Department of Health and Mental Hygiene (DHMH)

Consulting and Technical Services+ (CATS+)
Task Order Request for Proposals (TORFP)

LONG TERM SUPPORTS AND SERVICES SYSTEM (LTSS)
Operations & Maintenance (O&M)
CATS+ TORFP # DHMH OPASS 18-17607 / M00B8400002

Issue Date: June 2, 2017

KEY INFORMATION SUMMARY SHEET

This CATS+ TORFP is issued to obtain the services necessary to satisfy the requirements defined in Section 3 - Scope of Work. All CATS+ Master Contractors approved to perform work in the Functional Area under which this TORFP is released shall respond to this TORFP with either a Task Order (TO) Proposal to this TORFP or a Master Contractor Feedback form (See Section 4).

Solicitation Title:	LTSS O&M
DHMH OPASS (TORFP #):	DHMH OPASS 18-17607 / M00B8400002
Functional Area:	Functional Area 8 – Application Service Provider
Issue Date:	June 2, 2017
Questions Due Date and Time:	June 30, 2017 at 3:00 PM Local Time
Closing Date and Time:	July 24, 2017 at 2:00 PM Local Time
TO Requesting Agency:	Department of Health and Mental Hygiene (DHMH) Office of Health Services (OHS)
Send Proposals to:	Queen Davis Office Phone: (410) 767-5335 E-mail: queen.davis@maryland.gov ***E-mail submission strongly preferred.***
Send Questions to (e-mail only)	E-mail: dhmh.solicitationquestions@maryland.gov
TO Procurement Officer:	Queen Davis Office Phone Number: (410) 767-5335 Office Fax Number: (410) 333-5958
TO Contract Monitor:	Jane Holman Maryland DHMH Office of Health Services 201 West Preston Street, Room 117 Baltimore, Maryland 21201 Telephone: (410) 767-1294 Fax: (410) 333-5333 E-mail: Jane.Holman@maryland.gov
TO Type:	Fixed Price
Period of Performance:	Four (4) year Base Period with one (1) one-year Option Period, for a total of five (5) years if both the Base Period and Option Period are fully executed.
MBE Goal:	25% with no sub-goals
VSBE Goal:	0%
Small Business Reserve (SBR):	No
Primary Place of Performance:	Maryland DHMH 201 West Preston Street Baltimore, MD 21201

TO Pre-proposal Conference:	Maryland DHMH 201 West Preston Street, Room L1 Baltimore, MD 21201 June 21, 2017 at 1:30 PM Local Time See Attachment 6 for directions.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 1 - ADMINISTRATIVE INFORMATION

1.1   TORFP SUBJECT TO CATS+ MASTER CONTRACT

In addition to the requirements of this TORFP, the Master Contractors are subject to all terms and conditions contained in the CATS+ RFP issued by the Maryland Department of Information Technology (DoIT) and subsequent Master Contract Project Number 060B2490023, including any amendments.

All times specified in this document are local time, defined as Eastern Standard Time or Eastern Daylight Time, whichever is in effect.

1.2   ROLES AND RESPONSIBILITIES

Personnel roles and responsibilities under the TO:

A. **TO Procurement Officer** – The TO Procurement Officer has the primary responsibility for the management of the TORFP process, for the resolution of TO Agreement scope issues, and for authorizing any changes to the TO Agreement.

B. **TO Contract Monitor** - The TO Contract Monitor on behalf of the Department has the primary responsibility for the management of the work performed under the TO Agreement, administrative functions, including issuing written directions, and for ensuring compliance with the terms and conditions of the CATS+ Master Contract. The TO Contract Monitor may designate one or more persons to act as his representative in connection with the foregoing activities (e.g. DHMH's Project Manager).

The TO Contract Monitor will assign tasks to the personnel provided under this TORFP and will track and monitor the work being performed through the monthly accounting of hours deliverable for work types; actual work produced will be reconciled with the hours reported.

C. **TO Contractor** – The TO Contractor is the CATS+ Master Contractor awarded this TO. The TO Contractor shall provide human resources as necessary to perform the services described in this TORFP Scope of Work.

D. **TO Contractor Manager** – The TO Contractor Manager will serve as primary point of contact with DHMH's Project Manager to regularly discuss progress of tasks, upcoming tasking, historical performance, and resolution of any issues that may arise pertaining to the TO Contractor Personnel. The TO Contractor Manager will serve as liaison between the TO Contract Monitor and the senior TO Contractor management.

E. **TO Contractor Personnel** – Any official, employee, agent, Subcontractor, or Subcontractor agents of the TO Contractor who is involved with the TO over the course of the TO period of performance.

F. **Key Personnel** – A subset of TO Contractor Personnel whose departure during the performance period, will, in the State's opinion, have a substantial negative impact on TO performance. Key personnel proposed as part of the TO Proposal shall start as of TO Agreement issuance unless specified otherwise in this TORFP or the Offeror's TO Technical Proposal. Key Personnel may be identified after TO award.

G. **Software Development Contractor** – The vendor, furnished under a different contract, responsible for software development of the LTSS system.

H. **DHMH's Technical Support Team** – DHMH personnel that provide technical support, monitoring and oversight of the LTSS System.

I. **DHMH's Project Manager** – DHMH resource responsible for day-to-day oversight of the overall activities and contractors that support the LTSS System.

1.3   TO AGREEMENT

Based upon an evaluation of TO Proposal responses, a Master Contractor will be selected to conduct the work defined in Section 3 - Scope of Work. A specific TO Agreement, Attachment 3, will then be entered into between the State and the selected Master Contractor, which will bind the selected Master Contractor (TO Contractor) to the contents of its TO Proposal, including the TO Financial Proposal.

1.4   TO PROPOSAL SUBMISSIONS

The TO Procurement Officer will not accept submissions after the date and exact time stated in the Key Information Summary Sheet above. The date and time of an e-mail TORFP submission is determined by the date and time of arrival of all required files in the TO Procurement Officer's e-mail inbox. In the case of a paper TO Proposal submission, Offerors shall take such steps necessary to ensure the delivery of the paper submission by the date and time specified in the Key Information Summary Sheet and as further described in Section 4.

Requests for extension of this date or time will not be granted. Except as provided in COMAR 21.05.03.02F, Proposals received by the TO Procurement Officer after the due date will not be considered.

1.5   ORAL PRESENTATIONS

All Offerors and proposed TO Contractor Personnel will be required to make an oral presentation to State representatives. Significant representations made by a Master Contractor during the oral presentation shall be submitted in writing. All such representations will become part of the Master Contractor's proposal and are binding, if the TO is awarded to the Master Contractor. The TO Procurement Officer will notify Master Contractor of the time and place of oral presentations.

1.6   QUESTIONS

All questions must be submitted via e-mail to the TO Procurement Officer no later than the date and time indicated in the Key Information Summary Sheet. Answers applicable to all Master Contractors will be distributed to all Master Contractors who are known to have received a copy of the TORFP.

The statements and interpretations contained in responses to any questions, whether responded to verbally or in writing, are not binding on the Department unless the RFP is expressly amended. Nothing in any response to any question is to be construed as agreement to or acceptance by the Department of any statement or interpretation on the part of the entity asking the question.

1.7   TO PRE-PROPOSAL CONFERENCE

A pre-proposal conference will be held at the time, date and location indicated on the Key Information Summary Sheet. Attendance at the pre-proposal conference is not mandatory, but all Master Contractors are encouraged to attend in order to facilitate better preparation of their proposals.

Seating at the pre-proposal conference will be limited to two (2) attendees per company. Attendees should bring a copy of the TORFP and a business card to help facilitate the sign-in process.

The pre-proposal conference will be summarized in writing. As promptly as is feasible subsequent to the pre-proposal conference, the attendance record and pre-proposal conference summary will be distributed via e-mail to all Master Contractors known to have received a copy of this TORFP.

In order to assure adequate seating and other accommodations at the pre-proposal conference, please e-mail the TO Procurement Officer indicating your planned attendance, no later than three (3) business days prior to the pre-proposal conference. In addition, if there is a need for sign language interpretation and/or other special accommodations due to a disability, please contact the TO Procurement Officer no later than five (5) business days prior to the pre-proposal conference. The TO Requesting Agency will make reasonable efforts to provide such special accommodation.

1.8   CONFLICT OF INTEREST

The TO Contractor shall provide IT technical and/or consulting services for State agencies or component programs with those agencies, and shall do so impartially and without any conflicts of interest. Each Offeror shall complete and include with its TO Proposal a Conflict of Interest Affidavit and Disclosure in the form included as Attachment 4 of this TORFP. If the TO Procurement Officer makes a determination that facts or circumstances exist that give rise to or could in the future give rise to a conflict of interest within the meaning of COMAR 21.05.08.08A, the TO Procurement Officer may reject an Offeror's TO Proposal under COMAR 21.06.02.03B.

Master Contractors should be aware that the State Ethics Law, Md. Code Ann., General Provisions Article, Title 5, might limit the selected Master Contractor's ability to participate in future related procurements, depending upon specific circumstances.

By submitting a Conflict of Interest Affidavit and Disclosure, the Offeror shall be construed as certifying all personnel and Subcontractors are also without a conflict of interest, as defined in COMAR 21.05.08.08A.

1.9   LIMITATION OF LIABILITY

The TO Contractor's liability is limited in accordance with Section 27 of the CATS+ Master Contract. TO Contractor's liability under Section 27(c) of the CATS+ Master Contract for this TORFP is limited to two (2) times the total TO Agreement amount.

1.10   CHANGE ORDERS

If the TO Contractor is required to perform work beyond the scope of Section 3 of this TORFP, or there is a work reduction due to unforeseen scope changes, a TO Change Order is required. The TO Contractor and TO Contract Monitor shall negotiate a mutually acceptable price modification based on the TO Contractor's proposed rates in the Master Contract and scope of the work change. No scope of work changes shall be performed until a change order is approved by DoIT and executed by the TO Procurement Officer.

1.11   TRAVEL REIMBURSEMENT

Expenses for travel performed in completing tasks for this TORFP shall not be reimbursed.

1.12   MINORITY BUSINESS ENTERPRISE (MBE)

This TORFP has MBE goals with no sub-goals as stated in the Key Information Summary Sheet above.

A Master Contractor that responds to this TORFP shall complete, sign, and submit all required MBE documentation at the time of TO Proposal submission (See Attachment 2 Minority Business Enterprise Forms and Section 4 TO Proposal Format and Submission Requirements). **Failure of the Master Contractor to complete, sign, and submit all required MBE documentation at the time of TO Proposal submission will result in the State's rejection of the Master Contractor's TO Proposal.**

In 2014, Maryland adopted new regulations as part of its Minority Business Enterprise (MBE) program concerning MBE primes. Those new regulations, which became effective June 9, 2014 and are being

applied to this task order, provide that when a certified MBE firm participates as a prime contractor on a contract, an agency may count the distinct, clearly defined portion of the work of the contract that the certified MBE firm performs with its own forces toward fulfilling up to fifty percent (50%) of the MBE participation goal (overall) and up to one hundred percent (100%) of not more than one of the MBE participation subgoals, if any, established for the contract. Please see the attached MBE forms and instructions.

1.12.1   MBE PARTICIPATION REPORTS

DHMH will monitor both the TO Contractor's efforts to achieve the MBE participation goal and compliance with reporting requirements.

A) Monthly reporting of MBE participation is required in accordance with the terms and conditions of the CATS+ Master Contract by the 15th day of each month.

B) The TO Contractor shall provide a completed MBE Prime Contractor Paid/Unpaid MBE Invoice Report (Attachment 2-4A) and, if applicable, MBE Prime Contractor Report (Attachment 2-4B) to the TO Requesting Agency at the same time the invoice copy is sent.

C) The TO Contractor shall ensure that each MBE subcontractor provides a completed Subcontractor Paid/Unpaid MBE Invoice Report (Attachment 2-5).

D) Subcontractor reporting shall be sent directly from the subcontractor to the TO Requesting Agency. The TO Contractor shall e-mail all completed forms, copies of invoices and checks paid to the MBE directly to the TO Contract Monitor.

1.13   VETERAN OWNED SMALL BUSINESS ENTERPRISE (VSBE)

This TORFP does not have a VSBE goal.

1.14   NON-DISCLOSURE AGREEMENT (TO CONTRACTOR)

Certain system documentation may be required by the TO in order to fulfill the requirements of the TO Agreement. The TO Contractor and TO Contractor Personnel who review such documents will be required to sign a Non-Disclosure Agreement (TO Contractor) in the form of Attachment 10.

1.15   LIVING WAGE

The Master Contractor shall abide by the Living Wage requirements under Title 18, State Finance and Procurement Article, Annotated Code of Maryland and the regulations proposed by the Commissioner of Labor and Industry.

All TO Proposals shall be accompanied by a completed Living Wage Affidavit of Agreement, Attachment 12 of this TORFP.

1.16   IRANIAN NON-INVESTMENT

All TO Proposals shall be accompanied by a completed Certification Regarding Investments in Iran, Attachment 15 of this TORFP.

1.17   CONTRACT MANAGEMENT OVERSIGHT ACTIVITIES

DoIT is responsible for contract management oversight on the CATS+ Master Contract. As part of that oversight, DoIT has implemented a process for self-reporting contract management activities of TOs under

CATS+. This process typically applies to active TOs for operations and maintenance services valued at $1 million or greater, but all CATS+ TOs are subject to review.

Attachment 11 is a sample of the TO Contractor Self-Reporting Checklist. DoIT may send initial checklists out to applicable/selected TO Contractors approximately three months after the award date for a TO. The TO Contractor shall complete and return the checklist as instructed on the form. Subsequently, at six month intervals from the due date on the initial checklist, the TO Contractor shall update and resend the checklist to DoIT.

1.18   MERCURY AND PRODUCTS THAT CONTAIN MERCURY

THIS SECTION IS NOT APPLICABLE TO THIS TORFP.

1.19   PURCHASING AND RECYCLING ELECTRONIC PRODUCTS

THIS SECTION IS NOT APPLICABLE TO THIS TORFP.

1.20   DEFINITIONS

Access	An ability or means to read, write, modify, or communicate data/information or otherwise use any information system resource
Business Day	Monday through Friday (excluding State holidays)
Data Breach	The unauthorized acquisition, use, modification or disclosure of Sensitive Data
Department of Health and Mental Hygiene (DHMH, or the Department)	The unit of the Executive Branch of Maryland State government issuing the TORFP
Electronic Data Interchange (EDI)	EDI is the electronic interchange of business information using a standardized format; a process which allows one company to send information to another company electronically rather than with paper.
Handle	(As relates to data) Collect, store, transmit, have access to data
Health Insurance Portability and Accountability Act (HIPAA)	HIPAA (1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
Information Technology (IT)	All electronic information-processing hardware and software, including: (a) maintenance; (b) telecommunications; and (c) associated consulting services
Local Time	Time in the Eastern Time zone as observed by the State of Maryland. Unless otherwise specified, all stated times shall be Local Time, even if not expressly designated as such

Long Term Supports & Services (LTSS) System	All services and activities necessary to fully support the LTSS System as an Information System, described as services and/or products in this TORFP, to include facilities, hardware, software, networking, security, monitoring, configuration services, a Help Desk, and non-technical items such as LTSS System operational activities, management and other manual processes. This definition of the LTSS System includes all System Source Materials developed as a result of this Task Order.
	
	All Upgrades and regulatory updates shall be provided at no additional cost to the State.
	
	In general (see Section 3.3 for further detail), the LTSS System includes the following:
	
	1) LTSS module
	  a) LTSS on-line application
	  b) Interfaces
	  c) Claims file processing
	  d) Batch transaction processing
	2) In-home Support Assurance System (ISAS) module
	  a) ISAS on-line application
	  b) Interactive Voice Response (IVR)
	  c) One Time Password (OTP)
	3) Primary and Secondary Data Centers
	  a) Hosting facilities and services
	  b) Network on Communications infrastructure and monitoring
	  c) Security Monitoring
	4) Help Desk
	5) LTSS Code Library

Normal State Business Hours	Normal State business hours are 8:00 a.m. – 5:00 p.m. Monday through Friday except State Holidays, which can be found at: www.dbm.maryland.gov – keyword: State Holidays
Notice to Proceed (NTP)	A written notice from the TO Procurement Officer that work on the Task Order, project or Work Order shall begin on a specified date. Additional NTPs may be issued by either the TO Procurement Officer or the TO Contract Monitor regarding the start date for any service included within this solicitation with a delayed or non-specified implementation date.
NTP Date	The date specified in an NTP for work on the Task Order, project or Work Order to begin
Offeror	A Master Contractor that submits a proposal in response to this TORFP
Personally Identifiable Information (PII)	Any information about an individual maintained by the State, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security

	number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information
Protected Health Information (PHI)	Information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Security Incident	A violation or imminent threat of violation of computer security policies, Security Measures, acceptable use policies, or standard security practices. "Imminent threat of violation" is a situation in which the organization has a factual basis for believing that a specific incident is about to occur.
Security or Security Measures	The technology, policy and procedures that a) protect and b) control access to networks, systems, and data
Sensitive Data	Means PII; PHI; information about an individual that (1) can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; (2) is linked or linkable to an individual, such as medical, educational, financial, and employment information; or other proprietary or confidential data as defined by the State, including but not limited to "personal information" under Md. Code Ann., Commercial Law § 14-3501(d) and Md. Code Ann., State Gov't § 10-1301(c).
Service Level Agreement (SLA)	Measurable levels governing TO Contractor performance and establishing associated liquidated damages for failure to meet those performance standards
SLA Activation Date	The date on which SLA charges commence under this Task Order, which may include, but not be limited to, the date of (a) completion of Transition In, (b) a delivery, or (c) releases of work.
State	The State of Maryland
Subcontractor	An agent, service provider, supplier, or vendor selected by the TO Contractor to provide subcontracted services or products under the direction of the TO Contractor or other Subcontractors, and including any direct or indirect Subcontractors of a Subcontractor. Subcontractors are subject to the same terms and conditions as the TO Contractor.

System Availability	The period of time the System will work as required including non-operational periods associated with reliability, maintenance, and logistics.
System Source Materials	Those materials necessary to wholly reproduce and fully operate the most current version of the System in a manner equivalent to the original System including, but not limited to: a) The executable instructions in their high level, human readable form and a version that is in turn interpreted, parsed and or compiled to be executed as part of the computing system ("source code"). This includes source code created by the Contractor or Subcontractor(s) and source code that is leveraged or extended by the Contractor for use in the project. b) All associated rules, reports, forms, templates, scripts, data dictionaries and database functionality. c) All associated configuration file details needed to duplicate the run time environment as deployed in the current deployed version of the system. d) All associated design details, flow charts, algorithms, processes, formulas, pseudo-code, procedures, instructions, help files, programmer's notes and other documentation. e) A complete list of third party, open source, or commercial software components and detailed configuration notes for each component necessary to reproduce the system (e.g., operating system, relational database, and rules engine software). f) All associated user instructions and/or training materials for business users and technical staff
Task Order (TO)	The scope of work described in this TORFP
TO Agreement	The contract awarded to the successful Offeror pursuant to this Task Order Request for Proposals, the form of which is attached to this TORFP as Attachment 3
TO Proposal	As appropriate, either or both an Offeror's Technical or Financial Proposal to this TORFP
TO Request for Proposals (TORFP)	This Task Order Request for Proposal, including any amendments / addenda thereto
Technical Safeguards	The technology and the policy and procedures for its use that protect Sensitive Data and control access to it
Total Proposal Price	The Offeror's total proposed price for products/services proposed in response to this solicitation, included in the TO Price Sheet, and used in the financial evaluation of TO Proposals

Upgrade	A new release of any COTS component of the System containing major new features, functionality and/or performance improvements.
Veteran-owned Small Business Enterprise (VSBE)	A business that is verified by the Center for Verification and Evaluation (CVE) of the United States Department of Veterans Affairs as a veteran-owned small business. See Code of Maryland Regulations (COMAR) 21.11.13 and http://www.vetbiz.gov.
Work Order	A subset of work authorized by the TO Contract Monitor performed under the general scope of this TORFP, which is defined in advance of fulfillment, and which may not require a change order. Except as otherwise provided, any reference to the TO shall be deemed to include reference to a Work Order.
Working Day(s)	Same as "Business Day"

1.21   ACRONYMS

ADC	Annapolis Data Center
AES	Advanced Encryption System
AFF	Advanced File Format
AICPA	American Institute of Certified Public Accountants
ANSI	American National Standards Institute
API	Application Program Interface
AUS	Acceptable Use Policy
BI	Brain Injury
BIP	Balancing Incentive Program
CAP	Corrective Action Plan
CATS+	Consulting and Technical Services Plus
CCW	Change Control Workgroup
CFC	Community First Choice
CIFS	Common Internet File Services
Cisco ASA	Cisco Advanced Security Appliance
Cisco ASR	Cisco Application Specific Router
Cisco UP	Cisco Unified Process
CM	Case Manager
CO	Community Options
COMAR	Code of Maryland Regulations
COOP	Continuity of Operations Plan

COTS	Commercial Off-The-Shelf
CPAS	Community Personal Assistance Services
CPU	Central Processing Unit
DB	Database
DBMS	Database Management System
DDA	DHMH's Developmental Disabilities Administration
DHMH	Maryland's Department of Health and Mental Hygiene
DMZ	De-militarized Zone
DoIT	Maryland's Department of Information Technology
DPAF	Deliverable Product Acceptance Form
DR	Disaster Recovery
DRS	Distributed Resource Scheduling
EDI	Electronic Data Interchange
EPSDT	Early and Periodic Screening, Diagnosis and Treatment Program
ESXi	Elastic Sky X Interchange
ETL	Extraction, Transformation and Loading
EULS	End-User License Agreement
EVV	Electronic Visit Verification
FAQs	Frequently Asked Questions
FAS	Fabric Attached Storage
FCoE	Fiber Channel Over Ethernet
FIPS	Floating Point Instructions Per Second
FIPS	Federal Information Processing Standards
FW	Firewall
GB	Gigabytes
Gbps	Gigabytes Per Second
GHz	GigaHertz
HA	High Availability
HID	Host Intrusion Detection
HIPAA	Health Information Portability and Accountability Act
HRST	Health Risk Screening Tool
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IO	Input / Output

