		Define Process and Procedures for Level 1 and Level 2
		Provide Process Improvement and Technical Enhancements

1.1.1 Requirements Pertaining to all Service Areas Provided

- Device counts in any section of the agreement or in Appendix A are representative only. All devices installed for a service area are to be supported and the number of devices may increase or decrease during the term of the agreement. If the volume of required support activity changes due to the increase or decrease of devices either party can request a review as further described in the Introduction and Objectives of SOW Section 1.
- HNST is responsible to provide all monitoring and alerts through SolarWinds as well as ticketing and incident management through the Remedy system for all services supported in this agreement.
- Insight will participate in root cause analysis (RCA) and develop written RCA reports as needed or directed by HNST for all services areas provided. A written RCA is required for all critical incidents,
- Austin Metro is defined as any office located within the city of Austin or within a 25-mile radius of Austin and all service areas include onsite support if necessary for all HHS Austin Metro offices.
- Insight will be responsible for assisting in the maintaining of any lab environment associated with the services provided and for any set up, prep work, or testing for planned changes to production environment for all services provided.
- Insight will be responsible for making recommendations for standard configurations for all devices utilized in the delivery of the services being provided.

- Unless specifically documented otherwise within this agreement it is agreed Information Technology Infrastructure Library (ITIL) Service Management concepts and foundations are assumed to be integrated into all vendor provided services including:
    - Strategy
    - Design
    - Transition
    - Operation
    - Continual Improvement

1.1.2 High Level Service Descriptions

1.1.2.1 **WAN Routers and Circuit Support** - Insight will provide full support (Level 1, 2, 3) for all issues regarding WAN Routers at Austin Metro office locations and 750+/- remote field offices. WAN Routers and Circuit Support also includes third party services HHSC may contract for which are delivered over the MPLS WAN. This includes expert level troubleshooting for all issues. Insight will provide recommendations for iOS levels, hardware models, configurations and perform device upgrades. Insight will participate in root cause analysis as required.

1.1.2.2 **Core and Distribution Network Services** - Insight will provide full support (Level 1, 2, and 3) for the Core and Distribution network, including Legacy Core Network equipment such as VSSWAN and WAN6807 or other legacy devices. Support of all deployed F5 BIG IP load balancing equipment is also included. The support includes onsite support if necessary for all related equipment installed in any Austin Metro offices. Insight will provide all monitoring and alerts through HNST SolarWinds as well as managing the Incident Remedy queue. Insight will provide troubleshooting and incident management, change management, request fulfillment, and configuration management. Insight will provide recommendations for iOS levels and will implement that recommendations upon the direction of HNST. Insight will participate in root cause analysis as required.

1.1.2.3 **Perimeter Network and Security Services** - Insight will provide full support (Level 1, 2, and 3) and is responsible for monitoring and managing the Internet Perimeter Network Infrastructure, Proxy Services (IronPort), and all agency deployed firewalls. The operational focus is on protection of the network through proactive monitoring, analysis, assessment, and response to security threats as well as developing and approving security policy and posture in conjunction with HSSC Security Operations Team. The primary goal is the health and performance of the Internet Perimeter Network Infrastructure. Insight will also support Enterprise VPN and Site to Site VPN Tunnel Operations Support Services.

The email proxy services are dependent upon HNST deployed solutions and are intended to include but are not limited to Global Threat Analysis, Spam blocking, Graymail detection, Advanced Malware Protection, Outbreak filters, Web interaction

tracking, Outbound message control and Forged email detection. This includes automated monitoring and analysis of inbound and outbound traffic, application visibility and control as well as fast identification of zero-day attacks. The support includes onsite support if necessary for all related equipment installed in any Austin Metro offices.

These activities include incident management and resolution, change management, configuration management and problem management. Insight will provide recommendations for iOS levels, security best practices, configurations. Insight will provide Root Cause Analysis as needed.

1.1.2.4 AD Engineer Services - Insight will provide a dedicated full-time resource onsite to support Active Directory as directed by HHSC. This includes re-engineering, DNS support, GPO audits and creations, replication monitoring, domain consolidations and scripting for user and AD migrations. Resource will also provide recommendations on process improvement, configuration and the standardization of the Active Directory environment.

1.1.2.5 Network and Security Architecture Services - Insight will provide Network and Security Architecture Services to HNST based on evolving industry trends and vendor best practices. Insight will provide recommendations to integrate these technologies into the HHS Enterprise Network Infrastructure and will provide recommendations for hardware models and IOS/OS software versions. Additional responsibilities include assisting with developing test cases, identifying pros/cons of the technologies within enterprise core network, and helping to develop Root Cause Analysis (RCAs) for enterprise core network outages. The services to include architecture design support across all networking technologies and if the Insight onsite architect resources do not possess a certain technology skill set necessary to support an HNST request than Insight will locate another resource who can temporarily assist the onsite team to meet the need. The services to include architecture design support to Identify, evaluate, plan and move major connections/services from end of life equipment (including but not limited to VSS-WAN and WAN6807), to provide DMVPN Architecture support and Enterprise WAN troubleshooting, to provide design enhancement solutions support as well as implementation support. Insight support to include architecture assistance for IPv6 planning, RFC 1918 design or planning or other HNST IP address management architectural initiatives. Insight Architecture Services will also include support for designing and planning Cisco ISE. The Insight Network Architect(s) will be physically onsite located at the HHSC headquarters, John H. Winters building at 701 W. 51st Street or mutually agreed HNST Operations Center location.

1.1.2.6 **Local Area Network Services (LAN) -** Insight and HNST will share responsibility for providing Level 1 & 2 support for Austin Metro office locations. Insight will provide Level 3 support for Austin Metro office locations including onsite support if needed. HNST will provide Level 1 & 2 support for offices outside the Austin Metro area. Insight will provide Level 3 support for offices outside of the Austin Metro area. Insight will provide recommendations for iOS levels and configurations as directed by HNST. Insight will

participate in root cause analysis as required. This infrastructure supports all the remote field sites, which have HHSC IT Customer Service (ITCSO) remote hands available to assist for offices outside the defined Austin Metro area.

1.1.2.7 **Wireless Local Area Network Services** (WLAN) - Insight and HNST will share responsibility for providing Level 1 & 2 support for Austin Metro office locations. Insight will provide Level 3 support for Austin Metro office locations including onsite support if needed. HNST will provide Level 1 & 2 support for offices outside the Austin Metro area. Insight will provide Level 3 support for offices outside of the Austin Metro area. Insight will provide recommendations for iOS levels, FUS image, configurations as directed by HNST. Insight will participate in root cause analysis as required. This infrastructure supports all the remote field sites, which have HHSC IT Customer Service (ITCSO) remote hands available to assist for offices outside the defined Austin Metro area.

1.1.2.8 **Access Control Services** - Insight will provide full support (Level 1, 2, and 3) for the ISE, ACS and RSA servers currently hosted on HNST platforms located at the Winters Data Center (WDC), DIR NSOC and DR location(s). This service includes support for the administration and usability for the ISE and RSA applications as it applies to the HNST network environment. This service will provide support for the capacity and availability planning in support of HNST initiatives and expansion of the network. Insight will participate in root cause analysis as required. This service includes support for execution of migration of network Device Management from Cisco ACS to Cisco ISE.