IOPS	Input / Output Operations Per Second
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IRS	Internal Revenue Service
ISAS	Information Systems Analytics and Synthesis
ISAS	In-home Support Assurance System
iSCSI	Internet Small Computer Systems Interface
IT	Information Technology
ITPO	Information Technology Procurement Office
IV&V	Independent Verification and Validation
IVR	Integrated Voice Response
KPI	Key Performance Indicator
LAN	Local Area Network
LFF	Large Form Factor
LTSS	Long-Term Supports and Services System
MA	Medical Assistance
MBE	Minority Business Enterprise
Mbps	Megabytes Per Second
MDC	Medical Day Care
MDM	Master Data Management
MDOT	Maryland Department of Transportation
MDS	Managed Dedicated Server
MDS	Minimal Data Set
MFP	Money Follows the Person
MHz	MegaHertz
MITDP	Major Information Technology Development Project
MMIS	Medicaid Management Information System
MS	Microsoft
NAS	Network Attached Storage
NetApp	Network Applications
NFS	Network File System
NIST	National Institute of Standards and Technology
NOC	Network Operations Center

NTP	Notice to Proceed
O&M	Operations and Maintenance
OHS	DHMH's Office of Health Services
OPASS	DHMH's Office of Procurement and Support Services
OTP	One-Time Password
PHI	Protected Health Information
PII	Personally Identifiable Information
PKI	Performance Key Indicators
PMI	Project Management Institute
PMP	Project Management Plan or PMI's Project Management Professional
POS	Plan of Service
PP	Provider Portal
QoS	Quality of Service
QS	Quality Surveys
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RAM	Resident Access Memory
RAM	Random-Access Memory
RCA	Root Cause Analysis
RE	Reportable Events
REM	Rare and Expensive Medical
RPO	Recovery Performance Object
RTO	Retransmission Time Out
SAN	Storage Area Network
SATA	Serial Advanced Technology Attachment
SDLC	Software Development Life Cycle
SFF	Small Form Factor
SFTP	Secured File Transfer Protocol
SIOC	Serial Input / Output Controller
SIS	Support Intensity Scale
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOC	Security Operations Center or Service Organization Control
SQL	Structured Query Language

SSD	Solid State Drive
SSO	Single Sign-On
SSRS	SQL Server Reporting Services
SysLog	System Log
TB	Terabyte
TEFT	Testing Experience and Functional Tools
TO	Task Order
TORFP	Task Order Request for Proposal
TOP	Technical Operations Plan
UCS	Unified Computing System
UPS	Uninterruptible Power Source
URL	Internet File Name Extension
VAAI	VStorage Application Program Interface for Array Integration
vLAN	Virtual Local Area Network
VM	Virtual Machines
VMware	Virtual Machine File System
vNIC	Virtual Network Interface Controller
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VSBE	Veteran-Owned Small Business Enterprise
WAN	Wide Area Network
WBS	Work Breakdown Structure

1.22   HIPAA - Business Associate Agreement

Based on the determination by the Department that the functions to be performed in accordance with this solicitation constitute Business Associate functions as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the recommended awardee shall execute a Business Associate Agreement as required by HIPAA regulations at 45 C.F.R. §164.500 *et seq.* and set forth in **Attachment 19**. This Agreement must be provided within five (5) Business Days of notification of proposed TO Agreement award. However, to expedite processing, it is suggested that this document be completed and submitted with the TO Technical Proposal. Should the Business Associate Agreement not be submitted upon expiration of the five (5) Business Day period as required by this solicitation, the TO Procurement Officer, upon review of the Office of the Attorney General and approval of the Secretary, may withdraw the recommendation for award and make the award to the responsible Offeror with the next highest overall-ranked TO Proposal.

1.22.1   Compliance with Federal HIPAA and State Confidentiality Law

1.22.1.1   The TO Contractor acknowledges its duty to become familiar with and comply, to the extent applicable, with all requirements of the federal Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d et seq., and implementing regulations including 45 C.F.R. Parts 160 and 164. The TO Contractor also agrees to comply with the Maryland Confidentiality of Medical Records Act (MCMRA), Md. Code Ann. Health-General §§ 4-301 et seq. This obligation includes:

(a)   As necessary, adhering to the privacy and security requirements for protected health information and medical records under HIPAA and MCMRA and making the transmission of all electronic information compatible with the HIPAA requirements;

(b)   Providing training and information to Contractor Personnel regarding confidentiality obligations as to health and financial information and securing acknowledgement of these obligations from Contractor Personnel to be involved in the TO Agreement; and

(c)   Otherwise providing good information management practices regarding all health information and medical records.

1.22.1.2   Based on the determination by the Department that the functions to be performed in accordance with the scope of work set forth in the solicitation constitute business associate functions as defined in HIPAA, the TO Contractor shall execute a business associate agreement as required by HIPAA regulations at 45 C.F.R. 164.501 and in the form as required by the Department.

1.22.1.3   "Protected Health Information" as defined in the HIPAA regulations at 45 C.F.R. 160.103 and 164.501, means information transmitted as defined in the regulations, that is individually identifiable; that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and that is related to the past, present, or future physical or mental health or condition of an individual, to the provision of healthcare to an individual, or to the past, present, or future payment for the provision of healthcare to an individual. The definition excludes certain education records as well as employment records held by a covered entity in its role as employer.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 2 - COMPANY AND PERSONNEL QUALIFICATIONS

2.1 MINIMUM QUALIFICATIONS

2.1.1 OFFEROR'S COMPANY MINIMUM QUALIFICATIONS

No Company minimum qualifications.

2.1.2 OFFEROR'S PERSONNEL MINIMUM QUALIFICATIONS

Only those Master Contractors supplying proposed Key Personnel that fully meet all minimum qualification criteria shall be eligible for TORFP proposal evaluation.

The Key Personnel proposed under this TORFP must meet all minimum qualifications for the labor category proposed, as identified in the CATS + Master Contract Section 2.10, shown below. Resumes shall clearly outline starting dates and ending dates for each applicable experience or skill.

Master Contractors may only propose **four (4) Key Personnel** in response to this TORFP. All other planned positions shall be described generally in the Staffing Plan, and may not be used as evidence of fulfilling company or personnel minimum qualifications.

Job Description	Minimum Qualifications
Project Manager	**CATS+ Labor Category:** Project Manager **Education:** Bachelor's Degree from an accredited college or university in Engineering, Computer Science, Information Systems, Business or other related discipline. **General Experience:** At least five (5) years of experience in project management. **Specialized Experience:** At least five (5) years of experience in managing IT related projects and must demonstrate a leadership role in at least three successful projects that were delivered on time and on budget.
Help Desk Lead	**CATS+ Labor Category:** To be proposed in TORFP Technical Proposal **Based on the labor category selected**
Operations Lead	**CATS+ Labor Category:** To be proposed in TORFP Technical Proposal **Based on the labor category selected**
Technical Infrastructure Lead	**CATS+ Labor Category:** Network Technician (Senior) **Education:** An Associate's degree from an accredited college or university in Computer Science, Information Systems, Engineering or a related field; or Technical 'school certificate of completion in the data communications field including cable installation; or the equivalent military training. Two (2) additional years of specialized experience may be substituted for the required education. **General Experience:** Seven (7) years of experience in a computer-related field. **Specialized Experience:** Five (5) years of experience in the following areas: Installation, operation, and maintenance of data communication networks and devices.

In addition to the four (4) named resources, the Offeror shall demonstrate in its proposal the ability to fully support the scope of work in this TORFP through other skilled resources. The Offeror shall demonstrate a team-oriented approach and be able to fully staff all required resources.

2.2 OFFEROR AND PERSONNEL EXPERIENCE

2.2.1 Offeror Experience

The following TO Contractor company experience will be evaluated as part of the TO Technical Proposal.

The breadth and prior experience within the last seven (7) years in the following;

A) Prior experience furnishing Tier 1 Help Desk support. Experience furnishing such services at organizations with more than 1,000 end-users and/or with multiple full-time personnel will be given greater weight.

B) The extent to which the Offeror has demonstrated prior experience furnishing web-based application services hosting within the United States. Experience that includes both high availability and IVR will be given greater weight than those with one or neither.

C) The extent of experience with healthcare claims file processing, including use of COTS software capabilities to support balancing and reconciliation reporting, as well as troubleshooting at the batch file and/or individual claim levels. Experience with system transactions using EDI HIPAA X12 formats and data exchanges with other external systems will be given greater weight.

D) Prior experience providing COTS hardware and software services in a hosted environment. Experience as an application service provider for a technical solution similar in size, complexity and scope to the LTSS System, as described in Section 3.3, will be given greater weight.

E) Prior experience performing software releases and technical infrastructure maintenance and patch installations.

2.2.2 Offeror Personnel Experience

The following TO Contractor personnel experience will be evaluated as part of the TO Technical Proposal.

Job Description	Experience
Project Manager	Experience with any of: a. PMP Certification b. Leadership role on projects similar to the scope of work for this TORFP c. Leadership role in government (local, state or federal) IT-related project(s)
Help Desk Lead	Experience with any of: a. Help Desk operations, management and reporting b. Healthcare claims processing c. Care management systems or other relevant healthcare solutions
Operations Lead	Experience with any of: a. Data processing operations b. Healthcare claims processing operations c. COTS software that supports claims-related automated balancing and reconciliation capabilities d. Care management systems or other relevant healthcare solutions

Job Description	Experience
Technical Infrastructure Lead	Experience with any of: a. Virtualized Server configuration b. Microsoft .NET c. IBM Connect:Direct with Secure+ d. RavenDB or similar NoSQL database

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 3 - SCOPE OF WORK

3.1   PURPOSE

DHMH is issuing this CATS+ TORFP to obtain one (1) Master Contractor who shall provide managed hosting services and operations services for DHMH's Long Term Services & Supports (LTSS) System, in accordance with the scope of work described in this Section 3. The compiled code for the LTSS System's software shall be provided by DHMH and installed by the TO Contractor.

In addition to the managed hosting services, the TO Contractor shall provide an LTSS System Help Desk, manage LTSS System user credentialing, perform secure data replication, perform batch processing, manage and support current and future external connections, and process interface transactions that include batch processing of files for claims activity, eligibility updates, provider updates, data imports/exports and other interfaces as required.

It is crucial that the TO Contractor work closely with the Software Development Contractor to ensure a seamless, integrated approach to delivering functionality and support for the LTSS System.

As part of the evaluation of the proposal for this TO, **Master Contractors shall propose exactly four (4) named resources** and shall describe in a Staffing Plan how additional resources shall be acquired to meet the needs of the TO Requesting Agency. All planned positions other than the four named resources shall be described generally in the Staffing Plan, and may not be used as evidence of fulfilling company or personnel minimum qualifications.

This procurement shall result in a fixed-price TO Agreement between DHMH and the TO Contractor. The pricing covers the following components:

a. **Start-up Period** – a fixed-price deliverable that includes all activity from Notice to Proceed (NTP) until the cutover from the current O&M contractor to the TO Contractor has been approved by DHMH. DHMH requires cutover to occur within the first one hundred fifty (150) calendar days or earlier as more fully described in Section 3.6.3. Initial start-up includes establishing a new technical infrastructure for the LTSS System as described in the requirements.

b. **Managed Hosting Services** – a monthly recurring fixed price that includes all COTS software, hardware, and networking technologies to provide managed hosting services for DHMH's LTSS System, supporting additional LTSS modules as they are moved to production.

c. **Operations** – a monthly recurring fixed price that includes all operational tasks, processes, tools and resources to support healthcare claims and interfaces, as well as Help Desk functions.

d. **Additional Services** – The TO Contractor shall provide Additional Services, as authorized through the Work Order Process, as described in Section 3.9, and Change Control Process, as described in Section 3.6.1.3. The Additional Services may be on a one-time or recurring monthly basis.

DHMH intends to award this Task Order to one (1) Master Contractor that proposes a team of resources and a Staffing Plan that can best satisfy the TO requirements.

3.2   REQUESTING AGENCY BACKGROUND

Starting in 2012, Maryland embarked on a transformation of its Maryland Medical Assistance Program (Medicaid) Long Term Supports and Services (LTSS) system. The LTSS web application is a care management system that supports more than ten thousand Medicaid participants in receiving high-quality, well-coordinated LTSS services. Case managers, nurse monitors, Medicaid providers, and DHMH use the LTSS application to manage participant care including eligibility, assessment, enrollment, service planning,

service provision, service billing, incident management, and quality monitoring. In addition to care management, the state uses a piece of the LTSS application called ISAS for Electronic Visit Verification (EVV) and billing. Caregivers record their visits through an Integrated Voice Response (IVR) system, and visits are matched against the participant and provider data stored in LTSS. ISAS automatically generates pre-authorized visits into claims and submit claims to the Medicaid Management Information System (MMIS). LTSS and ISAS are a crucial part of the Medicaid LTSS program, and continue to grow and evolve as the needs of the program change.

The need for flexible, responsive technology to manage large volumes of data related to participant application, enrollment, and participation in LTSS is vital to the success of the Medical LTSS program. Federal requirements for quality monitoring and assurance cannot be met without technology support to gather, manage, and analyze data. To meet the need for technology, DHMH has integrated multiple programs to form the LTSS System. At this time, the LTSS System supports the Money Follows the Person (MFP) Demonstration, Waiver for Brain Injury (BI), Community Options Waiver (CO), Community Personal Assistance Services (CPAS), and Community First Choice (CFC). DHMH is continuing to grow the programs that are integrated into the LTSS application and will add the Medical Day Care Waiver (MDC) and the Developmental Disabilities Administration (DDA) program, among other programs.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

3.3   PROJECT BACKGROUND

The current LTSS System is the enabling technology platform with capabilities that support case management and pre-authorization of services for many of DHMH's Medicaid Waiver programs. The Medicaid Waiver programs are delivered utilizing the modular development concept. The LTSS System is a custom-developed software solution for the State of Maryland designed to be expanded to support DHMH's various business units. As such, modification and expansion of the underlying technology (e.g. custom and COTS software, networking gear, hardware and other technical infrastructure elements) are integral elements that support the expanding business functionality in the LTSS System.

The LTSS System is designed using the module concept. Several modules already reside in the production system, several modules are in progress and more are planned for the future. Additional modules may be necessary, pending legislative, regulatory and/or business need.

Current Live LTSS System Modules:
- CO Waiver
- CPAS Waiver
- CFC Waiver
- BI Waiver
- MDC Waiver

Current Live LTSS System Capabilities:
- Single Sign-on (SSO)
- Screening
- Assessment
- Registry
- Eligibility and Enrollment
- Plan of Service (POS)
- In-home Support Assurance System (ISAS), including these key components:
  - Integrated Voice Response (IVR)
  - One-Time Password (OTP)
  - Service Provider Billing
- Case Manager (CM) Billing
- Quality Surveys (QS)
- Reportable Events (RE)

Current Interfaces:
- Minimal Data Set (MDS) files, received from DHMH's Office of Health Care Quality (OHCQ) and processed via automated batch
- Medicaid Management Information System (MMIS) Provider and Recipient files

- Monthly Hilltop Institute database copy, via automated batch process that produces copy of the LTSS database that is automatically placed on an FTP server
- MMIS Eligibility files
- MMIS claims-related files

Under development and planned LTSS modules and system capabilities:
- Provider Portal (PP)
- Testing Experience and Functional Tools (TEFT) Web Tool
- TEFT Telephone Tool (via IVR) – note: this is an optional capability and DHMH will determine within sixty (60) calendar days from NTP if this initiative is to be implemented
- MDC Module additional functions
- DDA's program in multiple phases

Other modules and system capabilities under consideration:
- Service provider activity file transfer
- Service provider activity via mobile application
- Autism Waiver
- Rare and Expensive Medical (REM)
- Model Waiver
- Early and Periodic Screening, Diagnosis, and Treatment Program (EPSDT)

The LTSS System is a highly secure, available, reliable and scalable software solution that supports business operations on a 24x7x365 basis. Users of the LTSS System's online interface fall into two

categories – a.) Transactional Users perform business functions on a daily basis; and, b.) Self-service Users lookup relevant information predominantly in a browse mode through specifically designed web screens.

3.3.1 The current LTSS System software layer includes the following:

COTS Software:
- Microsoft Windows Server Data Center Edition
- Reporting and Ad Hoc Database – Microsoft SQL Server Standard (includes SSRS)
- Transaction Database – RavenDB Standard Plus, and Enterprise editions
- IBM Sterling Connect: Direct Standard Edition with Secure+
- VMware vSphere Enterprise Plus
- vCloud Suite
- Veeam Availability Suite v9
- Shavlik Protect
- SolarWinds Network Performance Monitor
- SolarWinds Application Performance Monitor
- Zenoss Enterprise
- Microsoft Operations Management 2016
- BlazeMeter
- Splunk
- Ndatalign

Custom-developed Software:
- ~ 1.6 million lines of custom code
- ~ 700 forms
- ~ 1700 screens
- ~ 182 reports (not including ad hoc reports)

3.3.2 Required Technical Infrastructure

The current LTSS System's technical infrastructure is deemed unable to support the future business needs and it cannot be incrementally expanded. DHMH developed a Technical Infrastructure Design (Attachment 20) for the purpose of supporting the LTSS System based on planned future business operations. Attachment 20Technical Infrastructure Design is a completely new LTSS System technical infrastructure that incorporates the lessons learned from the current infrastructure; however, none of the current hardware, COTS software or other infrastructure is transferrable for use in meeting the requirements of this TORFP.

The Technical Infrastructure Design provides a scalable solution for the LTSS System to meet business needs. The Technical Infrastructure Design establishes a BASE-level of functionality and then provides additional infrastructure specifications that are planned to meet EXPANDED volumes, as described in the table below. DHMH may choose to implement the EXPANDED solution at the time of the award of the TO Agreement; or, schedule the expansion to the BASE-level for a future date.

Item	Volume	Measurement	Reference
IVR Calls	600,000 Minimum	Per Month	3.6.5.5
Unique Active LTSS System Online Transactional Users	2,000 Minimum 3,000 EXPANDED	Point-in-time	3.6.5.8
New and Adjusted Claims	1.5 Million Minimum 3 Million EXPANDED	Per Month	3.6.6.1
Software Releases	12 Minimum	Per Year	3.6.6.3
Unique Help Desk Inquiries	1,500 Minimum	Per Month	3.6.6.21

At a high-level, there are two (2) data centers – the Primary Data Center and a Secondary Data Center. The Primary Data Center includes the production environment to support live business activity, as well as a pre-

production environment used to regression test LTSS System software releases prior to deployment to the production environment. The Secondary Data Center is the designated Disaster Recovery (DR) site. Both environments have a management environment used to support the LTSS System. The diagram below represents the BASE-Level as well as the EXPANDED requirements, which are described in detail in Attachment 20 Technical Infrastructure Design.

LTSS Infrastructure Diagram for BASE-Level Requirements
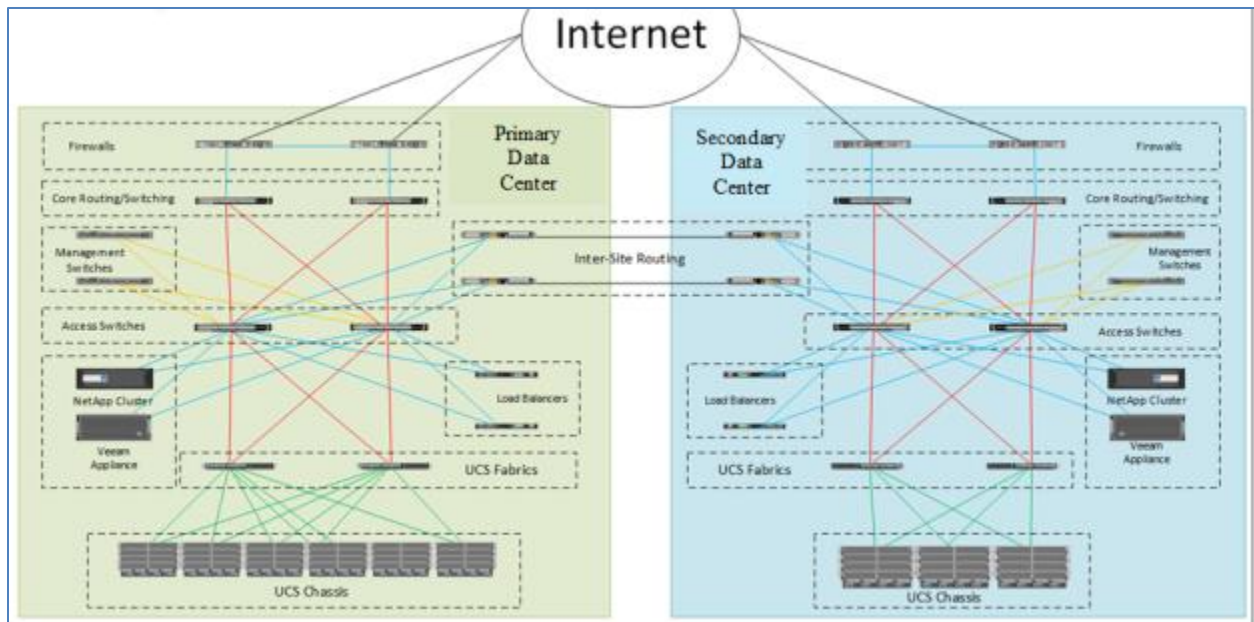
LTSS Infrastructure Diagram for EXPANDED Requirements
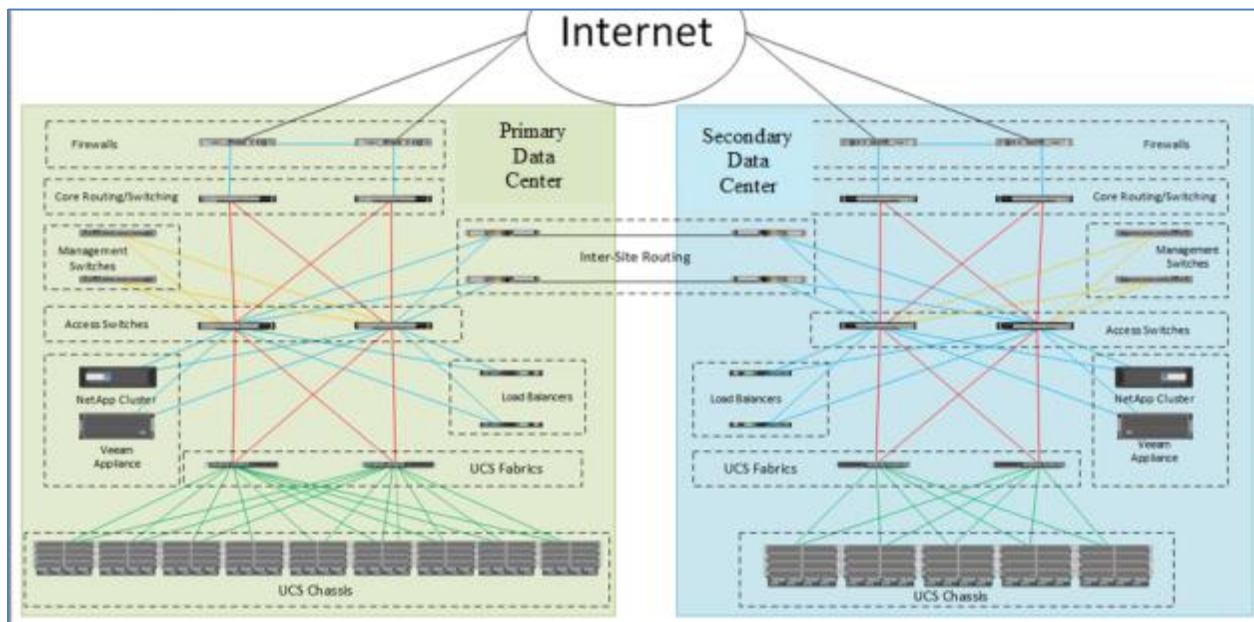
3.4   PROFESSIONAL DEVELOPMENT

Any TO Contractor Personnel provided under this TORFP shall maintain any required professional certifications for the duration of the resulting TO.