1.1.2.9 **IP Address Management Services –** Insight will provide Level 3 support of IP Address Management Services. IPAM (IP Address Management) is the administration of DNS and DHCP, which are the network services that assign and resolve IP addresses to machines in a TCP/IP network. HNST utilized tools include DNS and DHCP.

1.1.2.10 **Systems Services -** Insight will provide full (Level 1, 2, and 3) operational support of the Infrastructure Systems Platforms. These platforms include:

1. The Telecom Services Team systems at the Winters Data Center (WDC) and a Disaster Recovery/Backup system located at the DIR NSOC. This service includes system support of the VMWare/ v-Center infrastructure, UCS platform and the EMC UNITY and VNX SAN Storage systems for the HHSC Telecom Verint and Avaya platforms. System support includes the restoration of services from the backup location as required. Systems support will include infrastructure support for building application servers from OVA. Systems support includes support from the operating system down. Operating system support includes validating and applying vendor published hot fixes and updates as authorized by HNST or Telecom. Anti-virus and software firewalls are not included in operating system support. Insight will participate in root cause analysis as required.

2. The Network Services Team systems at the Winters Data Center (WDC) and the DIR NSOC. These systems include the HyperFlex UCS and other B and C series UCS and Dell compellent systems operated by the Network Division. System support includes the restoration of services from the backup location as required. Systems support will include infrastructure support for building application servers from OVA. Systems support includes support from the operating system down. Operating system support includes validating and applying vendor published hot fixes and updates as authorized by HNST. Insight will participate in root cause analysis as required.

1.1.2.11 **Network Tools Support Services -** Insight will provide Level 3 support of the Network Tools applications hosted on HNST platforms located at the Winters Data Center (WDC) or NSOC. Includes but may not be limited to SolarWinds, Skybox, NetScout or other applications or products utilized to monitor, maintain and manage all the network services. The support does not include support of the application code itself. Insight will participate in root cause analysis of issues as required.

1.1.2.12 **Video Conferencing -** Insight will provide full (Level 1, 2, and 3) operational support of the HNST Video Infrastructure Systems Platform located at the Winters Data Center (WDC), the DIR NSOC or Austin Metro locations. The platform is made up of TelePresence Video Communication Server (VCS), Expressway, Telepresence content server, TelePresence Management Suite (TMS) and the meeting server (CMS) components. The solution is hosted on HNST provided hardware located at the WDC and may be deployed at the DIR NSOC at some time during this agreement. The Video conferencing solution support internal endpoints, external endpoints (Internet/B2B) as well as neighbor zones for included agencies. Supported endpoints includes the TC and CE Series enabled endpoints from with a centralized phonebook. The support of the Video Platform system and its underlying infrastructure does include individual end user support or scheduling activities. Insight will participate in root cause analysis as required. No onsite office support is included outside a 25-mile radius of Austin. HNST expects Insight to leverage the current DSHS contract resources if possible to ensure HNST is getting the best overall value in the delivery of the combined DSHS and HNST video services.

1.1.2.13 **IEE/ TIRN Call Centers and EB/ DPC Offices Network Support Services** - Insight will provide full support (Level 1, 2, and 3) for network routers, LAN switches, firewalls, WLC, wireless APs (Ed Bluestein, Kramer Lane, San Antonio), ACS (Ed Bluestein), and DHCP server (IEE phones) at IEE Call Centers Network at Ed Bluestein, Austin, San Antonio, Athens and Edinburg, IEE and TIRN Data Center Networks at NSOC and SADC, EB Outreach offices at Houston, Abilene and Arlington and Document Processing Center Network at Kramer Lane, Austin and Athens. This includes onsite support if needed at all in-scope locations except TIRN call center locations. Insight will provide recommendations for iOS levels and as well as hardware models. Insight will participate in root cause analysis as required. Insight support shall include 211 TIRN Call Centers and both the IEE and HNST network components and services at the four IEE Call Centers Network at Ed Bluestein, Austin, San Antonio, Athens and Edinburg.

1.1.3 Network Technology Plan

Insight will develop and implement an enterprise network technology plan that is consistent with ENO Operations standards and strategies that enables the HNST to achieve their strategic plans and objectives. The development of the annual network technology plan shall be an iterative process to be carried out in consultation with HNST architects, directors, and managers as appropriate. The network technology plan shall be finalized by March 1st of each year.

Insight will include in the network technology plan, a technology roadmap detailing schedules, dependencies, and requirements for introducing new technological changes as well as acquiring, supporting, and retiring software and hardware. The roadmap shall have short-term and long-term goals demonstrating specific technology solutions that apply to new products and processes or emerging technologies.

Insight will develop and maintain pertinent ENO network diagrams and documentation in support of the in-scope network components and services. Updated network architecture diagrams must be continually maintained as changes occur. A full set of network diagrams and documentation must be provided on the Network Division share drive and any changes to network diagrams and documentation must be posted within 30 days.

Insight will assist HNST in developing and maintaining a detailed asset inventory of all devices at Austin Metro locations and all 750+/- WAN field office locations. Documentation shall include device type, serial number, name, maintenance coverage status, maintenance level, current deployed code level, latest available manufacturer code level, HNST business purpose, HW or SW EoS dates, deployed or depot, HNST asset number, as well as any other field the team determines is necessary to have an effective and accurate inventory management system. Any device replacements, moves, upgrade, RMA etc. will need to be tracked and changes to HNST asset tracking or SmartNet contract coverage is expected to be managed by Insight with oversight and direction from the HNST. Insight will coordinate completion and submission of any required asset transfer forms and SmartNet or other manufacturer maintenance coverage updates related to any changes for in-scope components.

Insight will provide an annual summary report of complete ENO network asset inventory to include components in production, spares and details of any RMAs completed. All Insight responsibilities related to Inventory and Assets will be fully coordinated with the HNST Asset and Inventory Coordinator.

1.1.4 Technology Currency

Insight will ensure all network devices, appliances, systems, software, and firmware are maintained at current versions and that a plan is in place to replace or upgrade any provider's product before manufacturer end of support date (EoS) are reached. Insight will perform periodic software upgrades in accordance with HNST patch management policy.

Insight will perform general maintenance, upgrades, QoS configurations, software / firmware updates, and performance upgrades to network devices, appliances, systems, and services

used for network monitoring. Work will be accomplished in compliance with HHSC Change Approval Board (CAB) approved processes and procedures.

1.2 Network Operational Availability and Support

1.2.1 Daily Operations

The entire Insight network services staff resources provided under this agreement shall be physically located on site at HHSC office at 701 W 51st St, Austin, TX 78751 - Winters Complex Building C. A total of 11 staff have been agreed to for delivery of the services in this agreement. Insight shall provide staff coverage as agreed to support the services being provided during work hours between 7 a.m. and 7 p.m. Monday through Friday excluding Texas state holidays.

Insight will work with HNST to provide suitable replacement resources for any planned time off away from HNST Operations of 5 or more consecutive business days.