3.5   REQUIRED POLICIES, GUIDELINES AND METHODOLOGIES

The TO Contractor shall comply and remain compliant with all applicable laws, regulations, policies, standards, and guidelines affecting information technology and technology projects, which may be created or changed periodically.

The TO Contractor shall adhere to and remain compliant with current, new, and revised laws, regulations, policies, standards and guidelines affecting security and technology project execution.

The foregoing may include, but are not limited to, the following policies, guidelines and methodologies that can be found at the DoIT site (http://doit.maryland.gov/policies/Pages/ContractPolicies.aspx).

    A. The State of Maryland System Development Life Cycle (SDLC) methodology
    B. The State of Maryland Information Technology Security Policy and Standards
    C. The State of Maryland Information Technology Non-Visual Access Standards
    D. The TO Contractor shall follow project management methodologies consistent with the Project Management Institute's Project Management Body of Knowledge Guide.
    E. TO Contractor assigned personnel shall follow a consistent methodology for all TO activities.
    F. The State's Information Technology Project Oversight Policies for any work performed under this TORFP for one or more Major IT Development Projects (MITDPs)

3.6   REQUIREMENTS

    A. **Start-up Period (One-time Fixed Price)**

1. The TO Contractor shall coordinate transition activities in collaboration with DHMH, the current O&M contractor and Software Development Contractor.

2. The TO Contractor shall confirm the Technical Infrastructure Design (Attachment 20), noting any exceptions, improvements, adjustments and/or deviations deemed necessary or that may provide added value to the overall LTSS System technical solution.

3. The TO Contractor shall establish the technical environment meeting the specifications in the Technical Infrastructure Design and recommended changes approved by DHMH.

4. The TO Contractor shall perform all necessary activities to prepare for, test and certify the LTSS System as ready for cutover to the TO Contractor's responsibility within one hundred fifty (150) days of the NTP. See Start-up Period requirements in Section 3.6.3.

5. The TO Contractor shall coordinate go / no go decision with DHMH regarding the (OPTION) TEFT IVR capability within sixty (60) calendar days from the NTP. See Requirement 3.6.5.5(b) and Attachment 22 TEFT IVR Proposed Call Flow.

    B. **Managed Hosting Services (Fixed Price on a Monthly basis)**

For the LTSS System, the TO Contractor shall provide managed hosting services for DHMH's LTSS System, including all necessary COTS software, hardware and networking technologies. DHMH shall provide the compiled code for the LTSS System's applications.

    C. **Operations (Fixed Price on a Monthly basis)**

The TO Contractor shall provision and manage the LTSS Help Desk and address all tier 1 and some tier 2 inquiries (excluding software development escalated inquiries), manage user credentialing, deploy LTSS System software releases in all environments, process interface transactions that include processing of files for claims activity, eligibility updates, provider updates, data imports/exports and other interfaces as required, and provide backup and disaster recovery services.

EXPANDED services, should they be authorized by the Department, shall follow a similar development and deployment process as for initial service setup during the Start-Up period. Invoicing for expanded services shall not commence until the Department's acceptance that the service is ready for production use.

D. Additional Services (Fixed Price basis)

The TO Contractor shall provide Additional Services, as authorized through the Work Oder Process, as described in Section 3.9, and Change Request Process, as described in Section 3.6.1.3. The Additional Services may be on a one-time or recurring monthly basis as described in the Work Order or Change Order.

Additional Services are intended to address, but not be limited to, the following situations:
   a. Activity beyond the established minimum volume levels for claims, Help Desk inquiries and/or IVR calls,
   b. Expansion of the technical infrastructure to support business needs,
   c. Enhancements to the LTSS System to mitigate risks and/or improve functionality,
   d. New technical capabilities to support business needs,
   e. Modifications to the technical solution and/or operations to support DHMH requirements, and
   f. Regulatory or other compliance related changes.

Below are examples of possible Additional Services:
   1. Incremental Services
       a. Incremental Claims Volume above threshold (assessed each month)
       b. Incremental Help Desk Inquiry Volume above threshold (assessed each month)
       c. Incremental IVR Call Volume above threshold (assessed each month)
   2. Managed Hosting Services
       a. Additional Compute
       b. Additional Storage
       c. Additional External Connections
       d. New and/or Additional COTS licenses
   3. One-time Services – includes planning, requirements, design, development, testing, implementation and other tasks necessary to support modifications to the LTSS System and/or operations.
       a. Analysis, planning, requirements, design and implementation of Technical Infrastructure Changes, including the following:
           i. Enable external systems to interface with LTSS (e.g. provider systems submitting files or via web service or comparable data exchange capability)
               1. Interface specifications
               2. External submitter enablement planning and/or design
               3. Gateway considerations
               4. Software options analysis
               5. Hardware and infrastructure analysis
               6. Operations analysis

       7. Other services, hardware and/or COTS software considerations as necessary

    ii. Replacement of the current Single Sign-on (SSO) software application

    iii. Replacement of the custom-developed claims translator with a COTS software solution

    iv. Installation of a new COTS software solution for Master Data Management (MDM) or File Transfer

    v. Migration from the current Database Management Systems (DBMS) to new platform(s)

    vi. Additional COTS software as required

  b. Increasing capabilities that may require TO Contractor to acquire additional hardware and COTS software, along with integration services for LTSS System expansion

  c. Changes to existing and/or new external Interfaces

  d. Other changes to meet State and/or federal mandates

E. OPTIONAL Database Support Services (Fixed Price on a Monthly basis)

For Database Support Services, DHMH does not require prospective TO Contractors to offer these services or propose a solution and pricing. For Offerors offering these services, the TO Technical Proposal should provide sufficient detail to ensure DHMH can evaluate the prospective TO Contractor's ability to support the LTSS System's database and data management activities effectively. Database Support Services include the following tasks on a Monthly basis:

1. Support for the Transactional DBMS – RavenDB
2. Support for the Reporting DBMS – Microsoft's SQL Server
3. Support for the Ad Hoc Reporting – Microsoft's SSRS
4. Manually processed data exports for external stakeholders
5. Tier 2 Help Desk inquiries related to data and/or database issues
6. Database server setup, software installation, configuration, monitoring and support
7. Coordination with DHMH and the Software Development TO Contractor

F. (OPTION) TEFT IVR implementation (Fixed Price basis)

At the Department's sole option and discretion, the full implementation of the TEFT IVR in support of the LTSS may be requested. Invoicing for TEFT IVR shall not commence until written acceptance from the Department that the service is ready for production usage. See Attachment 22 TEFT IVR Proposed Call Flow and Section 3.6.5.5(b) that describes the scope of TEFT IVR implementation.

3.6.1   TO CONTRACTOR RESPONSIBILITIES

The TO Contractor shall provide staffing and resources to fully supply the following services as identified in this Section 3.6 Requirements:

3.6.1.1.   Physical Office Requirements

  a. The TO Contractor shall maintain a physical office within the continental United States.

  b. TO Contractor and Subcontractors shall conduct all LTSS System work within the United States and include in the TO Technical Proposal all locations where work is to be performed and the nature of the work at each location. TO Contractor shall provide an address, phone number and a contact person for each location.

  c. The TO Contractor shall not process, transfer or store LTSS data under the services of this TO outside the United States.

3.6.1.2.   LTSS System Custom Software Release Execution
   a. The TO Contractor shall confirm DHMH deployment approval prior to deploying any software release.
   b. The TO Contractor shall execute deployment activities, actively communicating with DHMH throughout the deployment, including confirmation that the software release has been deployed successfully and, when the deployment is in the pre-production environment or production environment, is ready for DHMH and or its designee(s) to validate the functions.
   c. The TO Contractor shall establish and follow rollback procedures if the back out of a software release is necessary. These rollback procedures shall include communications, vetting and approval flow with the involvement of the TO Contractor, DHMH and the Software Development Contractor, as necessary.
   d. The TO Contractor shall closely monitor system performance for a period of time appropriate for each software release, longer for major releases. This monitoring shall include:
      i.   End user ability to access and login
      ii.   System response time
      iii. Availability of data in ad hoc reporting system
      iv.   Batch processing performance
      v.   Other system performance monitoring as mutually agreed upon
   e. TO Contractor may be required to deploy changes outside Normal State Business Hours.

3.6.1.3.   Change Control Process
   a. The Change Control Workgroup (CCW) is a joint group with responsibility for all aspects of the LTSS System. The CCW is led by DHMH personnel and includes participation from the Software Development Contractor and the TO Contractor. The CCW will maintain a change control tracker (e.g., MS Excel spreadsheet of potential changes that could impact the system's software, hardware or configuration). The change control tracker uniquely identifies the TO Contractor-related CCW item with a tracking number, brief description, long description, disposition (e.g. pending, approved, deferred, rejected, deployed), proposed cost, estimate breakdown, priority (1-critical, 2-high, 3-medium, and 4-low), rank, reported by, assigned to, key dates (e.g. identified, submitted to DHMH, approved by DHMH, deployed), notes/comments, and other fields as mutually agreed upon by DHMH and the TO Contractor.
   b. The TO Contractor shall record details of O&M changes using the change control tracker described in item "a" above.
   c. The TO Contractor shall participate in CCW meetings conducted at least once per month or at DHMH's request. The CCW will include DHMH's TO Contract Monitor, DHMH's Project Manager and representatives from key stakeholder groups, as unilaterally determined by DHMH. TO Contractor will typically be represented by the TO Contractor Manager as the required CCW member. Other TO Contractor Personnel shall be made available, as necessary, to facilitate productive execution of the CCW.
   d. TO Contractor shall follow the CCW process to request approval from DHMH in advance of making any changes. No change to the LTSS System shall be implemented without prior DHMH approval of the concept, approach, impact assessment and schedule.
   e. The list of candidate CCW items shall include enough information for the CCW to determine if the TO Contractor is required to submit a formal change request for an item.
   f. CCW will review proposed change requests. If approved, the TO Contractor shall provide a target completion date and provide updates to DHMH's Project Manager on all change requests in process.

g. The TO Contractor shall provide a Change Request Summary that includes the unique tracking number, short description, cost (if applicable), date submitted, date approved, current status, approved date, completion date and any relevant notes or comments. The TO Contractor shall provide a summary of the total cost and quantity of all approved/deployed change requests. "No Cost" change requests are also to be submitted for review and approval by the CCW.

h. For all CCW items implemented, the TO Contractor shall provide a thirty (30) calendar day post-launch warranty period, where the change request is free of defects, before billing for the item. Significant defects addressed during the warranty period reset the warranty period, based on the implementation date of the fix.

3.6.1.4.   LTSS System's Code Library

a. The TO Contractor shall furnish and manage a code library for compiled code and all associated documentation (including release notes and any deployment procedures) for the LTSS applications software and maintain them in a code library.

b. The TO Contractor shall coordinate with the Software Development Contractor for the transfer of releases and release documentation for each software release.

c. The TO Contractor shall ensure the System Source Materials are not made available to any party other than DHMH, except as directed in writing by DHMH.

d. The TO Contractor is responsible for labeling all documentation and code with the appropriate release numbering.

e. The TO Contractor shall make System Source Materials available to DHMH upon written request, within a mutually agreed upon timeframe.

3.6.1.5.   Additional Responsibilities

a. TO Contractor shall provide timely (e.g., typically within one (1) week, at the discretion of DHMH) and thorough response to Corrective Action Plans (CAPs), as required by DHMH, including completion of remediation tasks identified in the CAP and/or TO Contractor's response to the CAP, which could be initiated to remedy a contractual or TO Contractor performance issue or as an outcome from an Independent Verification & Validation (IV&V) or other audit or review.

b. End-of-Contract Transition: DHMH requires TO Contractor to collaborate with a successor contractor over a one hundred fifty (150) day transition period. TO Contractor shall provide the End of Contract Transition Plan five (5) months before the end of the TO Agreement term to ensure a quality, smooth, efficient, and timely data transition to the DHMH or DHMH's agents before the end of the TO Agreement. Near the end of the TO Agreement term, at a time requested by DHMH, the TO Contractor shall support end-of-Contract transition efforts with technical, business, and project support.

3.6.2   TO CONTRACTOR PERSONNEL DUTIES AND RESPONSIBILITIES

At a minimum, TO Contractor personnel under this TORFP shall perform the following:

A) Recurring Daily / Weekly / Monthly Duties

Typical recurring duties include:

3.6.2.1.   Operations:
a. Project management meetings
b. Coordination and communications with DHMH and the Software Development Contractor
c. CCW meetings
d. Tier 1 Help Desk
e. Tier 2 Help Desk for O&M inquiries

f. Software release deployment activities
g. Operations tasks
h. Troubleshooting
i. COTS patch installation
j. Continuous improvement of performance and operations
k. Claims file processing

l. Batch transaction processing
m. Interface file processing
n. End-user support
o. Activity and batch reporting/monitoring
p. O&M Issues & risks management
q. Support transition in and out tasks
r. Other duties as assigned

3.6.2.2. Hosting:
a. Data back-ups
b. System security
c. 24x7 Monitoring system performance
d. Hosting facilities management
e. System scanning for viruses, security anomalies and system performance

f. Hardware and software procurement
g. System performance test plan development and execution
h. Support transition in and out tasks
i. Other duties as assigned

3.6.3   START-UP PERIOD REQUIREMENTS

Start-up Period requirements relate to the tasks performed by the TO Contractor to prepare for and take responsibility of the live LTSS System.

3.6.3.1	TO Contractor shall complete the *Start-up Period* within one hundred fifty (150) calendar days from the NTP. During the *Start-up Period*, the TO Contractor shall complete the following:
	
	 a. Fully staff positions
	 b. Provide DHMH with a list of requested documentation from the current O&M contractor and/or Software Development Contractor
	 c. Conduct transition-in meetings with the current O&M contractor and the Software Development Contractor
	 d. Confirm the Technical Infrastructure Design (Attachment 20)
	 e. Complete the following Deliverables:
	     i. Integrated Project Schedule
	     ii. Kick-off Meeting
	     iii. Beginning of Contract Transition Plan
	     iv. Project Management Plan (PMP)
	     v. Technical Operations Plan (TOP)
	     vi. Help Desk Operations Plan
	     vii. Claims and Interfaces Operations Plan
	     viii. Technical Infrastructure Test Master Plan
	     ix. LTSS Code Library Management Plan
	     x. Software Deployment Plan
	     xi. Continuity of Operations Plan (COOP)
	     xii. Hosting and Cutover Readiness Meeting(s)
		3.8.4.1–13

ID #	Start-up Period Requirements	Associated Deliverable ID #
	xiii. Hosting and Operations Cutover f. Establish secure connectivity with the following: i. DHMH's MMIS hosted by the Annapolis Data Center (ADC) ii. Current O&M contractor to support the migration of data iii. Software Development Contractor to support migration of code and data iv. MDS file provider v. The Hilltop Institute for the monthly data download g. Implement and maintain a LTSS Code Library and use a configuration control mechanism for all compiled code, release notes, etc. so that releases can be rolled back, if necessary h. Ensure the Help Desk system integrates with the Software Development Contractor's system (Microsoft's Team Foundation Server) i. Design, procure, build, test and certify hardware and COTS software to support the LTSS System, in preparation for cutover from current O&M contractor to TO Contractor j. Perform business simulation testing over a minimum of a three (3) week period that demonstrates readiness to cutover, including the following: i. Business simulation test planning that incorporates a minimum of two (2) simulated business weeks ii. Stakeholder participation coordination iii. Business simulation test execution iv. Batch process execution v. Claims file execution (full round trip, including MMIS test file processing) vi. Test all interfaces and data exchanges vii. Monitor, report, troubleshoot and resolve simulation defects viii. Simulate high-volume usage scenarios ix. Simulate concurrent on-line transactions with batch processing and replication k. Establish secure data replication with the current O&M contractor l. Establish a baseline for the LTSS System's response time (see Section 3.6.5.25 for minimum requirement) m. Coordinate go / no go decision with DHMH on the (OPTION) TEFT IVR within sixty (60) calendar days from the NTP	
3.6.3.2	TO Contractor shall develop, with DHMH's input, other artifacts including: a. Biweekly Project Work Plan updates b. Monthly Performance Reports c. Monthly Progress Reports d. Monthly SLA Reports	3.8.4.1 3.8.4.5 3.8.4.20 3.8.4.21 3.8.4.22

ID #	Start-up Period Requirements	Associated Deliverable ID #
	e. As defined in the TOP: i. Maintenance Schedule ii. COTS Patches iii. Technical Infrastructure changes iv. Hardware Inventory v. Hardware Maintenance Agreements vi. COTS Software Licenses	
3.6.3.3	TO Contractor shall develop with DHMH and the Software Development Contractor: a. The method for diagnosing reported system issues and determining if the issue is a defect, including which party is responsible for resolving the defect b. The method for receiving UAT-approved code from the Software Development Contractor, deploying the code into pre-production environment, supporting DHMH and/or the Software Development Contractor's regression testing in pre-production and validating the code after deployment into the production environments (as documented in the Software Deployment Plan) c. Integration requirements and approach between the contractors with the defect and change request tracking systems	3.8.4.5 3.8.4.8 3.8.4.10
3.6.3.4	The TO Contractor shall provide a Project Management Plan (PMP) that includes the following Sections / sub-plans: a. RACI Matrix and/or swim lane diagram depicting roles and responsibilities of the TO Contractor, Software Development Contractor and DHMH b. Scope Management c. Schedule Management d. Procurement Management e. Quality Management f. System Change Management and Configuration Management (software versions and licensing, code libraries, etc.) g. Staffing Management (including MBE requirements) h. Communications Management i. Issues and Risk Management j. Assumptions k. Constraints	3.8.4.4
3.6.3.5	TO Contractor shall obtain DHMH approval of the TOP, which shall include all off-site procedures for back-ups and DR, locations and operational protocols.	3.8.4.5

ID #	Start-up Period Requirements	Associated Deliverable ID #
3.6.3.6	TO Contractor shall only commence hosting activities and associated billing upon TO Contract Monitor acceptance of the Hosting and Operations Cutover deliverable.	3.8.4.12 3.8.4.13 3.8.4.14
3.6.3.7	TO Contractor shall ensure that COOP measures are in place and operational as a prerequisite to cutover from the current O&M contractor. TO Contractor shall ensure no loss of data or configuration of the environments during Start-up Period activities.	3.8.4.11
3.6.3.8	TO Contractor shall work closely with the current O&M contractor to obtain, review and understand the following received from the current O&M contractor, in a mutually agreed upon format: a. Current Help Desk knowledge base b. All Help Desk inquiries that are to be loaded into the TO Contractors Help Desk tool c. Current versions of the following artifacts: o PMP o TOP o Help Desk Operations Plan o Claims and Interfaces Operations Plan o Defects Tracker o Technical Infrastructure Test Master Plan o LTSS Code Library Management Plan o Software Deployment Plan d. Server build instructions e. Other artifacts as determined by DHMH	3.8.4.6 3.8.4.17

3.6.4 DATA CENTER REQUIREMENTS

The Data Center requirements relate to the technical infrastructure required to support the Department under the TO. Refer to Attachment 20 for the Technical Infrastructure Design.