Insight will work with HNST to provide suitable replacement resources for any unplanned, emergency, or unforeseen situations on a best effort basis and as agreed to with HNST based on the situation.

HNST will provide work space, computers and telephones for all on-site staff. Travel between primary work location and any other Austin Metro office work location is included in this agreement and is to be at Insight's expense. Any requested travel outside the defined Austin Metro area may require additional charges. Network and Security Architecture staff positions are in addition to the defined onsite daily operations staff.

Incident management and the emergency change management window shall be considered (24X7X365). On-call after-hours operational support outside work hours is required during the defined period of this agreement. Major change activities are scheduled in advance, occur after 10:00 p.m. Monday – Friday unless otherwise authorized by CAB, and on weekends during approved maintenance windows.

HNST provides all Insight staff with HHSC email accounts, which include appointment/meeting calendars that serve as the official record of all communication and scheduling of appointments and meetings. Insight staff must follow all HHSC Security Requirements regarding email communications. Insight staff shall comply with any HHSC requirements to gain access to any HHSC system resources. Insight staff are required to use the HHSC provided email addresses for any and all communications related to delivery of services within this agreement

Insight will perform change management to proactively open network related change requests as required. Manage a queue within the HHSC change management system to create and monitor the initiation, progression, and completion of planned change activities and communicate same to HHSC change coordinators and/or management. Obtain required approvals and attend the HHSC Change Approval Board (CAB) to represent Insight managed change requests and to schedule work to be performed. Update change records to reflect system's return to normal operations.

Insight will perform incident management to proactively open network related incidents as required. Respond to network outages in accordance with agreed to service level requirements.

Mitigate, resolve, and escalate network issues to the attention of higher-level resources as appropriate. Coordinate provider break/fix activities as required. Verify normal operations before accepting systems back into operations.

Insight will routinely assess performance and load on infrastructure to identify systems that may require balancing or additional capacity. Insight will provide inputs and metrics to all capacity management initiatives.

Insight will develop, maintain and continually execute and report against a patch management plan that has been submitted to and approved by HNST.

Insight will perform backups for the data network equipment (configurations). Verify that restoration of configuration and/or data from backups is tested quarterly and demonstrated in a manner consistent with HNST ENO procedures for this task. Insight will develop, maintain and continually execute and report against a backup and storage management plan that has been submitted to and approved by HNST.

1.2.2 Operations Management

Insight will provide two Operations Management staff positions. One to focus on Perimeter Network and Security Services and the other to focus on all other elements of the network operations support services. Both managers will provide managerial and technical oversite for all operational activities that fall within Insight's scope. Operations Managers will provide prioritization and guidance for technical operations and incidents. Operations Managers will ensure all incidents and escalations are addressed within the required SLA's and SLO's. The Insight Operations Managers will work in conjunction with the Insight assigned Program Manager to report on governance objectives. Operations Managers will be responsible for leading efforts on escalated critical events and incidents categorized as high. Additionally, the Insight assigned Operations Managers have the responsibility to supervise Insight technical staff and enforces the overall standards for the Operations support of HNST. The Operations Managers will participate in all weekly / monthly / quarterly business reviews for operations with the HNST. This role will assist with operational engineers' interaction with vendors, HNST, and project managers within and outside of team. The Operations Managers will participate in management meetings with HNST, will respond to operational requests and will provide weekly updates to stakeholders on operational status. The Operations Managers will mentor and instruct operational engineers on the team and services being delivered. On-call will be supported for escalations as needed.

1.2.3 Monitoring

Insight will provide monitoring of the ENO network and respond per the agreed coverage period for the affected service or site. The emergency incident management window shall be considered (24X7X365). On-call after-hours operational support outside normal work hours is required during the defined period of this agreement for any services or sites documented as requiring (24X7X365) support. HNST has the sole discretion on determining which sites are to be considered (24X7X365) and the site list may change during the term of this agreement. Both parties agree to evaluate staffing levels based on changes to 24X7X365 site list. All other sites are best effort to have services up by next business day according to agreed SLA and SLO.

Insight will utilize HNST provided systems and tools to identify the appropriate action to take monitoring the operating states of hardware, operating systems, software applications, and services.

Insight will detect, acknowledge, record, classify, prioritize, and escalate incidents utilizing the HNST provided Remedy incident management system. Incidents may be detected and reported from automated alerts and events from tools in use or from incident report phone calls.

Insight will perform predictive analysis to forecast traffic patterns, peak period routing and equipment failures to provide optimal use of network resources and to provide feedback to authorized users of those resources. Insight will capture and summarize key operational performance measures for each operating period.

1.2.4 ITIL Process Implementation and Compliance

Insight will use and comply with all HNST ENO ITIL processes. The processes will apply to any changes in the standards, processes, procedures and controls or associated technologies, architectures, products, materials, equipment, systems or services provided, operated, managed, supported or used in connection with the services.

1.3 Management Oversight / Reporting

1.3.1 Meetings and Coordination

Insight will attend internal coordination, stakeholder coordination, Network Team program coordination, management reporting, and service level review meetings to assure alignment with HNST Operations objectives.

Insight will at the direction of the designated incident manager, initiate and/or participate in conference calls that require multi-function entities (i.e., network security, network services) to resolve.

Insight will conduct post-mortem meetings after network outages to determine and/or report on root cause. This includes submission of a Root Cause Analysis (RCA) report.

Insight shall be considered the SMEs of the ENO network and as such will participate in ENO Operations, CAB or other meetings as necessary to ensure efficient and effective delivery of the services.

1.3.2 Reporting

Insight will produce monthly trend reports to highlight network incidents and problems and establish pre-determined action and escalation procedures when incidents and problems are encountered.

Insight will produce monthly capacity utilization reports of circuits and equipment, exception reports and SLA, SLO reports for monthly review meetings. Reports shall include reported issues encountered throughout the reporting period.

Insight will present monthly system reports including fault and performance data, and analysis

information of ENO Network issues.

Insight will produce weekly and monthly Network Performance summary reports identifying potential connectivity issues to address.

The following daily, weekly and monthly reporting will be provided by Insight to HNST. HNST and Insight will work together to create and standardize on metrics and reports. Please note that all reporting tools and metrics will be collected, analyzed and gathered utilizing HNST ticketing systems and tools.

Reporting Element	Method	Frequency	Tools
Security Health Check Reports	Email	Daily	Remedy, SolarWinds
Program and Services Delivery Review (no meeting week of monthly Governance meeting)	Meeting	Weekly	Remedy, SolarWinds, SharePoint, PMO Tools
HNST News Letter	Email	Weekly	Multiple Sources
Governance Review	Meeting	Monthly	Remedy, SolarWinds
Quarterly Business Review	Meeting	Quarterly	Remedy, SolarWinds, SharePoint, PMO Tools
Technology Roadmap	Meeting	Semi-Annually	Multiple Sources
Technology Plan	Report	Annual	Multiple Sources

1.3.3 Service Level Objectives

Service Level Objectives are targets that will be reported on monthly during the governance meetings. In the event Insight does not perform against the service level objectives, HNST should escalate any issues or concerns to Insight Services Management so that Insight can provide HNST with a plan to remediate any gaps in meeting service objectives.

As previously stated in Section 1 HNST's goal is to always fix the issue, solve the problem, support the customer or do whatever should be considered reasonably necessary to assist. Any ongoing scope or capacity issues or concerns can be dealt with during the monthly governance meetings and change order process if it becomes necessary. HNST will always expect Insight to work as an extension of the HNST and any member of either team needs to be willing and allowed to assist on any issue as may benefit HNST within the allotted resource hours and representative skill sets of the team members.
If the Insight Operations Manager believes the attainment of Service Level Objectives (SLO) or Service Level Agreements (SLA) may be negatively impacted during any specific redirection of resources for other HHS enterprise network related initiatives, the HNST Director may provide temporary relief from the SLA requirements for Insight resources to undertake HNST directed priority activities.

Incidents escalated outside of the hours of 7AM-7PM CT, Monday-Friday, must be in the form of a text, automated notification sent to a phone number or a phone call.

1.3.4 Service Response and Service Resolution Definitions (SRDs)

Insight and HNST will utilize the following Service Level Objectives and they will be measured and reviewed monthly. These Service Level Objectives do not carry liquidated damages however Insight and HNST have agreed that they are the service levels everyone will strive to achieve monthly in the delivery of ENO network operations support services.

Problem Severity	Level 1 Response	Level 2 Response	Resolution Plan	Hardware Replacement	Problem Resolution
Critical Incident	Immediate escalation to Level 2, Network Director and Operations Manager	15 minutes	2 hours	2 hours if spares onsite, 6 hours if SNTP (4hr vendor replacement) or Next Business Day (NBD) for non (24x7x365) site	4 hours
High Incident	Immediate escalation to Level 2, Network Director and Operations Manager	15 minutes	4 hours	2 hours if spares onsite, 6 hours if SNTP (4hr vendor replacement) or Next Business Day (NBD) for non (24x7x365) site	8 business hours
Medium Incident	15 minutes	2 hours	12 hours	16 business hours	36 hours
Low Incident	15 minutes	4 hours	3 days	5 business days	6 days

1.3.5 Severity Definitions

Critical *	High	Medium	Low

Severe business impact Primary business function is stopped with no redundancy or backup Critical WAN site down	High business impact Primary business function is severely degraded or supported by backup or redundant system Risk of Sev-1 until redundancy restored	Non-critical business function is stopped or severely degraded Some specific network functionality is lost or degraded, such as loss of redundancy	A functional query or fault that has no business impact for the organization Non-critical business function is degraded

1.3.6 Support Level Definitions

Support Level	Responsibility	Goals
Level 1 Support	7-7 M-F service desk support. First line end user support. Opens trouble tickets. Works on problem up to 15 minutes, documents ticket and escalates to appropriate Insight level 2 support	Resolution of 25% of incoming tickets
Level 2 Support	Queue monitoring, network management. Place trouble tickets for software/hardware identified problems. Take calls from level 1, vendor, and level 3 escalations. Assume ownership of call until resolution. Manage change control. Implements after-hours changes. Coordinates 3rd party vendor support and equipment replacements.	Resolution of 50% of tickets escalated to level 2
Level 3 Support	Provide immediate support to level 2 for all Critical severity incidents. Works to help with all incidents unsolved by level 2.	Resolution of escalated incidents

1.3.7 Escalation Notification Matrix

Elapsed Time	Critical	High	Medium	Low

1 hour	Update to Network Director and Operations Manager, level 3 support, and Director of Converged Services	Update to Network Director and Operations Manager, level 3 support, and Director of Converged Services		
2 hours	Escalate to HHSC ECSS director and Insight Director of Services, Network Director, Operations Manager, and Director of Converged Services.	Update to Network Director and Operations Manager, level 3 support, and Director of Converged Services		
4 hours	Past 4H unresolved requires CIO notification	Escalate to HHSC ECSS director and Insight Director of Services, update to Network Director, Operations Manager, and Director of Converged Services.		
24 hours			HNST Operations Managers	
5 days	Root cause analysis to ECSS director, Network Director, Operations Manager, and Director of Converged Services			HNST Operations Managers

1.3.8 Service Level Objectives (SLO's)

1.3.8.1 SLO 1 - Mean-Time-To-Restore (MTTR): Core and Critical Components (CCC) and Non-Critical Components and connectivity.

The total restoration time of all incidents within a category is within target Mean restoration as

defined in the SRDs

All four (4) categories of incidents measured for MTTR will be measured separately and reported on separately monthly.

Mean-Time-To Restore (MTTR) specifies a compliance threshold for resolving incidents. Compliance is determined by first assessing the time to resolve all incidents during the assessment period in a category then by determining the total MTTR for all systems in that category.

This metric is defined from 7am to 7pm: Monday thru Friday.

1.3.8.2 SLO 2 - Critical Event Notification & Escalation

Appropriate notifications and escalations occurred within timeframes as defined in the Escalation Notification Matrix

Proper notification and escalations for 95% of all critical incidents during 7am to 7pm Monday - Friday except state holidays.

Critical Event Notification and Escalation specifies a compliance threshold for notifying or escalating HNST contacts of critical incidents within specified timeframes. Compliance is determined by first assessing the time to notify individuals as per the Escalation Notification Matrix during the measurement period. To achieve the SLO, 95% of those notifications and escalations must occur within timeframes as defined in the in the Escalation Notification Matrix.

1.3.8.3 SLO 3 - Change Management Implementation

Ninety-five percent of all changes are implemented within the approved change duration window.

Change Management Implementation assesses the timeliness of Level 2 change management activities. The SLO defines the minimum threshold for approved changes performed within the assigned change window. Compliance is determined by assessing the total time required to implement an approved change versus the scheduled and approved change window. For example, if the approved change window is two hours and it takes four hours to implement the change, the change was not completed within the approved change window. Ninety-five percent of all changes must be completed within their approved change window.

1.3.8.4 SLO 4 - Unrecorded/Unapproved Changes

The SLO is based on 7 x 24 x 365.
Unrecorded/Unapproved Changes defines the threshold for instances of unrecorded or unapproved changes as zero “0.” If a change is implemented without approval or a change is not recorded in the appropriate change management system, the SLO target is not achieved.

1.3.9 Service Level Agreements (SLA’s)

As previously stated in Section 1 HNST’s primary goal in acquiring vendor network operations support services is to support the Network Division mission to provide secure, scalable, reliable,

efficient, affordable and technologically advanced network services to all HHS programs and the constituencies they serve. HNST is not interested in enforcing a collection against any SLA failure as that means HNST and Insight have failed against the delivery of the mission. However, SLA's are required to ensure Insight throughout the term of the agreement continually provides the necessary resources to meet the primary goal and provides HNST with an enforceable remedy if an SLA is not met.

Also as previously stated in Section 1 HNST's goal is to always fix the issue, solve the problem, support the customer or do whatever should be considered reasonably necessary to assist. Any ongoing scope or capacity issues or concerns can be dealt with during the monthly governance meetings and change order process if it becomes necessary. HNST will always expect Insight to work as an extension of HNST and any member of either team needs to be willing and allowed to assist on any issue as may benefit HNST within the allotted resource hours and representative skill sets of the team members.