ID #	Data Center Requirements	Associated Deliverable ID #
PRIMARY Data Center Architecture and Environment Requirements		
3.6.4.1	TO Contractor shall provide access control, server management, data storage, connection and firewall equipment and software that meet or exceed the Technical Infrastructure Design (Attachment 20). Refer to the supporting diagrams for additional information on the required design. TO Contractor may provide recommendations and justifications of alternate hardware or software solutions that provide equivalent or increased capabilities to meet the following design requirements with higher effectiveness or cost-efficiency.	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
3.6.4.2	TO Contractor shall implement FlexPod architecture for LTSS Infrastructure compatible with or equivalent to Cisco Unified Computing, Cisco consolidated networking, NetApp storage and VMware virtualization.	3.8.4.5
3.6.4.3	TO Contractor shall physically secure the servers with access control readers.	3.8.4.5
3.6.4.4	TO Contractor shall provide, at a minimum, the following physical security services the Primary Data Center: a. Manned 24 hours a day, 7 days a week, 365 days a year b. Access restricted to authorized client personnel and data center employees c. Axis IP-based interior and exterior surveillance cameras d. Entrance and exit controlled by HID contact-less access cards e. Cabinet access controlled by combination dial system f. Mantraps	3.8.4.5
3.6.4.5	TO Contractor shall provide licensing for the COTS software or equivalent/compatible tools that meet the specifications in the Technical Infrastructure Design (Attachment 20).	3.8.4.5
3.6.4.6	TO Contractor shall support replication of data from the Primary Datacenter to the Secondary Data Center	3.8.4.5
3.6.4.7	TO Contractor shall provide a Primary Data Center consisting of six (6) chassis for redundancy (Cisco UCS 5108 or equivalent), each populated with six (6) blades consisting of forty (40) CPU cores and 256GB RAM (Cisco B200 M4 or equivalent).	3.8.4.5
3.6.4.8	TO Contractor shall provide a Primary Data Center that hosts three (3) application stacks (green, blue, and pre-production) as well as a management stack.	3.8.4.5
3.6.4.9	TO Contractor shall provide a Primary Data Center with a computing environment consisting of three (3) VMware Clusters. The clusters shall be provisioned as Production, Pre-Production, and Management.	3.8.4.5
3.6.4.10	TO Contractor shall build the Primary Data Center environments to host the LTSS System with Production stacks (Green and Blue stacks) to minimize planned outages.	3.8.4.5
3.6.4.11	TO Contractor shall build the Data Center Environments using the High Availability (HA) approach.	3.8.4.5
3.6.4.12	TO Contractor shall build pre-production environment. The pre-production environment shall operate exactly as the production environment, including performance, with the exception of accessibility	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
	offered by Network Address Translation to prevent IP Address conflicts with the production environment. The data and configurations shall remain identical with their roles in production, as of the latest backup.	
3.6.4.13	TO Contractor shall build pre-production without implementing a HA approach.	3.8.4.5
3.6.4.14	TO Contractor shall use a VMware vSphere hypervisor or equivalent for all environments.	3.8.4.5
3.6.4.15	TO Contractor shall use VMware's vCenter to manage virtual environments.	3.8.4.5
3.6.4.16	TO Contractor shall equip the Primary Data Center to accommodate single server failure or chassis failure, with automatic failover and continued full capacity operations.	3.8.4.5
3.6.4.17	TO Contractor shall build the Primary Data Center environments, so that each environment within the Data center reside on separate vLANs and separate VRFs to ensure that each environment is separate and unique	3.8.4.5
PRIMARY Data Center Storage System Requirements		
3.6.4.18	TO Contractor shall use Network Attached Storage configured to allow all controllers in each data center to operate as clusters for easy maintenance, high availability and reliable performance.	3.8.4.5
3.6.4.19	TO Contractor shall use all-flash storage systems with solid state drives for the active data in LTSS System, with archived data on spinning disks.	3.8.4.5
3.6.4.20	TO Contractor shall provide a storage cluster attached to the virtual environment to provide near line storage for archival systems.	3.8.4.5
3.6.4.21	TO Contractor shall equip the Primary Data Center with HA controllers with nodes configured to enable workload segregation or distribution across the available hardware.	3.8.4.5
3.6.4.22	TO Contractor shall configure the Primary Data Center to host one (1) storage system. The HA controllers shall be configured in a separate storage cluster available to the virtual infrastructure used by archive or near line database disks.	3.8.4.5
3.6.4.23	TO Contractor shall configure all storage systems for presentation to all VMware Hosts using NFS.	3.8.4.5
3.6.4.24	TO Contractor shall configure the clusters in two (2) physically and logically separate SAN/NAS fabrics, each containing two NetApp nodes and each having two controller modules for HA purposes. The four total nodes at each site shall be clustered for the production and pre-production environments. The management environment that contains all services	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
	critical for supporting the LTSS Application and Infrastructure may share a NetApp cluster with pre-production.	
3.6.4.25	TO Contractor shall configure storage clusters for accessibility only by the hosts, VMs, and devices that are part of the assigned enclave. The second cluster shall be provisioned to host pre-production, and management systems.	3.8.4.5
3.6.4.26	TO Contractor shall provide a storage system that offers equal performance to all hosts, and is controlled by VMware's storage IO control functions.	3.8.4.5
3.6.4.27	TO Contractor shall provide the ability to ensure that production servers can use as much IO as necessary via SIOC, VAAI API, network QoS, UCS Fabric, and the virtual network.	3.8.4.5
3.6.4.28	TO Contractor shall control resources to enable application performance testing in the pre-production environment while running the management stack in parallel.	3.8.4.5
3.6.4.29	TO Contractor shall configure the storage systems for integration with the TO Contractor's backup solution to enable archiving of NetApp snapshots.	3.8.4.5
3.6.4.30	TO Contractor shall configure the storage system that encrypts data at rest.	3.8.4.5
3.6.4.31	TO Contractor shall provide encryption at FIPS 140-2 level 2, with no performance impact.	3.8.4.5
PRIMARY Data Center Replication, Backup and Recovery Requirements		
3.6.4.32	TO Contractor shall use industry standard COTS software for backup and disaster recovery functions.	3.8.4.5
3.6.4.33	TO Contractor shall accommodate approximately 448TB of onboard storage at the Primary Data Center, storing backups locally to minimize RTO and RPO times and provide fast local recovery of files, volumes, snapshots, VMs, Active Directory Objects and SQL Objects. The Primary Data Center shall maintain local copies of backups and retain a copy of the opposite site's backup repository to enable rebuilding in the event of a catastrophic disaster at either site.	3.8.4.5
3.6.4.34	TO Contractor shall replicate databases, monitored in real-time to ensure that any replication events are flagged and addressed. The replication shall be configured and monitored to prevent data integrity issues or data inconsistencies.	3.8.4.5

DHMH LTSS O&M

DHMH OPASS 18-17607 /M00B8400002

ID #	Data Center Requirements	Associated Deliverable ID #
3.6.4.35	TO Contractor shall replicate SQL databases using SQL Replication. All backups shall be de-duplicated, compressed and encrypted for storage at the local site. After all backups have completed, they shall be replicated to the Secondary Data Center and retained for up to thirty (30) calendar days.	3.8.4.5
3.6.4.36	TO Contractor shall complete backups on a local drive. Virtual machines shall be backed up on the NetApp Storage system, then compressed, de-duplicated, and encrypted. Virtual server backups shall be retained for one (1) year.	3.8.4.5
3.6.4.37	TO Contractor shall backup all other systems in accordance with the policies and retention periods defined for each server type, per industry standards.	3.8.4.5
PRIMARY Data Center Networking and Firewall Requirements		
3.6.4.38	TO Contractor shall equip the Primary Data Center with a minimum of two (2) firewalls, two (2) routers, two (2) load balancers, two (2) fabric interconnect and compatible switches to comply with the required architecture design.	3.8.4.5
3.6.4.39	TO Contractor shall provide Internet access through an encrypted VPN connection from the firewall at the Primary Data Center. Two (2) one (1) gigabit-per-second circuits shall allow up to 250Mbps encrypted throughput per circuit, using the firewalls. This connection shall be used as a backup for the routers, which provide the requested encrypted throughput.	3.8.4.5
3.6.4.40	TO Contractor shall provide "blended" Internet services, mixing high-speed Internet feeds from two (2) or more Internet carriers for redundancy. The Internet bandwidth available to the LTSS environment shall be 1000 Mbps, with ports terminating on two (2) separate switches for hardware and connectivity diversity.	3.8.4.5
3.6.4.41	TO Contractor shall configure two (2) firewalls as an active/standby failover pair to serve as the Internet edge devices. These firewalls shall secure the data center environments from the Internet, and allow selected inbound and outbound access to the Internet in accordance with project requirements. The firewalls also shall manage site-to-site IPsec VPN tunnels to third parties, and VPN client access for remote management of the environment.	3.8.4.5
3.6.4.42	TO Contractor shall provide local area networking to perform all inter-VLAN routing functions.	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
3.6.4.43	TO Contractor shall ensure that all switch-to-switch connections are redundant, with redundant cabling in place.	3.8.4.5
3.6.4.44	TO Contractor shall provide switches to provide connectivity for WAN and security devices, as well as any LAN devices requiring 1Gbps copper ports.	3.8.4.5
3.6.4.45	TO Contractor shall provide balancers to load balance incoming IVR traffic to the IVR pool of web servers.	3.8.4.5
3.6.4.46	TO Contactor shall provide client VPN access to all environments located in the Primary Data Center for remote management and testing purposes	3.8.4.5
SECONDARY Data Center Architecture and Environment Requirements		
3.6.4.47	TO Contractor shall provide access control, server management, data storage, connection and firewall equipment and software that meet or exceed the Technical Infrastructure Design. Refer to the supporting diagrams for additional information on the required design. TO Contractor may provide recommendations and justifications of alternate hardware or software solutions that provide equivalent or increased capabilities to meet the following design requirements with higher effectiveness or cost-efficiency.	3.8.4.5
3.6.4.48	TO Contractor shall implement FlexPod architecture for LTSS Infrastructure compatible with or equivalent to Cisco Unified Computing, Cisco consolidated networking, NetApp storage and VMware virtualization.	3.8.4.5
3.6.4.49	TO Contractor shall physically secure the servers with access control readers.	3.8.4.5
3.6.4.50	TO Contractor shall provide, at a minimum, the following physical security services in both the Primary and Secondary Data Centers: g. Manned 24 hours a day, 7 days a week, 365 days a year h. Access restricted to authorized client personnel and data center employees i. Axis IP-based interior and exterior surveillance cameras j. Entrance and exit controlled by HID contact-less access cards k. Cabinet access controlled by combination dial system l. Mantraps	3.8.4.5
3.6.4.51	TO Contractor shall provide licensing for the COTS software or equivalent/compatible tools that meet the specifications in the Technical Infrastructure Design (Attachment 20).	3.8.4.5
3.6.4.52	TO Contractor shall support replication of data from the Secondary Datacenter to the Primary Data Center	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
3.6.4.53	TO Contractor shall build the Secondary Data Center Environments using the High Availability (HA) approach.	3.8.4.5
3.6.4.54	TO Contractor shall provide a Secondary Data Center which will provide an additional site to serve as a standby site for the LTSS System in the event of maintenance and disaster recovery of the Primary Data Center.	3.8.4.5
3.6.4.55	TO Contractor shall use a VMware vSphere hypervisor or equivalent for all environments.	3.8.4.5
3.6.4.56	TO Contractor shall use VMware's vCenter to manage virtual environments.	3.8.4.5
3.6.4.57	TO Contractor shall equip the Secondary Data Center to accommodate single server failure or chassis failure, with automatic failover and continued full capacity operations.	3.8.4.5
3.6.4.58	TO Contractor shall build the Secondary Data Center environments, so that each environment within the Secondary Data center reside on separate vLANs and separate VRFs to ensure that each environment is separate and unique	3.8.4.5
3.6.4.59	TO Contractor shall build the Secondary Data Center to provide a green-only production environment and provide failure redundancy.	3.8.4.5
SECONDARY Data Center Storage System Requirements		
3.6.4.60	TO Contractor shall use Network Attached Storage configured to allow all controllers in each data center to operate as clusters for easy maintenance, high availability and reliable performance.	3.8.4.5
3.6.4.61	TO Contractor shall use all-flash storage systems with solid state drives for the active data in LTSS System, with archived data on spinning disks.	3.8.4.5
3.6.4.62	TO Contractor shall provide a storage cluster attached to the virtual environment to provide near line storage for archival systems.	3.8.4.5
3.6.4.63	TO Contractor shall equip the Secondary Data Center with HA controllers with nodes configured to enable workload segregation or distribution across the available hardware.	3.8.4.5
3.6.4.64	TO Contractor shall configure the Secondary Data Center to host one storage system. The HA controllers shall be configured in a separate storage cluster available to the virtual infrastructure used by archive or near line database disks.	3.8.4.5
3.6.4.65	TO Contractor shall configure all storage systems for presentation to all VMware Hosts using NFS.	3.8.4.5
3.6.4.66	TO Contractor shall configure the clusters in two (2) physically and logically separate SAN/NAS fabrics, each containing two (2) NetApp	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
	nodes and each having two (2) controller modules for HA purposes. The four (4) total nodes at each site shall be clustered for the production and pre-production environments. The management environment that contains all services critical for supporting the LTSS Application and Infrastructure may share a NetApp cluster with pre-production.	
3.6.4.67	TO Contractor shall configure storage clusters for accessibility only by the hosts, VMs, and devices that are part of the assigned enclave. The second cluster shall be provisioned to host pre-production, and management systems.	3.8.4.5
3.6.4.68	TO Contractor shall provide a storage system that offers equal performance to all hosts, and is controlled by VMware's storage IO control functions.	3.8.4.5
3.6.4.69	TO Contractor shall provide the ability to ensure that production servers can use as much IO as necessary via SIOC, VAAI API, network QoS, UCS Fabric, and the virtual network.	3.8.4.5
3.6.4.70	TO Contractor shall control resources to enable application performance testing in the pre-production environment while running the management stack in parallel.	3.8.4.5
3.6.4.71	TO Contractor shall provide a Secondary Data Center that hosts a NetApp infrastructure similar to the primary datacenter, reduced in size but not performance, allowing for minimal downtimes, reduced management overhead, and the ability to perform disaster recovery or failover without reducing business continuity, and with little to no downtime.	3.8.4.5
3.6.4.72	TO Contractor shall configure the storage systems for integration with the TO Contractor's backup solution to enable archiving of NetApp snapshots.	3.8.4.5
3.6.4.73	TO Contractor shall configure the storage system that encrypts data at rest.	3.8.4.5
3.6.4.74	TO Contractor shall provide encryption at FIPS 140-2 level 2, with no performance impact.	3.8.4.5
SECONDARY Data Center Replication, Backup and Recovery Requirements		
3.6.4.75	TO Contractor shall use industry standard COTS software for backup and disaster recovery functions.	3.8.4.5
3.6.4.76	TO Contractor shall accommodate approximately 448TB of onboard storage at the Secondary Data Center, storing backups locally to minimize RTO and RPO times and provide fast local recovery of files, volumes, snapshots, VMs, Active Directory Objects and SQL Objects.	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
	The Secondary Data Center shall maintain local copies of backups and retain a copy of the opposite site's backup repository to enable rebuilding in the event of a catastrophic disaster at either site.	
3.6.4.77	TO Contractor shall replicate databases, monitored in real-time to ensure that any replication events are flagged and addressed. The replication shall be configured and monitored to prevent data integrity issues or data inconsistencies.	3.8.4.5
3.6.4.78	TO Contractor shall replicate SQL databases using SQL Replication. All backups shall be de-duplicated, compressed and encrypted for storage at the local site. After all backups have completed, they shall be replicated to the Primary Data Center and retained for up to thirty (30) calendar days.	3.8.4.5
3.6.4.79	TO Contractor shall complete backups on a local drive. Virtual machines shall be backed up on the NetApp Storage system, then compressed, de-duplicated, and encrypted. Virtual server backups shall be retained for one (1) year.	3.8.4.5
3.6.4.80	TO Contractor shall backup all other systems in accordance with the policies and retention periods defined for each server type, per industry standards.	3.8.4.5
SECONDARY Data Center Networking and Firewall Requirements		
3.6.4.81	TO Contractor shall equip the Secondary Data Center with a minimum of two (2) firewalls, two (2) routers, two (2) load balancers, two (2) fabric interconnect and compatible switches to comply with the approved architecture design.	3.8.4.5
3.6.4.82	TO Contractor shall provide Internet access through an encrypted VPN connection from the firewall at the Secondary Data Center. Two (2) one (1) gigabit-per-second circuits shall allow up to 250Mbps encrypted throughput per circuit, using the firewalls. This connection shall be used as a backup for the routers, which provide the requested encrypted throughput.	3.8.4.5
3.6.4.83	TO Contractor shall provide "blended" Internet services, mixing high-speed Internet feeds from two (2) or more Internet carriers for redundancy. The Internet bandwidth available to the LTSS environment shall be 1000 Mbps, with ports terminating on two (2) separate switches for hardware and connectivity diversity.	3.8.4.5
3.6.4.84	TO Contractor shall configure two (2) firewalls as an active/standby failover pair to serve as the Internet edge devices. These firewalls shall secure the data center environments from the Internet, and allow selected inbound and outbound access to the Internet in accordance with project	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
	requirements. The firewalls also shall manage site-to-site IPsec VPN tunnels to third parties, and VPN client access for remote management of the environment.	
3.6.4.85	TO Contractor shall provide local area networking to perform all inter-VLAN routing functions.	3.8.4.5
3.6.4.86	TO Contractor shall ensure that all switch-to-switch connections are redundant, with redundant cabling in place.	3.8.4.5
3.6.4.87	TO Contractor shall provide switches to provide connectivity for WAN and security devices, as well as any LAN devices requiring 1Gbps copper ports.	3.8.4.5
3.6.4.88	TO Contractor shall provide balancers to load balance incoming IVR traffic to the IVR pool of web servers.	3.8.4.5
3.6.4.89	TO Contractor shall operate the Secondary Data Center to resemble the network topology of the primary data center. At minimum, the hardware shall consist of an exact or reasonable duplicate of the main system equipment (firewalls, switches, load balancers, routers, etc.). All VLAN and connections between devices shall match production for easy server replication. Server and network management VLANs shall route between sites for easy of management and failover. All communication between the Primary and Secondary Data Centers shall go through an encrypted one (1) GB Ethernet circuit.	3.8.4.5
3.6.4.90	TO Contactor shall provide client VPN access to all environments located in the Secondary Data Center for remote management and testing purposes	3.8.4.5
PRIMARY and SECONDARY Data Centers Software Hosting and Operation Requirements		
3.6.4.91	TO Contractor shall maintain and operate all COTS and custom developed software and applications used for administration and delivery of LTSS.	3.8.4.5
3.6.4.92	TO Contractor shall operate the COTS software or equivalent tools for system management, database administration and application support. TO Contractor shall ensure that software functions and performance meet, at minimum, the capabilities of the COTS applications listed. TO Contractor may provide recommendations and justification for additional or alternative software that can meet or exceed design requirements more effectively or cost-efficiently. Any alternative software furnished by the TO Contractor is required to have similar capabilities and be compatible with: a. Microsoft Windows Server Data Center Edition	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
	b. Reporting and Ad Hoc Database – Microsoft SQL Server Standard (includes SSRS) c. Transaction Database – RavenDB Standard Plus, and Enterprise editions d. IBM Sterling Connect: Direct Standard Edition with Secure+ e. VMware vSphere Enterprise Plus f. vCloud Suite g. Veeam Availability Suite v9 h. Shavlik Protect i. SolarWinds Network Performance Monitor j. SolarWinds Application Performance Monitor k. Zenoss Enterprise l. Microsoft Operations Management 2016 m. BlazeMeter n. Splunk o. Ndatalign	
PRIMARY and SECONDARY Data Centers Enterprise Monitoring, Maintenance and Technical Support Requirements		
3.6.4.93	TO Contractor shall provide enterprise level monitoring for the all environments hosting the LTSS application using secure connections to enable proactive, real-time support.	3.8.4.5
3.6.4.94	TO Contractor shall provide industry proven advanced level patch management for the Primary and Secondary Data Center environments.	3.8.4.5
3.6.4.95	TO Contractor shall implement a patch protection agent with a VPN connection that allows a centralized technical service desk and system administrators to patch the LTSS System.	3.8.4.5
3.6.4.96	TO Contractor shall ensure that all patches are reviewed and tested within pre-production environment before promotion to upper level environments.	3.8.4.5
3.6.4.97	TO Contractor shall implement a change management process to ensure that all patches are approved prior to deployment.	3.8.4.5
3.6.4.98	TO Contractor shall develop an approved schedule for maintenance of both Primary and Secondary Data Center environments.	3.8.4.5
3.6.4.99	TO Contractor shall develop policies and maintenance windows for critical updates, patches, system changes, or fixes that cannot be scheduled in pre-approved maintenance windows.	3.8.4.5
3.6.4.100	TO Contractor shall provide technical service desk staff, available 24x7, who can enter incidents and resolve issues at all times.	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
3.6.4.101	TO Contractor shall ensure that all infrastructure and network equipment is monitored 24x7 and shall maintain standard procedures for escalation of issues.	3.8.4.5
3.6.4.102	TO Contractor shall ensure that all LTSS System servers within the data center environments have multiple layers of security implemented at a system level. Anti-virus tools shall be installed, monitored, and continually updated on both Primary and Secondary Data Center servers. All servers and devices shall be scanned and patched with the latest updates and patches on a monthly basis. Both Primary and Secondary Data Center servers shall be hardened at the operating system level. All user accounts and access shall be limited at the server level to implement a need-to-have access level approach.	3.8.4.5
3.6.4.103	TO Contractor shall ensure that all devices and servers within the primary and secondary data centers are analyzed and monitored by a separate security resource to provide continual monitoring of logs, alerts, and events.	3.8.4.5
3.6.4.104	TO Contractor shall implement a minimum of three firewall security zones (outside, DMZ, and inside) to provide layered protection for all Internet connections and traffic.	3.8.4.5
3.6.4.105	TO Contractor shall control access to Cisco network and security devices with a combination of a RADIUS (Remote Authentication Dial-In User Service) server, and user accounts configured in the Active Directory servers in the virtual environment. The network and security devices shall pass login authentication to a Windows RADIUS server, and the RADIUS server shall check the credentials against Active Directory. Password expiration and complexity rules for user accounts shall be implemented according to best practices. Emergency local accounts shall be configured on all network and security devices in the event the RADIUS and/or Active Directory servers are unavailable.	3.8.4.5
3.6.4.106	TO Contractor shall provide intrusion detection and protection. The IDS/IPS service shall be used at all times to protect each environment from malware attacks and provide reputation and category-based URL filtering for protection against suspicious web traffic. The IPS should actively take any and all industry acceptable actions necessary to prevent the detected event from harming the environments. The ASA shall be configured to send alerts to the security operations center.	3.8.4.5
3.6.4.107	TO Contractor shall monitor logging by sending all SysLog events for storage on a logging server in each environment.	3.8.4.5

ID #	Data Center Requirements	Associated Deliverable ID #
3.6.4.108	TO Contractor shall configure all network and security devices using Simple Network Management Protocol (SNMP). SNMP statistics shall be collected by the SNMP server located in the network operations center. Where possible, SNMPv3 shall be used for its higher level of security.	3.8.4.5
3.6.4.109	TO Contractor shall ensure that all LTSS System server, device, or system certificates are tracked throughout the duration of the TO Agreement. Upon start of operational hosting of the production environment, an inventory shall be performed to track all applicable LTSS certificates and their respective expiration dates.	3.8.4.5

3.6.5   HOSTING REQUIREMENTS

Hosting requirements relate to IT system hosting, operations and performance required under the TO. Refer to Attachment 20 for the Technical Infrastructure Design.