If the Insight Operations Manager believes the attainment of Service Level Objectives (SLO) or Service Level Agreements (SLA) may be negatively impacted during any specific redirection of resources for other HHS enterprise network related initiatives, the HNST Director may provide temporary relief from the SLA requirements for Insight resources to undertake HNST directed priority activities.

1.3.9.1 The following SLA's apply to (1) Core and Network Distribution Services, (2) Network Security Services, (3) Proxy Services and (4) System Services**.**

1.3.9.1.1 SLA 1 - Mean-Time-To-Restore (MTTR) – $5,000 Per Month

The total restoration time of all incidents within a category is within target Mean restoration as defined in the SRDs. All four (4) categories of incidents measured for MTTR will be aggregated monthly resulting in a single measurement instead of four (4) individual measurements. Mean-Time-To Restore (MTTR) specifies a compliance threshold for resolving incidents. Compliance is determined by first assessing the time to resolve all incidents during the assessment period in a category then by determining the total MTTR for all systems in that category. This metric is defined from 7am to 7pm: Monday thru Friday

1.3.9.1.2 SLA 2 - Critical Event Notification & Escalation - $500 Per Event

Appropriate notifications and escalations occurred within timeframes as defined in the Escalation Notification Matrix. Proper notification and escalations for 95% of all critical incidents during 7am to 7pm Monday - Friday except state holidays. Critical Event Notification and Escalation specifies a compliance threshold for notifying or escalating HHS contacts of critical incidents within specified timeframes. Compliance is determined by first assessing the time to notify individuals as per the Escalation Notification Matrix during the measurement period. To achieve the SLA, 95% of those notifications and escalations must occur within timeframes as defined in the in the Escalation Notification Matrix.

1.3.9.1.3 SLA 3 - Change Management Implementation - $2,500 Per Month

Ninety-five percent of all changes are implemented within the approved change duration window. Change Management Implementation assesses the timeliness of Tier 2 change management activities. The SLA defines the minimum threshold for approved changes performed within the assigned change window. Compliance is determined by assessing the total time required to implement an approved change versus the scheduled and approved change window. For example, if the approved change window is two hours and it takes four hours to implement the change, the change was not completed within the approved change window. Ninety-five percent of all changes must be completed within their approved change window.

1.3.9.2 The following SLA's apply to all Insight provided services**.**

1.3.9.2.1 SLA 4 - Unrecorded/Unapproved Changes - $500 Per Event

The SLA is based on 7 x 24 x 365. Unrecorded/Unapproved Changes defines the threshold for instances of unrecorded or unapproved changes as zero "0." If a change is implemented without approval or a change is not recorded in the appropriate change management system, the SLA target is not achieved.

1.3.9.2.2 SLA 5 - Response Time - $500 Per Event

The SLA is based on 7 x 24 x 365. Ninety-five percent of all critical and high incidents escalate to Level 3 are acknowledged within the response time as defined in the SLO Table (Figure 2.0). Response time assesses the timeliness of Level 3 acknowledgment of escalated issues. Compliance is determined by measuring the response time for each High and Critical incident escalated to Level 3. For example, if 100 critical/high incidents were escalated to Level 3, 95 must be acknowledged within the prescribed time.

1.3.10 Inventory and Asset Management

All Insight responsibilities related to Inventory and Assets will be fully coordinated with the HNST Asset and Inventory Coordinator.

Insight will ensure all network equipment or network associated equipment is properly tagged whenever a unit is placed into service.

Insight will ensure the physical location of where the device is located is reported to the asset management group on the designated form.

Insight will ensure that when an appliance fails, and parts are replaced, both the incoming and outgoing replacement part's identifying nomenclature, asset inventory number and serial numbers are appropriately reported to the asset management group on the designated HNST forms.

Insight will ensure that when an in-place device is upgraded by installing individual card(s) in an existing appliance, the identifying nomenclature and serial number of each card is associated with the parent unit's identifying nomenclature, asset inventory number, and serial numbers and are appropriately reported to the asset management group on the designated HNST forms.

Insight will notify HNST promptly if and to the extent any HNST-owned equipment will no longer be used to provide the services. The notification shall include the identification of the equipment,

the date it will no longer be needed by ENO Operations, and the reason for decommissioning.

Any equipment decommissioned by Insight will include wipe of any existing configuration information and readying for HHSC surplus processing.

1.3.11 Security Initiatives and Compliance

Insight will assist HNST to ensure all provided services comply with the following federal regulations and policies to which HHS is subject:

- Texas Health & Safety Code, Title 2, Subtitle I, Chapter 181: Medical Records Privacy, enacted 2011
- IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, revised 2010
- ARRA, including HITECH Act, enacted 2009
- CMS Policy for Information Security Program, dated 12/31/2008 (Document Number: CMS-CIO-POL-SEC02-03.2; sections 4.1.1, 4.7, 4.14, 4.16, and 4.17.4)
- FISMA, enacted 2002
- HIPAA, enacted 1996
- FERPA, enacted 1974
- Texas Government Code, Title 10, Subtitle B, Chapter 2059, Subchapter A, Sec. 2059.056: Responsibility for External and Internal Security Threats, enacted 2005
- Texas Business and Commerce Code, Title 11, Subtitle B, Chapter 521, Subchapter B, Sec. 521.052: Business Duty to Protect and Safeguard Personal Identifying Information, enacted 2005
- TAC Title I, Part 10, Chapter 202, Subchapter B, Rule 202.22 and 202.25, enacted 2004
- HHS Enterprise Information Security Standards and Guidelines (EISSG)

1.4 Adherence to HHSC Security Programs

ENO Network Operations Support Services and HHSC Enterprise Security share responsibility for monitoring and supporting various aspects of the network perimeter security infrastructure.

Insight shall participate in and adhere to all HHSC Security Program rules, regulations and guidelines.

2 Qualified Personnel Requirements

2.1 Insight Staff Roles

Insight will provide the following staff roles in the delivery of the in-scope services. The purpose of the roles definition below is to provide a frame of reference for the types of roles needed to provide the services. All services will be provided by a team physically located at the HHSC headquarters, John H. Winters building at 701 W. 51st Street or mutually agreed HNST Operations Center location. The agreed number of full-time onsite resources is stated in section 1.2.1. It is understood that the program manager and certain high-level escalation resources may not be physically on-site full time. However, it is HNST's expectation that the onsite Insight team will be able to support delivery of at least 90% of the in-scope services and that the onsite staff built into the monthly fee will be 100% dedicated to providing services to HNST under this

agreement. If any requests from HNST to Insight are determined to be out of scope of this agreement and require additional fees than Insight will obtain additional resources and the onsite team will not be utilized for delivery of the additional fee services.

Title	Description
Program Manager	A Program Manager will be assigned throughout the term of the contract and will be overall responsible for all governance and communications between HNST and Insight. The Program Manager will also oversee all aspects and Deliverables of all sub-phases of the program. All personnel for this engagement will roll up to the assigned program manager. The Program Manager will be responsible for all governance activities for the operations.
Operations Manager(s)	The Operations Manager supervises technical staff and enforces the overall standards for the Operations support of HNST. The Operations Manager will participate in all monthly / quarterly business reviews for operations with the HNST. This role will assist with operational engineers' interaction with vendors and HNST. Interacts with project managers within and outside of team. Attends management meetings with HNST. Responds to operational requests and provides weekly updates to stakeholders on operational status. Mentors and instructs operational engineers on the team.
Network Architect(s)	The architect position will provide oversight to the network services task for the security and network operations. The architect will provide technical oversight for all the Operations Support Service team members.
Senior Network Engineer(s) (Security)	The Senior Network Engineers for the perimeter operations will provide daily network support for perimeter operations and provide escalation responses for Network Engineers. This will include proactive monitoring, and response to security threats as well as validating security policy and posture.
Network Engineer(s) (Security)	The Network Engineers for the perimeter operations will assist Senior Network Engineers and provide daily network support for security operations.
Senior Network Engineer(s)	The Senior Network Engineers for the network operations will provide daily network support and provide escalation responses for Network Engineers. Will contain knowledge of network topology deployed in support of the HHSC agencies. The position will understand how the agency locations and regions are provided connectivity to the HNST core network and data centers and the shared data centers and Internet-facing connectivity operated with DIR.
Network Engineer(s)	The Network Engineers for the network operations will assist Senior Network Engineers and provide daily network support.
Systems Engineer(s)	The Systems Engineers for the systems operations will provide

Title	Description
	daily systems operations support and provide escalation responses. Will contain knowledge of systems deployed.

2.2 Staff Qualifications

Insight provided staff will have appropriate qualifications across different components including:

- Familiarity with common network components (e.g., routers, switches, firewalls) and interconnections (i.e., WAN circuits of various technologies and capacities including T1, DS3, metropolitan fiber, etc.) used within the HNST network.
- Knowledge of network topology technologies that are in use and deployed by HNST to support of the HHSC agencies. The positions will be educated and debriefed as part of an onboarding process so that the Insight teammates have an understanding of how agency locations and regions are provided connectivity to the HNST core network and data centers as well as to the shared data centers and Internet-facing connectivity operated by DIR.
- Experience and skills with common systems administration procedures including scheduled backup and on-demand restoration of large-scale software applications and/or related data.
- Experience in the use of common desktop tools (e.g., Excel) for the parsing and/or analysis of fault and performance data.
- Experience with inter-networking troubleshooting in a large-scale network environment.
- Knowledge of IP Internetworking, LAN Switching, PRIME Infrastructure, WAN Expertise, WLAN and Voice technologies.
- Familiarity with QoS mechanisms and configurations in an enterprise environment to support voice traffic.
- Experience with supporting a VoIP solution in an enterprise network as an end-to-end solution from IP Phones, access, distribution, and core layer switches. Insight will support configuration changes (provided by others) on the network devices for VOIP transport on the managed services platform.
- Familiarity with the use of enterprise-level tools for network fault and performance monitoring activities such as those within the SolarWinds Orion suite and Computer Associates (CA) products including Spectrum, eHealth, NetQoS Reporter Analyzer or similar products from other vendors.
- Familiarity with networking protocols within the TCP/IP family to include an understanding of basic network sub-netting and routing principles, DNS, and depth in the requirements and use of protocols common to networking monitoring and management including SNMP, Secure Shell (SSH), NetFlow, and others.
- Familiarity with the Telecom Infrastructure Systems Platform made up of a primary system at the Winters Data Center (WDC) and a Disaster Recovery/Backup system located at the DIR Network Security Operations Center (NSOC). This service include system support of the VMWare/ v-Center infrastructure, UCS platform and the EMC UNITY SAN Storage systems for the HNST and Telecom Verint and Avaya platforms. Systems support will include the Fabric switch and the interface/hand-off to the HNST infrastructure team.

2.3 Skill Sets

Insight resources within the ENO Network Operations Support Service team shall include engineers and technicians with knowledge and skillsets across the technologies utilized in the HNST ENO environment.

The provided resources shall have the following minimum qualifications and skill sets:

- Experience performing the duties listed in the Scope section of this SOW.
- Experience monitoring alerts, events, and network security solutions using technologies listed in the Current State Technologies section.
- Minimum of 5-years working experience
- Including professional certifications such as, CCIE, CCNP, and/or CCNP-Security or equivalent as needed to deliver the complete scope services in this agreement.
- Demonstrated ability to interact positively and constructively with customers
- Excellent oral and written communication skills to share findings in an understandable and actionable manner
- Ability to handle multiple competing priorities
- Capable of turning ambiguous problems into clear information
- A firm understanding of the concepts of confidentiality, integrity, and availability
- Experience working within and providing leadership to a team of network-management services personnel
- Experience in the use of RoD, including incident, change, and configuration management in support of established ITIL processes
- Experience in the use of common desktop tools (e.g., Excel) for the parsing and/or analysis of fault and performance data

2.4 Use of Subcontractors

Insight shall provide HNST with prior written notice and obtain written approval from HNST prior to any change in key personnel involved in providing services under this contract.

Subcontractors providing services under the contract shall meet the same requirements and level of experience as required of Insight. No subcontract under the contract shall relieve Insight of responsibility for ensuring the requested services are provided. If Insight is planning to subcontract all or a portion of the work to be performed, Insight shall identify the proposed subcontractors and HNST retains the right to check subcontractor's background and approve or reject the use of submitted subcontractors at any time during the life of the agreement.

2.5 HNST Request for Removal

HNST reserves the sole right to require removal of any specific Insight staff member for any reason from further work under this contract. In such an event HNST management will work with Insight to provide a reasonable amount of time to provide a replacement resource.

3 Transition and Turnover Plan

Turnover is defined as activities required for the Insight to perform turnover contract service delivery to HNST or to HNST's designated resources. The Turnover Phase and contract closeout will begin three (3) months prior to the end of the Contract Term, which may include optional renewal periods, or HNST's request for Contract termination.

3.1 Transition and Turnover Plan

Turnover includes the administrative and operational activities performed by Insight to transition operations to either a State agency or State-designated successor Vendor at the direction of the State.

Turnover tasks must be planned and coordinated with the State and State-designee to ensure stakeholders and HNST ENO users or stakeholders do not experience any adverse impact from the Turnover.

Turnover activities must be completed according to the State-approved Turnover Plan. Insight will be responsible for completion of all Service Requests (SR) agreed upon with the State prior to Turnover.

During turnover, Insight must ensure program stakeholders do not experience adverse impact from the transfer of services. Six (6) months prior to the end of the Contract term, Insight must develop and submit a comprehensive Turnover Plan detailing the proposed schedule, activities, and resource requirements associated with the turnover tasks identified.