ID #	Hosting Requirements	Associated Deliverable ID #
3.6.5.1	TO Contractor shall provide a Primary Data Center location in the continental United States.	3.8.4.5
3.6.5.2	TO Contractor shall provide a Secondary Data Center location in the continental United States that is at least fifty (50) miles from the Primary Data Center. Offeror's TO Technical Proposal shall describe how the Secondary Data Center location minimizes risk in the event of disaster, including service levels for recovery and minimizing data loss.	3.8.4.5 3.8.4.11
3.6.5.3	TO Contractor shall provide network protection to prevent attacks on DHMH's servers and to ensure DHMH's data, information, and networks are secured to prevent unauthorized access.	3.8.4.5
3.6.5.4	TO Contractor shall ensure both the Primary and Secondary Data Center facilities are compliant with SSAE16, and HIPAA standards.	3.8.4.5

3.6.5.5	TO Contractor shall provide an IVR capability that meets the minimum volume requirements specified in Section 3.3.
	
	a. Service Provider IVR shall include the functions for service providers to clock-in / clock-out. Refer to the current IVR solution in Attachment 20.
	
	  i. An IVR call must be from a verified LTSS System user.
	
	  ii. For clock-in/clock-out, verification requires the caller to enter a valid provider number and a valid social security number (SSN).
		3.8.4.5

ID #	Hosting Requirements	Associated Deliverable ID #

	b. (OPTION) TEFT IVR shall include the functions for users to check their program information. For the proposed call flow for the TEFT IVR, refer to Attachment 22.
	    i. An IVR call must be from a verified LTSS System user.
	    ii. The verification criterion for TEFT requires confirmation that a validated stakeholder initiated the call.	

3.6.5.6	TO Contractor shall provide all equipment required to provision, monitor, and manage the circuit to the Primary and Secondary Data Center facilities.	3.8.4.5
3.6.5.7	TO Contractor shall provide dedicated services with no comingling of data or resources with other clients other than the State of Maryland. This includes all Internet connectivity.	3.8.4.5
3.6.5.8	TO Contractor shall provide Internet connectivity with sufficient capacity and redundancy to support the LTSS System and future growth over the duration of the TO.	3.8.4.5
3.6.5.9	TO Contractor shall demonstrate in the TO Technical Proposal its ability to increase the size of the circuit in incremental increases of ten (10) Mbps, one hundred (100) Mbps, and one (1) Gbps, should DHMH require an increase in the future.	3.8.4.5
3.6.5.10	TO Contractor shall provide WAN encrypted tunnel support to DHMH from both the Primary and Secondary Data Centers.	3.8.4.5
3.6.5.11	TO Contractor shall provide a firewall and security solution that complies with the transmission security provisions of the HIPAA, as well as all relevant federal, State, and local laws.	
3.6.5.12	TO Contractor shall provide a description of the proposed network security, describing the effectiveness of the proposed system protocols and measures to prevent intrusion and protect DHMH's data.	3.8.4.5
3.6.5.13	TO Contractor shall provide Security services that include the following: a. The Security service shall provide monitoring for timely reporting of threats and intrusions. b. The Security services shall provide security protections to prevent unauthorized access to DHMH's information, software, and systems. c. The Security services shall include a security agent to control all traffic between the primary and secondary data centers and the outside world and to protect against unauthorized access or intrusions.	3.8.4.5

ID #	Hosting Requirements	Associated Deliverable ID #
	d. The Security services shall allow reporting for firewall and other statistics from any Internet browser with monthly analysis and recommendations to improve security and throughput.	
3.6.5.14	TO Contractor shall ensure the security, integrity and availability of the data to the Department, and shall describe in its TO Technical Proposal the levels it will achieve and how it intends to achieve security, integrity and availability, including DR services.	3.8.4.5
3.6.5.15	TO Contractor shall provide system and data reliability through off-site system and data backup in accordance with the SLA.	3.8.4.5
3.6.5.16	TO Contractor shall provide to DHMH's Project Manager the make and model number of all network components and infrastructure after award and before cutover. TO Contractor shall update this information as equipment is retired or added.	3.8.4.5
3.6.5.17	TO Contractor shall install and configure all hardware and software required to build out the following environments: a. Primary Data Center: • Pre-production environment • Production environment • Management environment b. Secondary Data Center • Production environment (on standby for DR purposes) • Management environment	3.8.4.5
3.6.5.18	TO Contractor shall provide monitoring and reporting features to clearly identify adherence to the SLA for availability of the technical solution; including reporting on bandwidth usage, backup frequency and success.	3.8.4.5
3.6.5.19	TO Contractor shall perform reporting on security incidents and breaches (both immediate reporting and summary reporting).	3.8.4.5
3.6.5.20	TO Contractor shall perform reporting on login attempts as requested by the agency	3.8.4.5
3.6.5.21	TO Contractor shall provide managed services, including: a managed firewall, system and application monitoring, performance monitoring, server startup and shutdown support, hardware maintenance, network alerts, troubleshooting and response, operating system patch installation and minor upgrades, file system management support, failure tracking and backup/restore of all system components and data.	3.8.4.5

ID #	Hosting Requirements	Associated Deliverable ID #
3.6.5.22	TO Contractor shall provide administrator level access to the LTSS System technical infrastructure and the LTSS Code Library for DHMH's technical support team to enable technical oversight of the LTSS System assets.	3.8.4.5
3.6.5.23	TO Contractor shall create and update, at least once per month, the Database Performance Report.	3.8.4.19
3.6.5.24	TO Contractor shall create and update, at least once per month, the technical solution performance report.	3.8.4.19
3.6.5.25	TO Contractor shall establish a baseline response time for the LTSS System's online transactions. TO Contractor and DHMH shall jointly develop a test script that can be executed by the Help Desk, monitored by TO Contractor and DHMH. The response time test script shall measure online transactions that do not change data and transactions that do change data. The baseline response time shall be established before cutover. Response time is measured on an ad hoc basis when requested by DHMH. **The required minimum baseline for average response time with 250 simultaneous users is 350 Milliseconds for web transactions (inclusive of on-line and web services).**	3.8.4.12 3.8.4.13
3.6.5.26	TO Contractor shall maintain the TOP and provide updates annually, or within twenty (20) days of changes that impact backup, DR, or other continuity of operations activities.	3.8.4.5

3.6.6   OPERATIONS REQUIREMENTS

Operations requirements relate to business processes provided or supported under the TO.

ID #	Operations Requirements	Associated Deliverable ID #
3.6.6.1	TO Contractor shall provide sufficient hardware and software services that support the LTSS System's claims file processing that meets the minimum volume requirements specified in Section 3.3, as follows. a. The capacity to process claims including the ANSI X12N file transactions: i. Execute, monitor and provide reconciliation reporting on batch processes that generate claims file ii. Send eligibility benefit inquiry (270 submission) request to MMIS to determine eligibility iii. Retrieve and process eligibility benefit response (271) from MMIS iv. Process service activity records and generate claim items through the 837/835 process	3.8.4.5 3.8.4.7

ID #	Operations Requirements	Associated Deliverable ID #
	v. Generate the weekly 837P claim batch per departmental policies vi. Submit the weekly claim batch (providers and case managers) to MMIS per departmental policies vii. Retrieve the claim batch functional acknowledgement (997) from MMIS per departmental policies viii. Retrieve and process payment remittance advice from MMIS (835) per departmental policies b. Support DHMH's processing of claims adjustments and dispositioning exceptions c. Claims activity reconciliation (summarized daily, weekly, and monthly) reporting. TO Contractor shall describe the methodology and provide sample reports with the submitted TO Technical Proposal. e. Claims balance (summarized daily, weekly, monthly) reporting. TO Contractor shall describe the methodology and provide sample reports with the submitted TO Technical Proposal	
3.6.6.2	TO Contractor shall process batch transactions and interfaces. For batch transactions, TO Contractor shall validate that batch processes are successfully executed. For interfaces, TO Contractor shall validate that interface data have been sent and received and validate that data were correctly processed. The current batch schedule for the LTSS System is as follows but shall be verified and updated during the Start-up Period:	3.8.4.5 3.8.4.7

Job Name	Schedule
Half Hourly match	Every day, Every half hour
Weekly Receive 999	1:00 PM Every day
Weekly Receive 999-2	1:15 PM every day
Weekly Receive 835	4:15 PM every day
Weekly Receive 835-2	4:30 PM every day
CM Billing All	8:15 PM every Wednesday
MMIS Client Import Daily - Init	5:15 AM and 8:15 PM every day
MMIS Client Import Daily Group 1	6:35 AM and 9:35 PM every day
MMIS Client Import Daily Group 2	6:35 AM and 9:35 PM every day
MMIS Client Import Daily Group 3	6:35 AM and 9:35 PM every day
CM Billing Receive 999	11:45 PM every Wednesday
CM Billing Receive 999-2	11:55 PM every Wednesday
MMIS Provider Import	12:15 AM every day
Activate SPA	1:30 AM every day
Update MDC provider Selection	1:30 AM every day

ID #	Operations Requirements		Associated Deliverable ID #
	Update CaseProgram.DewsProgressStatus	2:30 AM every day	
	Weekday All ISAS Claims	3:15 AM every day except Friday	
	Update Med Tech Redetermination Status	3:30 AM every day	
	Nurse Monitoring Process Creation	3:45 AM every day	
	Deactivate LOC	4:05 AM every day	
	MDS Client Import Daily - Init	5:05 AM every day	
	MDS Client Import Daily Group 1	6:06 AM every day	
	SA Validation Only	3:45 AM every Friday	

A sample of the interfaces with the LTSS System includes:

    a. Inbound Files processed via batch:
        i.   RecipInf – Recipient Information
        ii.   EligSpan – Recipient Eligibility Spans
        iii.   NRSHOM – Nursing Home Eligibility
        iv.   MASTER – Master Provider Table
        v.   ADDRESS – Provider Address
        vi.   NMPROV – Non-Medicaid Providers
        vii.   SPCPGM – Special Program Enrollment Spans
        viii.   Minimum Data Set (MDS)
        ix.   271 eligibility check return
        x.   835 payment remittance advice
        xi.   997 acknowledgment
        xii.   999 acknowledgment
        xiii.   Registry import
    b. Outbound Files processed via batch:
        i.   270 eligibility benefit inquiry
        ii.   837 claims
        iii.   837P batch claims
    c. Outbound Files processed manually:
        i.   Hilltop Institute Data Set
    d. Web Services
        i.   IVR provider services (clock-in/out)
        ii.   IVR TEFT Telephone Tool for activity inquiry, if decision by DHMH is to go forward
        iii.   Supports Intensity Scale (SIS) assessment request and results data exchange
        iv.   HRST assessment
        v.   Provider data exchange
        vi.   Other web services as required
    e. Others as required

ID #	Operations Requirements	Associated Deliverable ID #
3.6.6.3	TO Contractor shall deploy software releases to the pre-production and production environments, after confirming they are tested and approved for deployment by DHMH. Per year, twelve planned (12) software	3.8.4.10 3.8.4.15

ID #	Operations Requirements	Associated Deliverable ID #
	releases require deployment planning and coordination. Some software releases that do not require as much planning and coordination (such as critical and high defect fixes or high-priority software change requests) are deployed as needed.	
3.6.6.4	TO Contractor shall provide personnel and a system for the Tier 1 Help Desk for LTSS System users that meets the minimum volume requirements specific in Section 3.3. Tier 1 personnel create initial Help Desk inquiry, conduct triage, resolve Tier 1 inquiries, escalate to the appropriate party when necessary (e.g. DHMH, O&M contractor and/or Software Development Contractor). Tier 1 is defined as the initial receiver of inquiries from system users, either by telephone or email. TO Contractor shall have the capability to respond to phone and email inquiries in English and/or Spanish.	3.8.4.6
3.6.6.5	TO Contractor shall resolve Tier 2 O&M Help Desk inquiries. Tier 2 O&M is defined as any issue involving investigation into the hardware, COTS software, networking, operational or other component or function under the purview of the TO Contractor. Issues relating to the custom-developed software shall be escalated to the Software Development Contractor for Tier 2 resolution. Issues relating to interface and/or claims file processing determined outside the scope of the TO Contractor's responsibilities shall be escalated to the appropriate party.	3.8.4.6

3.6.6.6	TO Contractor shall provide a comprehensive web-based Help Desk tracking and reporting software that captures, at a minimum, the following data:
	 a. Help Desk representative
	 b. Source (e.g. phone, online feedback, email, other)
	 c. Source contact information
	 d. Open date and timestamp
	 e. Status with status change dates to show history
	 f. Reported by name
	 g. Short description
	 h. Long description (including updates)
	 i. System component(s) impacted
	 j. Escalation – current level and escalation path history
	 k. Resolution
	 l. Priority
	
	      i. High –major portions of the system and/or the business is impacted, security issue, sensitive data loss, some payment and/or claims issues, system is slow, data is unavailable
	      ii. Normal –non-critical features are not operating as specified, worker(s) or user(s) are unable to perform their tasks in the system
		3.8.4.6

ID #	Operations Requirements	Associated Deliverable ID #
	iii. Low –lower priority features that can be performed manually are not operating as specified, request for service with ample lead time	
3.6.6.7	Help Desk inquiries and issues can be accessed by authorized individuals within DHMH.	3.8.4.6
3.6.6.8	TO Contractor shall, on at least a monthly basis, analyze Help Desk records and provide recommendations to minimize or eliminate recurring problems.	3.8.4.6
3.6.6.9	TO Contractor shall provide formal Help Desk quality assurance and customer satisfaction reports on a quarterly basis.	3.8.4.6
3.6.6.10	TO Contractor shall provide monthly Help Desk reports and metrics to designated DHMH resources. These reports will include, but are not limited to, metrics on previously opened inquiries, new inquiries, closed inquiries, currently open inquiries, quality assurance survey results, speed to answer and abandon rate.	3.8.4.6 3.8.4.20
3.6.6.11	TO Contractor shall provide credentials management and support for users of the LTSS System.	3.8.4.6
3.6.6.12	TO Contractor shall record, troubleshoot and resolve questions and issues for LTSS System users including passwords, login, network or other issues related to connecting with the LTSS System.	3.8.4.6
3.6.6.13	TO Contractor shall provide email status updates to the LTSS system user when new inquiries are entered and again when closed by the Help Desk.	3.8.4.6
3.6.6.14	TO Contractor shall provide various modes by which callers may request assistance including: a. Toll free telephone service (800 or similar number for domestic and an alternative number for international calls) b. Web forms c. Web-based self-help, documentation, FAQS, email Note: the Software Development Contractor shall provide release notes and, when appropriate, training to support the TO Contractor's knowledge base updates to the Help Desk tool associated with a particular release.	3.8.4.6
3.6.6.15	TO Contractor shall provide the LTSS System user with an opportunity to provide feedback for each of the help mechanisms listed in Section 3.6.6.14 that the user used.	3.8.4.6
3.6.6.16	TO Contractor shall provide redundant systems to ensure Help Desk availability including, but not limited to, the telephone system used by the	3.8.4.6

ID #	Operations Requirements	Associated Deliverable ID #
	TO Contractor. Voice mail shall be accessible on a twenty-four (24) hour basis.	
3.6.6.17	TO Contractor shall provide training of DHMH resources using the TO Contractor-provided Help Desk tool.	3.8.4.6
3.6.6.18	TO Contractor shall provide Help Desk system user credentials for DHMH staff. These credentials may be individual or group accounts.	3.8.4.6
3.6.6.19	TO Contractor shall, as part of its ongoing operational services, provide updates to the Help Desk scripts and knowledge base in accordance with LTSS System releases.	3.8.4.6
3.6.6.20	TO Contractor shall, as part of its ongoing operational services, perform ongoing training of customer service representatives in the LTSS System.	3.8.4.6
3.6.6.21	TO Contractor shall staff the Help Desk to handle the minimum volume requirements specified in Section 3.3, as part of the Start-up phase. Offeror shall describe the ability to ramp up staffing to meet additional inquiry volumes, as may be executed through the Additional Services Work Order process. The metrics on inquiries are intended for staffing purposes. Hang-ups, wrong numbers, abandoned calls, and other situations that do not engage the Help Desk staff on LTSS-related inquiries are not counted in the inquiry metrics. Inquiries on the same issue are counted as one (1) unique inquiry. For example, an outage that generates many calls and/or emails into the Help Desk counts as one (1) inquiry. The TO Contractor should establish processes to actively communicate such instances to limit calls and/or emails to the Help Desk. Inquiries shall contain all the information listed in 3.6.6.6.	3.8.4.6
3.6.6.22	TO Contractor shall create and maintain email distribution lists, including but not limited to the following: a. DHMH users by division b. Service providers by program c. Service provider administrators by program d. Others as required	3.8.4.6
3.6.6.23	TO Contractor shall propose, procure, install, test and deploy COTS software package to support the claims file processing operations. The COTS software shall provide reporting for balancing and reconciliation. The proposed solution shall support reporting on daily, weekly, monthly, and other durations as required. The solution shall support troubleshooting	3.8.4.15

ID #	Operations Requirements	Associated Deliverable ID #
	at the aggregate and detail level. TO Contractor shall ensure the Operations Lead is proficient in the proposed solution. The TO Technical Proposal shall provide sufficient information for DHMH to evaluate and select COTS software that meets these requirements.	

OPTIONAL SERVICE: Database Support Services Requirements		
These requirements apply only to those prospective Offerors proposing a solution to meet the Department's needs. If these services are not included as part of the TO Technical Proposal, prospective Offerors should indicate "SERVICES NOT PROPOSED". The State, at its sole option and discretion may elect to request the services described in the TO Contractor's proposal.		
ID #	**Database Support Services Requirements**	**Associated Deliverable ID #**

3.6.6.24	Daily monitoring for all RavenDBs, SQL Server DBs and database servers, including:
	
	1) Review alerts from monitoring jobs.
	2) Monitor LTSS MD DBA folder for queries and requests.
	3) Database Backup: validate backup is complete and was created per schedule for:
	   a) RavenDB backup
	   b) SQL server backup
	4) Monitor and review nightly processing.
	5) Review RavenDB server logs: Review errors, warnings and any abnormality.
	6) Review SQL Server Log.
	   a) Check for errors
	   b) Check for security breaches
	7) SQL Server Agent jobs (ltssprodsql01, ltssprodssrs01, ltssprodssrs02):
	   a) Check if there is job failure
	   b) Check if the job finished in the expected time frame
	8) Windows event log: check if any Windows or hardware error or warning requires attention.
	9) Replication monitoring and replication log review:
	10) Make sure replication completed with no errors and replication lag is normal
	11) Correct data delay as needed
	12) Performance log:
	   a) Check if database baseline is exceeded
	   b) Check the index and server statistics
	   c) Check the database statistics and fragmentation
	   d) Check for user access and query runtime, access pattern
	   e) Monitor if the code is not optimized
		3.8.4.23

OPTIONAL SERVICE: Database Support Services Requirements

These requirements apply only to those prospective Offerors proposing a solution to meet the Department's needs. If these services are not included as part of the TO Technical Proposal, prospective Offerors should indicate "SERVICES NOT PROPOSED". The State, at its sole option and discretion may elect to request the services described in the TO Contractor's proposal.