3.2 Turnover Activities

The Turnover activities include, but may not be limited to:

- Submission of and adherence to the HNST approved Turnover Plan, including specific completion and Acceptance Criteria.
- Turnover Inventory, including a complete inventory of all Insight artifacts, tasks, systems, tools, and hardware, being turned over to HNST.
- Turnover Results Report.
- Develop and implement an HNST approved, comprehensive Turnover Plan detailing the proposed scheduled, activities, and resource requirements associated with the turnover tasks identified. During turnover, Insight must ensure program stakeholders do not experience any adverse impact from the transfer of services. Turnover commences three (3) months prior to the end of the Contract Term, which may include any optional renewal periods, or HNST's request for Contract termination.
- Transfer of information on all software tools currently in use
- Implement a quality assurance process to monitor turnover activities
- Training HNST and/or its designated resources on the delivery of operational phase services

- On-boarding the Insight Turnover Service Domain Lead
- Preparing a Turnover Plan identifying tasks, task owners, and turnover milestone dates
- Execute the approved Turnover Plan in cooperation with the State or State-approved successor transition plan.
- Maintain service delivery staffing levels during the turnover period and only reduce staffing levels with prior approval by HNST.
- Notify HNST of reassignment, resignation, or termination of contract for any of its Key Personnel during the Turnover Phase.
- Provide to HNST or its designee, within 15 business days of the request, data and reference tables, scripts, other documentation, and records required by HNST or its designee.
- Prepare a Turnover Inventory (inventory of all Insight artifacts, tasks, systems, tools, and hardware being turned over to HNST).
- Hand off the operation and management of all service delivery functions to HNST or its designee. Plan and manage Turnover without disruption of service to users, clients and/or beneficiaries.
- Work closely with HNST to ensure Turnover of responsibilities and the necessary knowledge transfers by the end of the contract period.
- Respond within State-approved timeframes to all HNST requests regarding turnover information.
- Provide knowledge transfer services to the State or the State's designee during Turnover period including, implementation of a quality assurance process to monitor Turnover knowledge transfer activities and training for HNST staff and/or HNST designees on the delivery of services.
- Provide a Turnover Results Report
- Provide 90 business days of on-site post-turnover support to address technical questions from HNST or HNST's designee.
- Both Parties agree that neither Party will directly or indirectly solicit, offer employment or hire any current or former employee or consultant of the other party who was directly involved in the HNST ENO Network Operations Support Services. This provision does not restrict the right of either party to solicit or recruit generally in the media and does not prohibit either party from hiring an employee of the other who answers any advertisement or who otherwise voluntarily applies for hire without having been initially personally solicited or recruited by the hiring party.
- Both parties agree that there will be a reduced Transition and Turnover Plan Services Fee if ENO Transition and Turnover Plan Services and TIERS Transition and Turnover Plan Services, contract # HHS000461400001, initiate and occur simlulaneously. In this instance, the reduced ENO Transition and Turnover Plan Services Fee will be $68,906.00 for a TIERS and ENO combined amount of $300,000.00

4 Fees – ENO Network Operations Support Services

4.1 ENO Network Operations Support Services - Fee Table

Insight will provide HNST the "ENO Network Operations Support Services" at the fixed daily or monthly fees listed below. HNST will be invoiced monthly at these rates at the end of each month of service starting from November 25, 2019 through December 31, 2020. HNST may

extend the term of this Agreement for up to twenty-four (24) successive one-month periods after the expiration of the initial term, or as necessary to complete the mission of the procurement.

Frequency	Day or Months Number	Coverage Period	Fee
Day	6	November 25, 2019 through November 30, 2019 ($9,894.64 per day)	$59,367.84
Month	13	December 01, 2019 through December 31, 2020 ($296,839.33 per month)	$3,858,911.29
Month	24	January 01, 2021 through December 31, 2022 ($296,839.33 per month)	$7,124,143.92
Month	6	Transition and Turnover Plan Services	$231,094.00
		Project Services	$1,500,000.00
Total			**$12,773,517.05**

4.2 Projects Services - Fee Table

At the written request of HNST, Insight will provide hourly or fixed fee project services for any projects or initiatives mutually agreed to fall outside of the defined base services described within this agreement. These services will utilize the established Change Request process and will not exceed $1,500,000.00 throughout the duration of the agreement. Utilization of this change request process to authorize project services up to the $1,500,000.00 will not require an amendment to this agreement.

Frequency	Role	Hourly Rate
As Agreed by Each Project	Fixed Fee Project	TBD Per Each Project
Monthly Bill	Architect	$198.00
Monthly Bill	Sr. Engineer	$165.00
Monthly Bill	Engineer	$125.00
Monthly Bill	Project Management	$145.00
Monthly Bill	Technicians	$85.00
Monthly Bill	Cabling Techs	$65.00

4.3 Change Request Process and Form

HNST and Insight will utilize the change request form below to document any utilization of the project services authorized within this agreement.

CHANGE REQUEST FORM **CHANGE REQUEST #** XXXX			
Client / Client's Contract No#	**Original Project Name**	**Original Insight SoW #:**	
Insight Services Manager/Director	**Client Project Sponsor**	**Request Date**	
Purchase Order to Apply to Changes:			
Change Request Summary			
Original Scope Task	Enterprise Network Operations Support Services		
Reason for Change			
Description of Change			
Schedule			
Pricing			
Signatures			
Insight Authorized Signer:		**Date:**	
Print Name:	**Title:**		
TX HHSC Authorized Signer:		**Date:**	
Print Name:	**Title:**		

Appendix A - Current State Technologies

This section provides summary data regarding current state technologies. The provided device counts are representative only and may increase or decrease based upon the business requirements of HNST. This is not a fixed fee contract for a fixed number of devices being managed. As stated in the Reporting Section - If the operational activities increase or decrease by 15% either party may request a meeting to accelerate a recalibration of provided resource levels/roles to make adjustments to ensure HNST target objectives are met.

A.1. Physical Network Diagrams

The following diagrams provides conceptual illustration of the components and services infrastructure, used within the ENO Core, Distribution Perimeter Security Network Operations Support Services environment

Figure 1 – ENO Overview

A.2. WAN Routers

In-Scope Equipment	Quantity
Cisco ISR4321	230
Cisco ISR4331	276
Cisco ISR4351	1
Cisco ISR4431	51
Cisco ISR4451	2
Cisco ISR2911	103
Cisco ISR2921	1
Cisco ASR 1001-X	2
Cisco MAR2612	2
Cisco 2811VE	9

A.3. Core and Distribution Network Related Equipment

In-Scope Equipment	Quantity
Core L3 & ToR Switches	
Cisco Catalyst 6880-X	2
Cisco Catalyst 6807-XL	3
Cisco Catalyst 6509-V-E	2
Cisco Catalyst 4500X	15

In-Scope Equipment	Quantity
Cisco Catalyst 3850	18
Cisco Catalyst 3750	1
Cisco Catalyst 3560	4
Nexus / FEX	
Cisco Nexus 9508	2
Cisco Nexus 9504	2
Cisco Nexus 2248PQ	2
Cisco Nexus 2348UPQ	2
UCS	
Cisco UCS 6248 FI	2
Cisco UCS 5108	1
Cisco UCS C220 M5	4
Cisco UCS B200M4	4
Video	
Cisco BE7K / UCSC-C240-M4S2	2
Cisco CMS1000 / UCSC-C220-M4S	1
Cisco BE6K / UCSC-C220-M4S	2
Cisco BE6M-M4-K9	2
Routers	
Cisco ASR1006X	2
Cisco ASR1002-X	2
Cisco ASR1001	2
Cisco ISR 2901	2
WAAS	
Cisco WAVE-8541	2