ID #	Database Support Services Requirements	Associated Deliverable ID #
	13) Storage capability: a) Validate the storage support database b) Backup batch process in short term 14) DB backup and restore support to pre-prod and dev/test environments.	
3.6.6.25	Daily corrective action based on monitoring for all RavenDBs, SQL Server DBs and database servers, including: 1) Log issue in tracking tool and notify DHMH and all other relevant parties by follow-up email. 2) For urgent issues, take appropriate action and notify team accordingly as soon as possible. 3) Check for possibilities for improvement based on review and analysis of issues. 4) Try to automate processes and setup error alerts for new processes or implementations.	3.8.4.23
3.6.6.26	Daily end user support, including: 1) Provide data and validation support as needed. 2) Assist with preparing ad hoc and user reports as needed. 3) Provide support for user tools as needed.	3.8.4.23
3.6.6.27	Daily change management, including: 1) Track all changes/versions in the version control system for each scheduled release or emergency update. 2) Provide user access support and follow proper change control processes. 3) Monitor scripts/utilities development and maintenance. 4) Assist with database deployment: a) Review database release scripts b) Support application deployments c) Install data patches independent of deployments	3.8.4.23
3.6.6.28	Weekly support, including: 1) Test backup regularly to make sure restore from the backup within SLAs can be achieved. 2) Gather performance information for capacity planning and suggestions.	3.8.4.23

	OPTIONAL SERVICE: Database Support Services Requirements These requirements apply only to those prospective Offerors proposing a solution to meet the Department's needs. If these services are not included as part of the TO Technical Proposal, prospective Offerors should indicate "SERVICES NOT PROPOSED". The State, at its sole option and discretion may elect to request the services described in the TO Contractor's proposal.	
ID #	**Database Support Services Requirements**	**Associated Deliverable ID #**
	a) Review disk usage, growth rate and performance for short-term and long-term planning. b) Review metrics and trends to identify suggestions for IO/CPU storage needs or memory. 3) Review the SQL Server patches and service packs that could potentially improve database performance. 4) Test recommended patches in the DEV environment and coordinate testing and performance reviews with the Development team. 5) Log support inquiry, if needed. 6) Review RavenDB patches and in the DEV environment as needed. 7) Check to ensure documentation is up-to-date.	

3.6.6.29	Monthly / Sprint Checklist, including:
	
	1) Backup validation (comprehensive):
	  a) Conduct backup
	  b) Test the restore and document the process and time used in each step.
	  c) Validate that the database can be restored accurately and the application functions properly.
	  d) Verify the server version and compatibility.
	2) Test the Disaster Recovery Plan.
	3) Refresh the pre-production environment on demand or as needed for troubleshooting.
	4) Review the database architecture and identify potential improvement.
	5) Review needs for database version upgrade (RavenDB and SQL server DB). Refer to Upgrades, below.
	6) Review and update the checklist for meetings.
		3.8.4.23

3.6.6.30	Minor database and server instance upgrades, including: 1) Testing and validation 2) Report compatibility regression testing 3) Replication 4) SQL replication 5) Performance testing 6) High availability and load balance testing	3.8.4.23
3.6.6.31	Major server version upgrades, including: 1) Upgrade	3.8.4.23

ID #	Database Support Services Requirements	Associated Deliverable ID #

<div align="center">

OPTIONAL SERVICE: Database Support Services Requirements

These requirements apply only to those prospective Offerors proposing a solution to meet the Department's needs. If these services are not included as part of the TO Technical Proposal, prospective Offerors should indicate "SERVICES NOT PROPOSED". The State, at its sole option and discretion may elect to request the services described in the TO Contractor's proposal.

</div>

ID #	Database Support Services Requirements	Associated Deliverable ID #
	2) Report performance testing 3) Compatibility and regression testing	
3.6.6.32	RavenDB customized build, including: 1) Customized performance enhancement testing 2) Customized upgrade monitoring and testing	3.8.4.23
3.6.6.33	Testing new database features and functions, as required.	3.8.4.23

3.6.7   SERVICE LEVEL AGREEMENT (SLA)

3.6.7.1 Service Level Agreement Liquidated Damages

Time is an essential element of the TO and it is important that the work is vigorously prosecuted until completion. For work that is not completed within the time(s) specified in the performance measurements below, the TO Contractor shall be liable for liquidated damages in the amount(s) provided for in this TO Agreement, provided, however, that due account shall be taken of any adjustment of specified completion time(s) for completion of work as granted by approved change orders and/or Work Orders.

The parties agree that any assessment of liquidated damages shall be construed and treated by the parties not as imposing a penalty upon the TO Contractor, but as liquidated damages to compensate the State for the TO Contractor's failure to complete the TO Agreement work, including Work Orders, in a timely manner.

A "Problem" is defined as any situation or issue reported via a Help Desk inquiry that is related to the System operation that is not an enhancement request.

"Problem resolution time" is defined as the period of time from when the Help Desk inquiry is opened to when it is properly resolved. Section 3.6.6.6 defines high, normal and low priority.

For purposes of SLA credit calculation, Monthly Charges are defined as the charges invoiced during the month of the breach for the relevant Monthly Fixed Unit Price, including any Increase to the Fixed Monthly Unit Price for additional monthly volume Incremental Unit(s), as set forth in Attachment 1, Price Sheet. For example, if there are 1,501 Help Desk inquiries in a given month where an SLA credit is due, the Monthly Charges would include the Fixed Monthly Unit Price, as defined in Part II A. (Help Desk) Fixed Monthly Unit Price *PLUS* the Increase to the Fixed Monthly Unit Price of one (1) Incremental Unit, as defined in Part III A. Increase to the Fixed Monthly Unit Price for Additional Help Desk Inquiries.

3.6.7.2 SLA Effective Dates

SLA for Start-up Period shall be in effect for each calendar day beyond 150 calendar days after the NTP Date for cutover from the current O & M Contractor to the TO Contractor.

All other SLAs set forth herein shall be in effect beginning with the commencement of monthly services as of the completion of the Start-up Period. The TO Contractor shall be responsible for complying with all performance measurements and shall also ensure compliance by all Subcontractors.

For any performance measurement not met during the monthly reporting period, the SLA credit for that individual measurement shall be applied to the Monthly Charges.

3.6.7.3 Service Level Reporting

The TO Contractor shall provide detailed monthly reports evidencing the attained level for each SLA set forth herein.

The TO Contract Monitor or designee will monitor and review TO Contractor performance standards on a monthly basis, based on TO Contractor-provided reports for this Task Order. The TO Contractor shall provide a monthly summary report for SLA performance via e-mail to the TO Contract Monitor and DHMH's Project Manager.

If any of the performance measurements are not met during the monthly reporting period, the TO Contract Monitor or designee will notify the TO Contractor of the standard that is not in compliance.

3.6.7.4 Credit for failure to meet SLA

TO Contractor's failure to meet an SLA will result in a credit, as liquidated damages and not as a penalty, to the Monthly Charges payable by the State during the month of the breach. The reductions will be cumulative for each missed service requirement. The State, at its option for amount due the State as liquidated damages, may deduct such from any money payable to the TO Contractor or may bill the TO Contractor as a separate item. In the result of a catastrophic failure affecting the entire System, all affected SLAs shall be credited to the State. In no event shall the aggregate of all SLA credits paid to the State in any calendar month exceed 25% of the Monthly Charges.

Example: If the Monthly Charges were $100,000 and one SLA were missed, with an applicable 4% credit, the credit to the monthly invoice would be $4,000, and the State would pay a net Monthly Charge of $96,000.

The reductions will be aggregated for each measurement of a service requirement. For example, if LTSS System Availability is measured at 99%, the resulting failure to meet stated SLA #7 for LTSS System Availability of 99.75% and 99.25% will result in a 2% credit for failure to meet 99.75% plus an additional 2% credit for failure to meet 99.25%, totaling a 4% credit against the Monthly Charges for that month.

Exception for Start-up Period: SLA #10 shall not be computed as a credit against the Monthly Charges, but shall instead be computed as a credit against the Start-up Period Fixed Fee set forth in Attachment 1 Price Sheet.

3.6.7.5 Root Cause Analysis

If the same SLA Service Requirement yields an SLA credit more than once, the TO Contractor shall conduct a Root Cause Analysis. Such Root Cause Analysis shall be provided within thirty (30) calendar days of the second breach and every breach thereafter.

3.6.7.6 Service Level Measurements Table (System performance)

The TO Contractor shall comply with the service level measurements in the following tables.

Operations – Help Desk SLAs:

Operations – Help Desk SLA credit is applied to the Part II A. Fixed Monthly Unit Price Operations – Help Desk and Part III A. Increase to the Fixed Monthly Price for Additional Help Desk Inquiries lines of the Attachment 1 Price Sheet.

ID #	Service Requirement	Measurement	SLA	SLA Credit
1	Problem Resolution Time - High	Resolution Time for each High Priority Problem Problem resolution time is defined as the period of time from when the Help Desk inquiry is opened to when it is properly resolved. Section 3.6.6.6 defines high, normal and low priority.	98% < 4 hours	1%
2	Problem Resolution Time - Normal	Resolution Time for Normal Priority Problems	98% < 24 hours	1%
3	Problem Resolution Time - Low	Resolution Time for Low Priority Problems	98% < 72 hours	1%
4	Help Desk Operations – Daily Email & Voicemail	Time for Help Desk to Create an Inquiry for Email & Voicemail (90% goal)	90% < 1 Business Day	2%
5	Help Desk Operations – Backlog Email & Voicemail	Time for Help Desk to Create an Inquiry for Email & Voicemail (98% goal)	98% < 3 Business Days	2%

Operations – Claims SLAs:

Operations – Claims SLA credit is applied to the Part II B. Fixed Monthly Unit Price for BASE-Level Operations – Claims or Part V B. Fixed Monthly Unit Price for EXPANDED Operations Claims, whichever is effective during the month, and Part III B. Increase to the Fixed Monthly Unit Price for Additional Claims lines of the Attachment 1 Price Sheet.

ID #	Service Requirement	Measurement	SLA	SLA Credit
6	Claims Operations – Claims Payment Submission Cycles	100% of cycles for payment submission shall be processed for payment submission within that claim's billing cycle. Payment submission cycles are treated as separate occurrences. Currently, DHMH's claims payment submission cutoff is 3:00 PM EST each Thursday, unless DHMH issues guidance for a deviation to the schedule due to holiday schedule or other need.	Per occur-rence	2%

Hosting SLAs:

Hosting SLA credit is applied to the following: <u>Part II D. Fixed Monthly Unit Price Hosting – IVR</u> and <u>Part III C. Increase to the Fixed Monthly Unit Price for Additional IVR Calls</u> (if IVR is affected); or, <u>Part II E. Fixed Monthly Unit Price for BASE-Level Managed Hosting Services</u> or <u>Part V A. Fixed Monthly Price for EXPANDED Managed Hosting Services</u> (whichever is effective during the month) lines of the Attachment 1 Price Sheet. The SLA Credit shall apply to the Hosting services line(s) depending on which components are not meeting the requirements.

ID #	Service Requirement	Measurement	SLA	SLA Credit
7	System Availability	The LTSS System (including IVR) shall be available 24x7x365, unless DHMH approves scheduled downtime for maintenance. All application functions and accessibility shall be maintained at 99.8% uptime performance levels. Contractor shall minimize or eliminate unscheduled network downtime to .2% or less. Scheduled maintenance that is pre-approved by DHMH as requiring an outage does not count against uptime. The SLA Credits for this Measurement are aggregated, i.e. each lower level of failure adds the stated additional percentage (for a maximum 10% credit).	99.8% to 99.5%	2%
			99.49% to 99.0%	+2%
			98.99% to 98.5%	+3%
			98.49% or less	+3%
8	System Response Time Issue Resolution	System response time issues shall be resolved within four (4) hours of confirmation that the issue is related to hosting that is within the TO Contractor's purview. The LTSS System and IVR call transactions shall be processed within one (1) second of the established response time baseline for transactions that do not change data and transmitted within a three (3) seconds of the established response time baseline for transactions that do change data. The baseline response time shall be established prior to cutover. Response time is measured on an ad hoc basis when requested by DHMH. The response time test script shall be processed by the Help Desk, monitored by TO Contractor and DHMH (refer to Section 3.6.5.25 for minimum requirement).	4 to 12 hours	1%
			> 12 to 24 hours	+1%
			> 24 to 48 hours	+3%
			> 48 hours	+5% credit

ID #	Service Requirement	Measurement	SLA	SLA Credit
		The SLA Credits for this Measurement are aggregated, i.e. each lower level of failure adds the stated additional percentage (for a maximum 10% credit).		
		As determined through Root Cause Analysis (RCA), defects and/or inefficiencies confirmed by DHMH to be the fault of the custom LTSS software or functions outside the control of the TO Contractor is excluded from the SLA.		
9	System Recovery	In the event of a declared disaster the recovery time objective of the System is forty-eight (48) hours. The System should be fully operation and available.	48 to 72 hours	5%
			> 72 to 96 hours	+10%
		The SLA Credits for this Measurement are aggregated, i.e. each lower level of failure adds the stated additional percentage (for a maximum 25% credit).	> 96 hours	+10%

Start-up Period SLA:

Start-up SLA credit is applied to the Part I. Deliverable Based Subtotal – Start-up Period line of the Attachment 1 Price Sheet.

ID #	Service Requirement	Measurement	SLA	SLA Credit
10	LTSS System Cutover – Over 150 calendar days	LTSS System shall be cutover from the current O&M contractor to the TO Contractor and accepted by DHMH within 150 calendar days from NTP. The SLA Credits for this Measurement are aggregated, for a maximum 25% credit.	Each calendar day beyond 150 days past the NTP Date	1%

3.6.8   BACKUP / DISASTER RECOVERY

As part of the Hosting activities provided under this Task Order, the TO Contractor shall furnish the following:

ID #	Backup and COOP	Associated Deliverable ID #
3.6.8.1	TO Contractor shall provide all necessary planning and activities necessary to ensure continued LTSS System operations in accordance with the Service Requirement Measurements set forth in Section 3.6.7.6.	3.8.4.11
3.6.8.2	TO Contractor shall document all backup and disaster recovery procedures in a Continuity of Operations (COOP) plan.	3.8.4.11
3.6.8.3	The COOP Plan shall be updated no less than once annually, and within ten (10) days of a significant change in operations that impact backups, disaster recovery, or other COOP procedures.	3.8.4.11
3.6.8.4	TO Contractor shall provide the COOP Plan in hard and soft copy to DHMH and shall provide DHMH with up-to-date copies within ten (10) business days when changes are required.	3.8.4.11
3.6.8.5	The COOP plan shall include: a. Objectives of the plan b. Situations and conditions covered by the plan c. Disaster declaration process d. Executing the COOP plan e. Technical considerations f. Roles and responsibilities of Contractor staff and DHMH personnel g. How and when to notify the Department's TO Contract Monitor and DHMH's Project Manager h. Recovery procedures (disaster recovery) i. Data backup, to include: i. the configuration of online backup procedures, ii. the configuration of export procedures, iii. the configuration of import procedures, iv. maintenance of archived data, v. scheduling and performance of backups, vi. monitoring of backup logs, vii. recovery of databases with their required structures and objects, and viii. secure off-site storage of all critical transactions and data j. Procedures for deactivating the COOP plan	3.8.4.11
3.6.8.6	TO Contractor shall provide in the COOP plan contact information for personnel who can be contacted and reachable 365x24x7, for COOP purposes.	3.8.4.11

ID #	Backup and COOP	Associated Deliverable ID #
3.6.8.7	The COOP plan shall be approved by DHMH's Project Manager and include the restoration of the site, in its entirety, from stored backups.	3.8.4.11
3.6.8.8	TO Contractor shall provide a Secondary Data Center sufficient for fully supporting the LTSS System in the event the Primary Date Center is disabled. The secondary site shall include Uninterruptable Power Source (UPS), voice, data and telecommunications circuit provisioning.	3.8.4.5 3.8.4.11
3.6.8.9	TO Contractor shall perform backups of all servers at on a regular basis according to industry standards. This shall include daily incremental backups and full weekly backups of all volumes of servers.	3.8.4.5 3.8.4.11
3.6.8.10	TO Contractor shall ensure that current, historical, and archived data, tables, and files in the System are protected in an off-site location approved by DHMH to mitigate the risk of a natural or man-made disaster.	3.8.4.5 3.8.4.11
3.6.8.11	TO Contractor shall ensure that all back-up files are encrypted. The key for encryption shall not be stored with the System backup files and data. The encryption process shall be performed and verified prior to shipping the files and data backups off-site. DHMH reserves the right to audit the back-up process at its discretion.	3.8.4.5 3.8.4.11
3.6.8.12	TO Contractor shall perform an annual COOP test, involving the loading and recovery of the data backup media and shall include, at a minimum, the verification of data integrity.	3.8.4.11 3.8.4.17
3.6.8.13	TO Contractor shall execute the COOP test at no additional cost to DHMH. DHMH reserves the right to waive part or all or the demonstration. In the event that the TO Contractor's demonstration fails to meet the stated goals and objectives of the demonstration, TO Contractor shall continue to execute the demonstration until satisfactory to DHMH, at no additional cost.	3.8.4.11 3.8.4.17
3.6.8.14	TO Contractor shall perform an annual review of the DR procedures for all off-site storage and validation of security procedures. A report of the DR procedures review shall be submitted within fifteen (15) business days of the review. DHMH reserves the right to inspect the Secondary Data Center at any time with 24-hour notification.	3.8.4.11 3.8.4.18
3.6.8.15	TO Contractor shall provide check point/restart capabilities and other features necessary to ensure reliability and recovery, including	3.8.4.5 3.8.4.11

ID #	Backup and COOP	Associated Deliverable ID #
	telecommunications for voice and data circuits in the event of a disaster. These checkpoint/restart capabilities shall be documented in the COOP plan.	
3.6.8.16	TO Contractor shall provide detailed instructions for installation and recovery of the System including operating system, applications, voice, data and Help Desk.	3.8.4.11
3.6.8.17	TO Contractor shall include detailed instructions for the rotation to the Secondary Data Center. Procedures shall be specified for updating off-site materials.	3.8.4.11

3.6.9   REQUIREMENTS FOR HARDWARE, SOFTWARE, AND MATERIALS

TO Contractor shall provide all necessary COTS software, hardware and networking technologies to provide managed hosting services for DHMH's LTSS System. Material costs shall be passed through with no mark-up by the TO Contractor, per CATS+ Master Contract RFP from Section 2.2.1.

3.7   PERFORMANCE AND PERSONNEL

3.7.1   WORK HOURS

A. State Business Hours Support: The TO Contractor's collective assigned Personnel shall support core State business hours (7:00 AM to 6:00 PM), Monday through Friday except for State holidays, Service Reduction days, and Furlough days observed by DHMH. TO Contractor Personnel may also be required to provide occasional support outside of core business hours, including evenings, overnight, and weekends, to support specific efforts and emergencies to perform maintenance and/or software releases, resolve system repair or restoration.

B. Help Desk Hours: The Help Desk has supports two types of users: LTSS and ISAS. Help Desk services shall be provided Monday through Friday, excluding State observed holidays (note that Help Desk is expected to be in operation during Service Reduction days and Furlough days), during the following hours:

   o Regular business hours, 9:00 AM to 5:00 PM Eastern Standard Time, for the LTSS Help Desk
   o Extended business hours, 6:00 AM to 8:00 PM Eastern Standard Time, for the ISAS Help Desk

The Department prefers a centralized Help Desk operation. However, Help Desk representatives may work from home with written approval from DHMH. TO Contractor shall ensure compliance with Attachment 21 Work-from-Home Help Desk Representative Security Policy.

C. Non-Business Hours Support: After hours support may be necessary to respond to IT Security emergency situations. Additionally, services may also involve some evening and/or weekend hours in addition to core business hours to perform planned activities.

D. <u>State-Mandated Service Reduction Days</u>: TO Contractor Personnel shall be required to participate in the State-mandated Service Reduction Days as well as State Furlough Days. In this event, the TO Contractor will be notified in writing by the TO Contract Monitor of these details.

3.7.2   DIRECTED PERSONNEL REPLACEMENT

A. The TO Contract Monitor may direct the TO Contractor to replace any TO Contractor Personnel who, in the sole discretion of the TO Contract Monitor, are perceived as being unqualified, non-productive, unable to fully perform the job duties, disruptive, or known, or reasonably believed, to have committed a major infraction(s) of law or Department, Contract, or Task Order requirement.

B. If deemed appropriate in the discretion of the TO Contract Monitor, the TO Contract Monitor shall give written notice of any TO Contractor Personnel performance issues to the TO Contractor, describing the problem and delineating the remediation requirement(s). The TO Contractor shall provide a written Remediation Plan within three (3) days of the date of the notice. If the TO Contract Monitor rejects the Remediation Plan, the TO Contractor shall revise and resubmit the plan to the TO Contract Monitor within five (5) days of the rejection, or in the timeframe set forth by the TO Contract Monitor in writing. After a Remediation Plan has been accepted in writing by the TO Contract Monitor, the TO Contractor shall immediately implement the Remediation Plan.

C. If performance issues persist despite the approved Remediation Plan, the TO Contract Monitor will give written notice of the continuing performance issues and either request a new Remediation Plan within a specified time limit or direct the removal and replacement of the TO Contractor Personnel whose performance is at issue. A request for a new Remediation Plan will follow the procedure described in Section 3.7.2B.

D. In circumstances of directed removal, the TO Contractor shall provide a suitable replacement for TO Contract Monitor approval within fifteen (15) days of the date of the notification of directed removal, or the actual removal, whichever occurs first, or such earlier time as directed by the TO Contract Monitor in the event of a removal on less than fifteen (15) days notice

E. Normally, a directed personnel replacement will occur only after prior notification of problems with the requested remediation, as described above. However, the TO Contract Monitor reserves the right to direct immediate personnel replacement without using the remediation procedure described above.

F. Replacement or substitution of TO Contractor Personnel under this Section shall be in addition to, and not in lieu of, the State's remedies under the Task Order or which otherwise may be available at law or in equity.

3.7.3   SUBSTITUTION OF PERSONNEL

3.7.3.1 PRIOR TO AND 30 DAYS AFTER TASK ORDER EXECUTION

Prior to Task Order Execution or within thirty (30) days after Task Order Execution, the Offeror may substitute proposed Key Personnel only under the following circumstances: vacancy occurs due to the sudden termination, resignation, or approved leave of absence due to an Extraordinary Personnel Event, or death of such personnel. To qualify for such substitution, the Offeror must describe to the State's satisfaction the event necessitating substitution and must demonstrate that the originally proposed personnel are actual full-time direct employees with the Offeror

(subcontractors, temporary staff or 1099 contractors do not qualify). Proposed substitutes shall be of equal caliber or higher, in the State's sole discretion. Proposed substitutes deemed by the State to be less qualified than the originally proposed individual may be grounds for pre-award disqualification or post-award termination.

An **Extraordinary Personnel Event** means Leave under the Family Medical Leave Act; an incapacitating injury or incapacitating illness, or other circumstances that in the sole discretion of the State warrant an extended leave of absence, such as extended jury duty or extended military service.

3.7.3.2 SUBSTITUTION POST 30 DAYS AFTER TASK ORDER EXECUTION

The procedure for substituting personnel after Task Order execution is as follows:

A) The TO Contractor may not substitute personnel without prior approval of the TO Contract Monitor.

B) To replace any personnel, the TO Contractor shall submit resumes of the proposed individual specifying the intended approved labor category. Any proposed substitute personnel shall have qualifications equal to or better than those of the replaced personnel.

C) The proposed substitute individual shall be approved by the TO Contract Monitor. The TO Contract Monitor shall have the option to interview the proposed substitute personnel and may require that such interviews be in person. After the interview, the TO Contract Monitor shall notify the TO Contractor of acceptance or denial of the requested substitution. If no acceptable substitute personnel is proposed within the time frame established by the TO Contract Monitor, the TO Agreement may be cancelled.

3.7.4   PREMISES AND OPERATIONAL SECURITY

A) TO Contractor Personnel may be subject to random security checks during entry and exit of State secured areas. The State reserves the right to require TO Contractor Personnel to be accompanied while on secured premises.

B) TO Contractor Personnel shall, while on State premises, display their State issued identification cards without exception.

C) TO Contractor Personnel shall follow the State of Maryland IT Security Policy and Standards throughout the term of the TO Agreement.

D) The State reserves the right to request that the TO Contractor submit proof of employment authorization for non-United States citizens, prior to commencement of TO Contractor Personnel work under the Task Order.

E) TO Contractor shall remove any TO Contractor Personnel from working on the resulting TO Agreement where the State of Maryland determines that said TO Contractor Personnel has not adhered to the security requirements specified herein.

F) The cost of complying with all security requirements specified herein are the sole responsibility and obligation of the TO Contractor and its Subcontractors and no such costs shall be passed through to or reimbursed by the State or any of its agencies or units.

3.7.5 WORK SPACE, WORKSTATIONS, NETWORK CONNECTIVITY AND SOFTWARE

The TO Contractor will provide all necessary office space, network connectivity and required workstation hardware/software necessary to complete the requirements of this Task Order.

3.8 DELIVERABLES

3.8.1 DELIVERABLE SUBMISSION

For every deliverable, the TO Contractor shall request that the TO Contract Monitor confirm receipt of that deliverable by sending an e-mail identifying the deliverable name and date of receipt.

For every deliverable the TO Contractor shall submit by e-mail an Agency Deliverable Product Acceptance Form (DPAF), provided as Attachment 8, to the TO Contract Monitor in MS Word (2007 or greater).

Unless specified otherwise, written deliverables shall be compatible with Microsoft Office, Microsoft Project and/or Microsoft Visio versions 2007 or later. At the TO Contract Monitor's discretion, the TO Contract Monitor may request one hard copy of a written deliverable.

A standard deliverable review cycle will be elaborated and agreed-upon between the State and the TO Contractor. This review process is entered into when the TO Contractor completes a deliverable.

For any written deliverable, the TO Contract Monitor may request a draft version of the deliverable, to comply with the minimum deliverable quality criteria listed in Section 3.8.3. Drafts of each final deliverable, except status reports, are required at least two weeks in advance of when the final deliverables are due (with the exception of deliverables due at the beginning of the project where this lead time is not possible, or where draft delivery date is explicitly specified). Draft versions of a deliverable shall comply with the minimum deliverable quality criteria listed in Section 3.8.3.

3.8.2 DELIVERABLE ACCEPTANCE

A final deliverable shall satisfy the scope and requirements of this TORFP for that deliverable, including the quality and acceptance criteria for a final deliverable as defined in Section 3.8.4 Deliverable Descriptions/Acceptance Criteria.

The TO Contract Monitor shall review a final deliverable to determine compliance with the acceptance criteria as defined for that deliverable. The TO Contract Monitor is responsible for coordinating comments and input from various team members and stakeholders. The TO Contract Monitor is responsible for providing clear guidance and direction to the TO Contractor in the event of divergent feedback from various team members.

The TO Contract Monitor will issue to the TO Contractor a notice of acceptance or rejection of the deliverable in the DPAF (Attachment 8). Following the return of the DPAF indicating "Accepted" and signed by the TO Contract Monitor, the TO Contractor shall submit a proper invoice in accordance with the procedures in Section 3.10 Invoicing.

In the event of rejection of a deliverable, the TO Contract Monitor will formally communicate in writing any deliverable deficiencies or non-conformities to the TO Contractor, describing in those deficiencies what shall be corrected prior to acceptance of the deliverable in sufficient detail for the TO Contractor to address the deficiencies. The TO Contractor shall correct deficiencies and resubmit the corrected deliverable for acceptance within the agreed-upon time period for correction.

At the TO Contract Monitor's discretion, subsequent project tasks may not continue until deliverable deficiencies are rectified and accepted by the TO Contract Monitor or the TO Contract Monitor has specifically issued, in writing, a waiver for conditional continuance of project tasks.

3.8.3   MINIMUM DELIVERABLE QUALITY

The TO Contractor shall subject each deliverable to its internal quality-control process prior to submitting the deliverable to the State.

Each deliverable shall meet the following minimum acceptance criteria:

A) Be presented in a format appropriate for the subject matter and depth of discussion.

B) Be organized in a manner that presents a logical flow of the deliverable's content.

C) Represent factual information reasonably expected to have been known at the time of submittal.

D) In each Section of the deliverable, include only information relevant to that Section of the deliverable.

E) Contain content and presentation consistent with industry best practices in terms of deliverable completeness, clarity, and quality.

F) Meets the acceptance criteria applicable to that deliverable, including any State policies, functional or non-functional requirements, or industry standards.

G) Contains no structural errors such as poor grammar, misspellings or incorrect punctuation.

A draft written deliverable may contain limited structural errors such as incorrect punctuation, and shall represent a significant level of completeness toward the associated final written deliverable. The draft written deliverable shall otherwise comply with minimum deliverable quality criteria above.

3.8.4   DELIVERABLE DESCRIPTIONS / ACCEPTANCE CRITERIA

The TO Contractor may suggest other subtasks, artifacts, or deliverables to improve the quality and success of the assigned tasks.

Start-up Period Deliverables:

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
3.8.4.1	Integrated Project Schedule	Format: Microsoft Project 2007 Microsoft Project schedule demonstrating tasks, task estimates, resource assignments, and dependencies for both Agency and TO Contractor Personnel, with tasks no less than 8 hours and no greater than 80 hours.	Initial Delivery: NTP+ 10 business days Updates: Weekly
3.8.4.2	Kick Off Meeting	Format: Microsoft Word 2007 Agreed upon agenda and presentation materials in Microsoft Office formats for kick-off meeting. The kick-off meeting materials shall cover: a. Introduction of personnel from the TO Contractor team and DHMH b. Review of work plan	Initial Delivery: NTP+ 5 business days

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
		c. Discussion of assumptions, risks and issues d. Logistics for communications e. Additional topics as determined necessary	
3.8.4.3	Beginning of Contract Transition Plan	Format: Microsoft Word 2007 Includes a planned approach for transitioning all Contract activities within the specified one hundred fifty (150) calendar day timeframe. The plan shall include the TO Contractor's: a. Proposed approach a. Technical Infrastructure Design confirmation findings, recommendations and prioritization b. Tasks, subtasks, and schedule for activities c. Organizational Governance Chart d. Project Team Organization Chart e. Contract list of all key personnel and executives involved in the project f. High-level timeline that encompasses all major project-related activities g. Identification of any potential risks or issues to timely implementation, and proposed mitigations h. A detailed description of a process for review, revision, and approval of all deliverables and project artifacts to be approved by DHMH	Initial Delivery: NTP+ 10 business days
3.8.4.4	Project Management Plan (PMP)	Format: Microsoft Word 2007 (PMP) The PMP shall include the following Sections / sub-plans: a. RACI Matrix and/or swim lane diagram depicting roles and responsibilities of the TO Contractor, Software Development Contractor and DHMH b. Scope Management c. Schedule Management d. Procurement Management e. Quality Management f. System Change Management and Configuration Management (software versions and licensing, code libraries, etc.) g. Staffing Management (including MBE requirements) h. Communications Management i. Issues and Risk Management	Initial Delivery: NTP+ 20 business days Updates: Within 20 business days of a change, annual updates at a minimum

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
		j. Assumptions k. Constraints	
3.8.4.5	Technical Operations Plan (TOP)	Format: Microsoft Word 2007; Visio 2007 (diagrams and schematics) TO Contractor shall have technical infrastructure networked with the Software Development Contractor's infrastructure. To support networking and integration, the TO Contractor shall provide a technical architecture (hardware, software, net gear, etc.) schematic of its technical infrastructure, roles and responsibilities of staff, methods and procedures for maintenance and operations of TO Contractor's technical infrastructure, and communications protocols. At a minimum, the TOP shall include: b. Technical Architecture Schematic c. Systems Monitoring d. Patch Management e. Maintenance Schedule f. Points-of-contact and Backups g. Technical Support h. Security i. HIPAA Compliance j. Database Replication k. Ad Hoc Reporting Repository l. Licensing and Warranty Tracking for Hardware and COTS Software m. Certificate Expiration Date Tracking n. Other items as mutually agreed upon	Initial Delivery: NTP+ 20 business days Updates: Within 20 business days of a change, annual updates at a minimum
3.8.4.6	Help Desk Operations Plan	Format: Microsoft Word 2007 TO Contractor shall include in their TO Technical Proposal their approach for Help Desk operations. TO Contractor shall provide their detailed plan for Help Desk Operations, including: a. Help Desk infrastructure (hardware and software) b. Staffing plan c. Metrics and key performance indicators (KPIs) d. System response time test script execution e. Knowledgebase maintenance f. Continuous improvement approach g. Escalation protocol	Initial Delivery: NTP+ 20 business days Updates: Within 20 business days of a change, annual updates at a minimum

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
		h. Contact information i. Other items as mutually agreed upon	
3.8.4.7	Claims & Interfaces Operations Plan	Format: Microsoft Word 2007 TO Contractor shall provide its detailed plan for Claims and Interfaces Operations, including: a. Claims process flow b. Claims reconciliation process and reporting c. Claims balancing reporting d. Batch transaction processing e. Batch schedule with timing and duration information f. Metrics and key performance indicators (KPIs) g. Interface matrix, listing each interface, source and destination, format, frequency, description, points-of-contact, etc. h. Continuous improvement approach i. Escalation protocol j. Contact information k. Other items as mutually agreed upon	Initial Delivery: NTP+ 20 business days Updates: Within 20 business days of a change, annual updates at a minimum
3.8.4.8	Defects Tracker	Format: Microsoft Excel 2007 List of known technical solution defects by tracking number, severity, brief description, disposition and target implementation date (required for 1 – Critical and 2 – High defects, optional for 3 – Medium and 4 – Low defects).	Initial Delivery: NTP+ 20 business days Updates: Weekly
3.8.4.9	Technical Infrastructure Test Master Plan	Format: Microsoft Word 2007 Microsoft Word document that provides the Technical Infrastructure Test Master Plan fully in accordance with required State SDLC Methodology. At a minimum, the Technical Infrastructure test process shall address performance (including baseline system response time as discussed in Section 3.6.5.26), load and stress on all impacted system components. Technical Infrastructure testing shall be executed prior to the cutover from current O&M contractor to TO Contractor.	Initial Delivery: NTP+ 20 business days
3.8.4.10	LTSS Code Library Management Plan	Format: Microsoft Word 2007 The LTSS Code Library Management Plan describes the TO Contractor's approach, tools, coordination with the Software Development Contractor, and roll	Initial Delivery: NTP+ 20 business days

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
		back procedures if a software deployment requires reverting to a prior version of the LTSS software.	
3.8.4.11	COOP Plan	Format: Microsoft Word 2007 The COOP shall describe the TO Contractor's protocols, including communications with DHMH, for interruptions in normal business operations. The COOP shall include a Section describing Disaster Recovery processes, methodology, resources and key performance metrics. This Section shall explain how the TO Contractor will mitigate downtime and ensure COOP protocols are in place for the LTSS System and the TO Contractor's hosting and operations.	Initial Delivery: NTP+ 30 business days Updates: Within 10 business days of a change, annual updates at a minimum.
3.8.4.12	Hosting and Operations Cutover Readiness Meeting	TO Contractor shall hold one (1) or, at the discretion of the Department, more meeting(s) during which the TO Contractor shall present its readiness for cutover and certify that the hosting and operations cutover is ready for Go-Live.	Initial Delivery: Within 30 calendar days prior to the scheduled cutover date
3.8.4.13	Hosting and Operations Cutover	TO Contractor shall certify that the hosting and operations cutover is completed. The LTSS System is "Live" on the TO Contractor's technical infrastructure and O&M tasks and responsibilities are under their purview. LTSS System shall be fully operational, including all technical components (e.g. web-based, IVR, toll-free numbers) and connectivity for interfaces and claims processing. Hosting and operations cutover requires DHMH's approval prior to TO Contractor exiting the Start-up Period phase.	NTP+ 150 calendar days
3.8.4.14	Claims Operations COTS Software Plan	Format: Microsoft Word 2007 Identifies proposed COTS software that meets requirements in Section 3.6.6.23. Describes in detail the features, capabilities and system requirements for the proposed solution. Includes sample reports, screenshots and detailed description for operational use of the solution in supporting the TO Contractor's claims operations support services.	NTP+ 60 calendar days

Deliverables for Each Software Release Deployment or LTSS System Change:

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
3.8.4.15	Detailed Deployment Strategy and Work Plan	Format: Microsoft Word 2007 and Microsoft Project 2007 (work plan) Description of activities, processes, roles, responsibilities, rollback procedures and hour-by-hour timeframes of the deployment of a "go live" and/or major software release. Contact information of all key personnel involved in the deployment, including decision-making personnel is mandatory.	Within 10 business days prior to software release "go live" or in an alternate timeframe as deemed necessary by DHMH
3.8.4.16	System Documentation Updates	Format: Microsoft Word 2007 Updates to Technical Manuals and other reference material related to hosting and operations.	Within 5 business days prior to "go live"
3.8.4.17	Help Desk Training and Knowledgebase Updates	Format: Microsoft Word 2007 or PowerPoint 2007 The Software Development Contractor is responsible for providing release notes and, in some cases, training to the Help Desk on each software release. The TO Contractor shall collaborate with the Software Development Contractor and implement the updates to the knowledge base, including updated scripts for the Help Desk staff.	Within 5 business days prior to "go live"

Additional Deliverables:

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
3.8.4.18	Annual COOP Test	Format: Microsoft Word 2007, Excel 2007 and Microsoft Project 2007 (work plan) On an annual basis, the TO Contractor shall conduct a test of its COOP plan, including DR executed through a live exercise of the systems, facilities and personnel. COOP Test Plan – shall contain information that defines tasks, roles and responsibilities, timelines, communications, verification process and goals and objectives of the Annual COOP Test. COOP Test Plan – within ten (10) business days before the start of the COOP Test. The Annual COOP Test includes three components – the test plan, the execution and the after-action report. COOP Test After Action Report – identifies the results of the Annual COOP Test, including areas for improvement and recommended changes. COOP Test	Conducted annually, at least 20 business days prior to the end of the TO Agreement year

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
		After Action Report – within ten (10) Business Days after the conclusion of the test.	
3.8.4.19	End of Contract Transition Plan	Format: Microsoft Word 2007 Defines tasks, roles & responsibilities, timelines, communications, and processes to transition TO Contractor's activities to a new contractor, DHMH or other party identified by DHMH.	At the Department's discretion, usually within four (4) months before end of Contract term

Reports:

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
3.8.4.20	Monthly Performance Report	Format: Microsoft Word 2007 and Excel 2007 TO Contractor shall provide a Monthly Performance Report that includes the following Sections: a. Database Metrics and Performance b. Technical Solution Metrics and Performance c. Claims, Batch Transaction and Interfaces Operations (summary of the claims and interface file activity, balance reports and reconciliation reports) d. Help Desk Operations e. SLA compliance	Every month by the 5th business day of the following month
3.8.4.21	Monthly Progress Reports	Format: Microsoft Word 2007 and Excel 2007 Document coordinated with monthly schedule updates. The Monthly Progress Reports shall include: a. Updated deliverables tracking matrix b. Updated Issues / Risks reporting c. Financial update, based on deliverables d. Updated staffing plan e. Performance reporting with metrics for schedule, budget, staffing, quality and scope f. Other items as mutually agreed upon	Every month by the 5th business day of the following month
3.8.4.22	Monthly SLA reports	Format: Microsoft Word 2007 and Excel 2007 Any additional reports necessary to demonstrate meeting the SLAs set forth in Section 3.6.7.	Every month by the 5th business day of the following month

(OPTION) Database Support Services Deliverable: This deliverable applies only to those prospective bidders interested in proposing a solution to meet the Department's needs. If these services are not included as part of the TO Technical Proposal, prospective bidders should indicate "SERVICES NOT PROPOSED".

ID #	Deliverable	Acceptance Criteria	Due Date/Frequency
3.8.4.23	Monthly Database Support Report	Format: Microsoft Word 2007 and Excel 2007 TO Contractor shall provide a Monthly Database Support Report that includes the following Sections: a. Database and replication metrics b. Summary of Status c. Issues and/or Risks d. Tasks Completed e. Tasks Planned	Every month by the 5th business day of the following month

3.9   WORK ORDER PROCESS

A) Additional services and/or resources will be provided via a Work Order process and will be issued for fixed price pricing and be deliverables based.

B) The TO Contract Monitor shall e-mail a Work Order Request (See Attachment 16) to the TO Contractor to provide services or resources that are within the scope of this TORFP. The Work Order Request will include:

1) Technical requirements and description of the service or resources needed
2) Performance objectives and/or deliverables, as applicable
3) Due date and time for submitting a response to the request
4) Required place(s) where work must be performed

C) The TO Contractor shall e-mail a response to the TO Contract Monitor within the specified time and include at a minimum:

1) A response that details the TO Contractor's understanding of the work;
2) A price to complete the Work Order Request using the format provided in Attachment 16;
3) A description of proposed resources required to perform the requested tasks;
4) An explanation of how tasks shall be completed. This description shall include proposed subcontractors and related tasks;
5) State-furnished information, work site, and/or access to equipment, facilities, or personnel; and
6) The proposed personnel resources, including any subcontractor personnel, to complete the task.

D) The TO Contract Monitor will review the response and will confirm the proposed labor rates are consistent with this TORFP. For a fixed price Work Order, the TO Contract Monitor will review the response and will confirm the proposed prices are acceptable.

E) The TO Contract Monitor may contact the TO Contractor to obtain additional information, clarification or revision to the Work Order, and will provide the Work Order to the TO Procurement Officer for a determination of compliance with the TO and a determination whether a change order is appropriate. Written TO Procurement Officer approval is required before Work Order execution by the State.

F) Proposed personnel on any type of Work Order shall be approved by the TO Contract Monitor. The TO Contractor shall furnish resumes of proposed personnel. The TO Contract Monitor shall have the option to interview the proposed personnel and, in the event of an interview or not, shall notify the TO Contractor of acceptance or denial of the personnel.

G) Performance of services under a Work Order shall commence consistent with an NTP issued by the TO Contract Monitor for such Work Order.

3.10   INVOICING

A. Invoice payments to the TO Contractor shall be governed by the terms and conditions defined in the CATS+ Master Contract.

B. Proper invoices for payment shall be submitted to the TO Contract Monitor for payment approval as described below. Invoices shall be submitted monthly.

C. Invoicing for BASE services shall not commence until Department acceptance of initial services during Start-Up period.

D. Invoices for EXPANDED services shall not commence until the Department accepts the TO Contractor is ready to furnish EXPANDED services under this Contract.

3.10.1   INVOICE SUBMISSION PROCEDURE

A) Proper invoices for payment shall contain the TO Contractor's Federal Tax Identification Number, "DHMH" as the recipient, date of invoice, TO Agreement number, invoiced item description, invoiced item number (e.g.,"2.7.4.1."), period of performance covered by the invoice, a total invoice amount, and a TO Contractor point of contact with telephone number.

B) All invoices submitted for payment shall be accompanied by signed notice(s) of acceptance as described below. Payment of invoices will be withheld if the appropriate signed acceptance form documentation is not submitted.

1) To be considered a proper Fixed Price invoice with deliverables (for Task Order requirements and for fixed price Work Orders issued under this Task Order) the TO Contractor shall include with the signed invoice a signed DPAF (Attachment 9) for each deliverable invoiced. Payment will only be made upon completion and acceptance of the deliverables as defined in Section 3.8.

2) To be considered a proper Fixed Price invoice for services and reports. The TO Contractor shall include with the signed invoice a list of reports delivered in this invoice period.

C) The TO Contractor shall mail the original of each invoice and signed notice(s) of acceptance to the TO Requesting Agency; DHMH/Office of Health Services, Attention: Jane Holman, 201 W. Preston Street, Room 117, Baltimore, MD 21201.

D) Invoices for final payment shall be clearly marked as "FINAL" and submitted when all work requirements have been completed and no further charges are to be incurred under the TO Agreement. In no event shall any invoice be submitted later than sixty (60) calendar days from the TO Agreement termination date.

3.10.2   For the purposes of this Task Order an amount will not be deemed due and payable if:

A) The amount invoiced is inconsistent with the Task Order Agreement.

B) The proper invoice has not been received by the party or office specified in the Task Order Agreement.

C) The invoice or performance under the contract is in dispute or the TO Contractor has failed to otherwise comply with the provisions of the Task Order Agreement

D) The item or services have not been accepted.

E) The quantity of items delivered is less than the quantity ordered.