A.4. Perimeter Security Support Services

In-Scope Equipment	Quantity
Firewalls	
Cisco ASA 5585-X	4
Cisco ASA 5555-X	6
Cisco ASA 5540	2
Cisco ASA 5525-X	2
Cisco ASA 5520	3
FirePOWER IPS & Manager	
Firepower 8350	4
FS2000	1
FireEye & Manager	

In-Scope Equipment	Quantity
CM7400	1
NX10450	2
IXIA iBypass Switches	
IBPVHD	2

A.5. Proxy Services

In-Scope Equipment	Quantity
WSA & Manager	
Cisco WSA S690	16
Cisco WSA S680	2
Cisco WSA S670	2
Cisco WSA S370	2
Cisco WSA S170	1
Cisco CSM M300V	1
Cisco CSM M690	1
Cisco CSM M695F	1
ESA & Manager	
Cisco WSA S690	6
Cisco CSM M690	1
Load Balancers	
BIG-IP i2600	4
BIG-IP i2800	6
BIG-IP 5250F	2

A.6. LAN Sites

In-Scope Equipment	Quantity
Cisco Catalyst 3560	23
Cisco Catalyst 37xx	30
Cisco Catalyst 2924R	1
Cisco Catalyst 2950	7
Cisco Catalyst 2960	961
Cisco Catalyst 3560	59
Cisco Catalyst 3850	108
Cisco Catalyst 4500X	21
Cisco Catalyst 4900M	2
Cisco Catalyst 6506	4
Cisco Catalyst 6807-XL	2
Cisco Catalyst 68xx	5

In-Scope Equipment	Quantity
Cisco Catalyst 9xxx	21
Cisco Catalyst 6503	6

A.7. WLAN

In-Scope Equipment	Quantity
Wireless LAN Controllers	7
Cisco Wireless Access Points	656
Meraki Wireless Access Points	1201

A.8. Access Control Systems

In-Scope Equipment	Quantity
ISE	
Cisco SNS 3495	6
ACS	
Cisco ACS (Legacy) - 1121-K9	2
Cisco ACS (ENO) - VM	2

A.9. System Services (Telecom Related VM – UCS)

In-Scope Equipment	Quantity
Cisco UCS 6296 Fabric Interconnect	2
Cisco UCS 5108 Chassis	3
Cisco UCS B200 Blades	18
EMC Unity 400 Storage	1
EMC Unity 450F Storage	1
Cisco MDS 9148 Fiber Channel Switch	2
Cisco UCS 6248 Fabric Interconnect	2
Cisco UCS 5108 Chassis	2
Cisco UCS B200 Blades	13
EMC Unity 400 Storage	1
EMC Unity 450F Storage	1
Dell R730	10
BIG IP F5	1
Cisco MDS 9148 Fiber Channel Switch	2

A.10. Network Management and Monitoring Systems

In-Scope Equipment	Quantity
SolarWinds - VM	1
Cisco Prime - VM	1
Infoblox IB-2225	2

In-Scope Equipment	Quantity
Infoblox IB-1415	2
Infoblox ND-V2205	1
Infoblox IB-V2205	1

A.11. Video Conferencing

In-Scope Equipment	Quantity
Cisco Meeting Server	1
Cisco TelePresence DX70	1
Cisco TelePresence SX20	47
Cisco TelePresence SX80	2
Cisco Webex Codec Plus	22
TANDBERG Codec C90	1
TANDBERG Codec C20	2
TANDBERG Codec C40	2
TANDBERG EX90	23
TANDBERG VCS	4
TANDBERG Tactical MXP 2	1

A.12. IEE/TIRN Call Centers and EB/DPC Sites

In-Scope Equipment	Quantity
Switches	
Cisco C9300	32
Cisco C4948	2
Cisco 3850	39
Cisco C3750X	7
Cisco C3750V2	48
Cisco C2960	5
Cisco C2960S	4
Cisco C2960X	3
Firewalls	
Cisco ASA5510	1
Cisco ASA5515	2
Cisco ASA5520	10
Cisco ASA5555	6
Routers	
Cisco ISR3900	21
Cisco ISR2900	29
Cisco ISR4321	19

In-Scope Equipment	Quantity
Cisco ISR4431	2
Cisco ISR4331	5
Cisco ASR1002-X	6
UCS	
Cisco C220-M3L	3
Wireless AP	
Cisco AAP3802I	80
Cisco CAP3702I	6
Cisco CT5508	1
Cisco RM3000M=	2

Event Details

Event ID	Format	Type	Round	Version
HHSTX-HHS0005583	Buy	RFx	1	1

Event Name

RFQIT_INFORMAL_TELECOMMUNICATIONS MANAGED SERVICES

Post Date	Due Date
07/24/2019	09/24/2019

Event Currency: US Dollar

Bids Allowed in Other Currency: No

Respondent: **INTERNAL EVENT DETAILS**

Bidder Name

Tin

Address

Phone

Fax

Email

Submit To: HHS Purchasing

See Part A for Submission Instructions

United States

Contact: Davenport,Charles S

Event Description

RFQIT_INFORMAL_TELECOMMUNICATIONS MANAGED SERVICES AGREEMENT FOR TIERS

General Comments

- This procurement is for a DIR Managed Services Telecommunications Contract network operations support contract for HHSC and TIERS ongoing operations support. Justification: To provide for critical network operations services while the agency determines the best long term strategy and approach for consolidating network operations and support for the areas of TIERS, Enterprise Network and legacy DSHS. Additional time is needed to develop the strategy and approach, formulate into requirements, develop procurement documents, conduct a completive procurement and evaluation, and to allow for time to transition to a new vendor. This is a $0 requisition to establish a requisition

- This procurement is for a DIR Managed Services Telecommunications Contract network operations support contract for HHSC and TIERS ongoing operations support. Justification: To provide for critical network operations services while the agency determines the best long term strategy and approach for consolidating network operations and support for the areas of TIERS, Enterprise Network and legacy DSHS. Additional time is needed to develop the strategy and approach, formulate into requirements, develop procurement documents, conduct a completive procurement and evaluation, and to allow for time to transition to a new vendor. This is a $0 requisition to establish a requisition

Event Details

Event ID	Format	Type	Round	Version
HHSTX-HHS0005583	Buy	RFx	1	1
Event Name				
RFQIT_INFORMAL_TELECOMMUNICATIONS MANAGED SERVICES				
Post Date		**Due Date**		
07/24/2019		09/24/2019		

Event Currency: US Dollar

Bids Allowed in Other Currency: No

Respondent: **INTERNAL EVENT DETAILS**

Bidder Name

Tin

Address

Phone

Fax

Email

Submit To: HHS Purchasing

See Part A for Submission Instructions

United States

Contact: Davenport,Charles S

Line Details

Line: 1 **NIGP Class Item:** 958 **Expected Qty:** 1 **UOM:** EA

For "No Bid", LEAVE BLANK

	Quantity:	Price
Vendor Response :	1	

Line Description : A TELECOMMUNICATIONS MANAGED SERVICES AGREEMENT FOR TIERS NETWORK OPERATIONS SUPPORT AND SERVICES.