F) The items or services do not meet the quality requirements of the Task Order

G) If the Contract provides for progress payments, the proper invoice for the progress payment has not been submitted pursuant to the schedule contained in the agreement

H) The Contractor has not submitted satisfactory documentation or other evidence reasonably required by the TO Procurement Officer or by the contract concerning performance under the Task Order Agreement and compliance with its provisions.

3.11   RETAINAGE

THIS SECTION IS NOT APPLICABLE TO THIS TORFP.

3.12   SOC 2 TYPE II AUDIT

3.12.1   This clause applies to the TO Contractor and Subcontractors who host the implemented LTSS System for the State. The TO Contractor and/or Subcontractors who provide services that handle Sensitive Data (see definition of Handle in Section 1.20) for the LTSS System must also comply with this clause, assuming the TO Contractor and/or Subcontractor receives copies of any data for use in providing services, including any system and/or user acceptance testing of the new System and any provided data that contains Sensitive Data.

3.12.2   The TO Contractor shall have an annual audit performed by an independent audit firm of the TO Contractor and/or Subcontractors' handling of Sensitive Data and/or the Department's critical functions, which is identified as the LTSS System and shall address all areas relating to information technology security and operational processes. These services provided by the TO Contractor and/or Subcontractors that shall be covered by the audit will collectively be referred to as the "Information Functions and/or Processes." Such audits shall be performed in accordance with audit guidance: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) as published by the American Institute of Certified Public Accountants (AICPA) and as updated from time to time, or according to the most current audit guidance promulgated by the AICPA or similarly-recognized professional organization, as agreed to by the Department, to assess the security of outsourced client functions or data (collectively, the "Guidance") as follows: The type of audit to be performed in accordance with the Guidance is a SOC 2 Type 2 Audit (referred to as the "SOC 2 Report"). The initial SOC 2 Report audit shall be scheduled and completed within a timeframe to be specified by the State and submitted to the TO Agreement Manager. All subsequent SOC 2 audits that are arranged after this initial audit shall be performed on an annual basis.

3.12.2.1   The SOC 2 Report shall report on the description of the TO Contractor and/or Subcontractors' system and controls and the suitability of the design and operating effectiveness of controls over the Information Functions and/or Processes relevant to the following trust principles: Security, Availability, Confidentiality, and Privacy as defined in

the aforementioned Guidance. The SOC 2 Report should also report on the suitability of the design and operating effectiveness of controls of the Information Functions and/or Processes to meet the requirements of the TO Agreement, specifically the security requirements identified in Section 3.14.

3.12.2.2   The audit scope of each year's SOC 2 Report may need to be adjusted (including the inclusion or omission of the relevant trust services principles of Security, Availability, Confidentiality, Processing Integrity, and Privacy) to accommodate any changes to the TO Contractor's and/or Subcontractors' environment since the last SOC 2 Report. Such changes may include but are not limited to the addition of Information Functions and/or Processes through change orders or Work Orders under the TO Agreement; or, due to changes in information technology or operational infrastructure implemented by the TO Contractor and/or Subcontractors. The TO Contractor and/or Subcontractors shall ensure that the audit scope of each year's SOC 2 Report engagement shall accommodate these changes by including in SOC 2 Report all appropriate controls related to the current environment supporting the Information Functions and/or Processes, including those controls required by the TO Agreement.

3.12.2.3   The scope of the SOC 2 Report shall include work performed by any Subcontractors that provide essential support to the TO Contractor and/or essential support to the Information Functions and/or Processes provided to the Department under the TO Agreement. The TO Contractor shall ensure the audit includes all of these Subcontractor(s) in the performance of the SOC 2 Report.

3.12.2.4   All SOC 2 Reports, including those of the TO Contractor and/or Subcontractor, shall be performed at no additional expense to the Department.

3.12.2.5   The TO Contractor and/or Subcontractors shall promptly provide a complete copy of the final SOC 2 Report to the TO Contract Monitor upon completion of each annual SOC 2 Report engagement.

3.12.2.6   The TO Contractor shall provide to the TO Contract Monitor, within 30 calendar days of the issuance of each annual final SOC 2 Report, a documented corrective action plan which addresses each audit finding or exception contained in the SOC 2 Report. The corrective action plan shall identify in detail the remedial action to be taken by the TO Contractor and/or Subcontractors along with the date(s) when each remedial action is to be implemented.

3.12.2.7   If the TO Contractor and/or Subcontractors currently have an annual information security assessment performed that includes the operations, systems, and repositories of the products/services being provided to the Department under the TO Agreement, and if that assessment generally conforms to the content and objective of the Guidance, the Department will determine in consultation with appropriate State government technology and audit authorities whether the TO Contractor and/or Subcontractors' current information security assessments are acceptable in lieu of the SOC 2 Report.

3.12.2.8   If the TO Contractor and/or Subcontractors fail during the TO Agreement term to obtain an annual SOC 2 Report by the date specified in 3.12.2.1, the Department shall have the right to retain an independent audit firm to perform an audit engagement of a SOC 2

Report of the Information Functions and/or Processes being provided by the TO Contractor and/or Subcontractors. The TO Contractor and/or Subcontractors agree to allow the independent audit firm to access its facility/ies for purposes of conducting this audit engagement(s), and will provide the support and cooperation to the independent audit firm that is required to perform the SOC 2 Report. The Department will invoice the TO Contractor for the expense of the SOC 2 Report(s), or deduct the cost from future payments to the TO Contractor.

3.13   INSURANCE

Offeror shall confirm that, as of the date of its TO Technical Proposal, the insurance policies incorporated into its Master Contract are still current and effective at the required levels (See Master Contract Section 2.7).

The Offeror shall also confirm that any insurance policies intended to satisfy the requirements of this TORFP are issued by a company that is licensed to do business in the State of Maryland. The recommended awardee must provide a certificate(s) of insurance with the prescribed coverages, limits and requirements set forth in this Section 3.13 "Insurance" within five (5) Business Days from notice of recommended award. During the period of performance for multi-year contracts the TO Contractor shall update certificates of insurance annually, or as otherwise directed by the TO Contract Monitor.

3.13.1   CYBER SECURITY / DATA BREACH INSURANCE

In addition to the insurance specified in the Master Contract Section 2.7, TO Contractor shall maintain Cyber Security / Data Breach Insurance in the amount of ten million dollars ($10,000,000) per occurrence. The coverage must be valid in at all locations where work is performed or data or other information concerning the State's claimants and/or employers is processed or stored.

3.14   SECURITY REQUIREMENTS

Note to Offerors: If you follow a more stringent standard(s) than those specified in this TORFP, map the standard you follow to NIST to show how you comply with those requirements.

3.14.1 Additional security requirements may be established in a Task Order and/or a Work Order.

3.14.2 Information Technology

3.14.2.1 The TO Contractor agrees that it and TO Contractor Personnel shall (i) abide by all applicable federal, State and local laws, rules and regulations concerning Security of Information Systems and Information Technology security and (ii) comply with and adhere to the State IT Security Policy and Standards as each may be amended or revised from time to time. Updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy.

3.14.3 The State shall, at its discretion, have the right to review and assess the TO Contractor's compliance to the security requirements and standards defined in the TO Agreement.

3.14.4 TO Contractor Personnel

3.14.4.1 TO Contractor Personnel shall display his or her company ID badge in a visual location at all times while on State premises. Upon request of authorized State personnel, each such TO Contractor Personnel shall provide additional photo identification.

3.14.4.2 At all times at any facility, the TO Contractor Personnel shall cooperate with State site requirements that include but are not limited to being prepared to be escorted at all times and providing information for State badge issuance.

3.14.4.3 TO Contractor shall remove any TO Contractor Personnel from working on the TO Agreement where the State determines, at its sole discretion, that said TO Contractor Personnel has not adhered to the Security requirements specified herein.

3.14.4.4 The State reserves the right to request that the TO Contractor submit proof of employment authorization of non-United States Citizens, prior to commencement of work under the TO Agreement.

3.14.5 Background Checks

3.14.5.1 The TO Contractor shall include the provisions of this section in every applicable subcontract so that such provisions will be binding upon such relevant Subcontractor.

3.14.5.2 The State shall, at its discretion, have the right to review and assess the TO Contractor's compliance to the security requirements and standards defined in the Task Order.

3.14.5.3 The TO Contractor shall obtain from all Contractor Personnel assigned to work on the Task Order a signed statement permitting a criminal background check. Within forty-five (45) days after NTP, the TO Contractor shall secure at its own expense a national criminal history record check and provide the TO Contract Manager with completed checks on such Contractor Personnel prior to assignment. This check may be performed by a public or private entity.

3.14.5.4 At a minimum, these background checks must include all convictions and probation before judgment (PBJ) dispositions. The TO Contractor may not assign an individual whose background check reflects any criminal activity to work under this Task Order unless prior written approval is obtained from the TO Contract Manager.

3.14.5.5 TO Contractor shall be responsible for ensuring that TO Contractor Personnel background check certifications are renewed annually, and at the sole expense to the TO Contractor.

3.14.5.6 Further, TO Contractor Personnel may be subject to random security checks during entry and exit of State secured areas. The State reserves the right to require TO Contractor Personnel to be accompanied while on secured premises.

3.14.5.7 TO Contractor Personnel shall follow the State of Maryland IT Security Policy and Standards throughout the term of the TO Agreement.

3.14.5.8 The cost of complying with all security requirements specified herein are the sole responsibility and obligation of the TO Contractor and its subcontractors and no such costs shall be passed through to or reimbursed by the State or any of its agencies or units.

3.14.5.9 TO Contractor shall complete a criminal background check prior to any individual TO Contractor Personnel being assigned work on the project. TO Contractor shall provide a Criminal Background Check Affidavit (Attachment 17) within 45 days of notice to proceed.

3.14.6 Data Protection and Controls

TO Contractor shall ensure satisfaction of the following requirements:

3.14.6.1 Administrative, physical and technical safeguards shall be implemented to protect State data that are no less rigorous than accepted industry practices for information security such as those listed below (see 3.14.5.2), and all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of and disclosed shall comply with applicable data protection and privacy laws as well as the terms and conditions of this TO Agreement.

3.14.6.2 To ensure appropriate data protection safeguards are in place, at minimum, the TO Contractor shall implement and maintain the following controls at all times throughout the term of the TO Agreement (the TO Contractor may augment this list with additional controls):

1. Establish separate production, test, and training environments for systems supporting the services provided under this TO Agreement and ensure that production data is not replicated in test and/or training environment(s) unless it has been previously anonymized or otherwise modified to protect the confidentiality of Sensitive Data elements.

2. Apply hardware and software hardening procedures as recommended by Center for Internet Security (CIS) guides https://www.cisecurity.org/cis-benchmarks/ , Security Technical Implementation Guides (STIG), or similar industry best practices to reduce the surface of vulnerability, eliminating as many security risks as possible and documenting what is not feasible and/or not performed according to best practices. Any hardening practices not implemented shall be documented with a plan of action and milestones including any compensating control. These procedures may include but are not limited to removal of unnecessary software, disabling or removing unnecessary services, removal of unnecessary usernames or logins, and the deactivation of unneeded features in the system configuration files.

3. Ensure that State data is not comingled with any other data through the proper application of compartmentalization security measures.

4. Apply data encryption to protect State data, especially personal identifiable information (PII), from improper disclosure or alteration. For State data the TO Contractor manages or controls, data encryption should be applied to State data in transit over networks and, where possible, at rest; as well as to State data when archived for backup purposes. Encryption algorithms which are utilized for this purpose must comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-2.

   http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
   http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

5. Enable appropriate logging parameters on systems to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system and application manufacturers and information security standards, including State of Maryland Department of Information Security Policy.

6. Retain the aforementioned logs and review them at least daily to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation, if required. The Department shall have the right to inspect these policies and

procedures and the TO Contractor's performance to confirm the effectiveness of these measures for the services being provided under this TO Agreement.

7. Ensure system and network environments are separated by properly configured and updated firewalls.

   i. Restrict network connections between trusted and untrusted networks by physically and/or logically isolating systems from unsolicited and unauthenticated network traffic.

   ii. By default "deny all" and only allow access by exception.

8. Review at regular intervals the aforementioned network connections, documenting and confirming the business justification for the use of all service, protocols, and ports allowed, including the rationale or compensating controls implemented for those protocols considered insecure but necessary.

9. Establish policies and procedures to implement and maintain mechanisms for regular vulnerability testing of operating system, application, and network devices. Such testing is intended to identify outdated software versions; missing software patches; device or software misconfigurations; and to validate compliance with or deviations from the TO Contractor's security policy.   TO Contractor shall evaluate all identified vulnerabilities for potential adverse effect on security and integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The Department shall have the right to inspect these policies and procedures and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided under this TO Agreement.

10. Enforce strong user authentication and password control measures to minimize the opportunity for unauthorized access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with the most current State of Maryland Department of Information Technology's Information Security Policy (http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx), , including specific requirements for password length, complexity, history, and account lockout.

11. Ensure Sensitive Data under this service is not processed, transferred, or stored outside of the United States.

12. Ensure TO Contractor's Personnel shall not connect any of its own equipment to a State LAN/WAN without prior written approval by the State, which may be revoked at any time for any reason. The TO Contractor shall complete any necessary paperwork as directed and coordinated with the Contract Monitor to obtain approval by the State to connect TO Contractor-owned equipment to a State LAN/WAN.

13. Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the services provided under this TO Agreement; that the anti-virus and anti-malware software is automatically updated; and that the software is configured to actively scan and detect threats to the system for remediation. The Contractor shall perform routine vulnerability scans and take corrective actions for any findings.

14. Where website hosting or Internet access is the service provided or part of the service provided, the TO Contractor and/or Subcontractor shall conduct regular external vulnerability testing. External vulnerability testing is an assessment designed to examine the TO Contractor and/or Subcontractor's security profile from the Internet without

benefit of access to internal systems and networks behind the external security perimeter. The TO Contractor and/or Subcontractor shall evaluate all identified vulnerabilities on Internet-facing devices for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The Department shall have the right to inspect these policies and procedures and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided under this TO Agreement.

3.14.6.3 Access to Security Logs and Reports

The TO Contractor shall provide reports to the State in a mutually agreeable format.

Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all State files related to this TO Agreement.

3.15 RIGHT TO AUDIT

A. The State reserves the right, at its sole discretion and at any time, to perform an audit of the TO Contractor's and/or Subcontractors' performance under the TO Agreement resulting from this TORFP. An audit is defined as a planned and documented independent activity performed by qualified personnel, including but not limited to State and federal auditors, to determine by investigation, examination, or evaluation of objective evidence from data, statements, records, operations and performance practices (financial or otherwise) the TO Contractor's compliance with the agreement, including but not limited to the adequacy and compliance with established procedures and internal controls over the services being performed for the State.

B. Upon three (3) business days' notice, the TO Contractor and/or Subcontractors shall provide the State reasonable access to their records during normal business hours to verify conformance to the terms of the TO Agreement. The Department shall be permitted to conduct these audits with any or all of its own internal resources or by securing the services of a third party accounting/audit firm, solely at the Department's election. The Department shall have the right to copy, at its own expense, any record related to the services performed pursuant to this agreement.

C. TO Contractor and/or Subcontractors shall cooperate with Department or Department's designated auditor and shall provide the necessary assistance for Department or Department's designated auditor to conduct the audit.

D. The right to audit shall include subcontractors in which goods or services are subcontracted by TO Contractor and/or Subcontractors and that provide essential support to the services provided to Department. TO Contractor and/or Subcontractors shall insure Department has the right to audit with subcontractor(s).

3.16 INCIDENT RESPONSE

The TO Contractor shall adhere to DHMH's Incident Response Protocol and incorporate these actions into the TO Contractor's processes and procedures for addressing information security (refer to Attachment 18 Incident Response Protocol).

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 4 - TO PROPOSAL FORMAT AND SUBMISSION REQUIREMENTS

4.1   REQUIRED RESPONSE

Each Master Contractor receiving this CATS+ TORFP shall respond no later than the submission due date and time designated in the Key Information Summary Sheet. Each Master Contractor is required to submit one of two possible responses: 1) a TO Proposal; or 2) a completed Master Contractor Feedback Form. The feedback form helps the State understand for future contract development why Master Contractors did not submit proposals. The form is accessible via the CATS+ Master Contractor login screen and clicking on TORFP Feedback Response Form from the menu.

A TO Proposal shall conform to the requirements of this CATS+ TORFP.

4.2   SUBMISSION

4.2.1   E-MAIL SUBMISSION

DHMH strongly prefers TO Proposal submissions be made via e-mail.

DHMH can only accept e-mails that are less than or equal to 25 MB. If a submission exceeds this size, split the submission into two or more parts and include the appropriate part number in the subject (e.g., part 1 of 2) after the subject line information. Zip files are not acceptable and will be rejected by DHMH's email system.

DHMH will contact Offerors for the password to open each e-mail's contents. Each file in the TO Technical Proposal shall be encrypted with the same password. A password separate and distinct from the TO Technical Proposal password shall be used for files in the TO Financial Proposal. The TO Procurement Officer will only contact those Offerors with TO Proposals that are reasonably susceptible for award. Offerors that are unable to provide a password that opens the TO Proposal documents will be deemed not susceptible for award. Subsequent submissions of TO Proposal content will not be allowed.

For TO Proposals submitted via e-mail, the TO Technical Proposal shall be submitted in one or more encrypted e-mails separate from the TO Financial Proposal. This e-mail shall include:

A. Subject line "CATS+ TORFP # **DHMH OPASS 18-17607 / M00B8400002** Technical" plus the Master Contractor Name
B. One attachment labeled "TORFP # **DHMH OPASS 18-17607 / M00B8400002** Technical - Attachments" containing all TO Technical Proposal Attachments (see Section 4.3 below), signed and in PDF format.
C. One attachment labeled "TORFP # **DHMH OPASS 18-17607 / M00B8400002** Technical – Proposal" in Microsoft Word format (2007 or later).

The TO Financial Proposal shall be contained in one e-mail containing as attachments all submission documents detailed in Section 4.4.2, with password protection.

A. Subject line "CATS+ TORFP # **DHMH OPASS 18-17607 / M00B8400002** Financial" plus the Master Contractor Name
B. One attachment labeled "TORFP # **DHMH OPASS 18-17607 / M00B8400002** Financial" containing the TO Financial Proposal contents, signed and in PDF format.

4.2.2   PAPER SUBMISSION

DHMH strongly desires TO Proposal submissions in e-mail format. An Offeror wishing to deliver a hard copy (paper) TO Proposal shall contact the TO Procurement Officer for instructions.

4.3   SUMMARY OF ATTACHMENTS

No attachment forms shall be altered. Signatures shall be clearly visible.

The following signed attachments shall be included with the TO Technical Proposal in PDF format (for e-mail delivery).

A. Attachment 2 - MBE forms 1A
B. Attachment 4 – Conflict of Interest Affidavit and Disclosure
C. Attachment 5A and 5B- Attachment 5A Minimum Qualifications Summary and Attachment 5B Personnel Resume Form
D. Attachment 12 – Living Wage Affidavit of Agreement
E. Attachment 15 - Certification Regarding Investments in Iran

The following attachments shall be included with the TO Financial Proposal:

A. Attachment 1 Price Sheet – Signed PDF

4.4   PROPOSAL FORMAT

A TO Proposal shall contain the following Sections in order:

4.4.1   TO TECHNICAL PROPOSAL

Important: A TO Technical Proposal shall include NO pricing information.

A) Proposed Services

1) Executive Summary: A one-page summary describing the Offeror's understanding of the TORFP scope of work (Section 3) and proposed solution.

2) Proposed Solution: A more detailed description of the Offeror's understanding of the TORFP scope of work, proposed methodology and solution. The proposed solution shall be organized to exactly match the requirements outlined in Section 3. The proposed solution shall include a DRAFT of the Beginning of Contract Transition Plan, as defined in Section 3.8.4.3.

3) Draft Work Breakdown Structure (WBS): A matrix or table that shows a breakdown of the tasks required to complete the requirements and deliverables in Section 3 - Scope of Work. The WBS should reflect the chronology of tasks without assigning specific time frames or start / completion dates. The WBS may include tasks to be performed by the State or third parties, for example, independent quality assurance tasks. If the WBS appears as a deliverable in Section 3 – Scope of Work, the deliverable version will be a final version. Any subsequent versions shall be approved through a formal configuration or change management process.

4) Draft Project or Work Schedule: A Gantt or similar chart containing tasks and estimated time frames for completing the requirements and deliverables in Section 3 - Scope of Work. The final schedule should come later as a deliverable under the TO after the TO Contractor has had an opportunity to develop realistic estimates. The Project or Work Schedule may include tasks to be performed by the State or third parties.

5) Draft Risk Assessment: Identification and prioritization of risks inherent in meeting the requirements in Section 3 - Scope of Work. Includes a description of strategies to mitigate risks. If the Risk Assessment appears as a deliverable in Section 3 – Scope of Work, that

version will be a final version. Any subsequent versions should be approved through a formal configuration or change management process.

6) Assumptions: A description of any assumptions formed by the Offeror in developing the TO Technical Proposal.

7) Tools the Master Contractor owns and proposes for use to meet any requirements in Section 3.

8) Sample COOP or DR Plan for proposed Primary and Secondary Data Centers.

9) SOC2 reports within the last three (3) years from Proposal due date for the proposed Primary and Secondary Data Centers. If a SOC2 is not available, provide an alternative third-party evaluation that demonstrates adherence to published practices and procedures for the proposed Primary and Secondary Data Centers.

10) Proposed COTS software to support the claims operations, including: a.) summary of TO Contractor's past experience with the COTS software, b.) approach for integration into the LTSS System, c.) sample reports for balancing and reconciling claims, and d.) proposed plan for ensuring Operations Lead can support DHMH using the COTS software.

11) Summary of proposed resources and solution for Optional Services – Database Support Services.

B) Compliance with Offeror's Company Minimum Qualifications

Offerors will complete the following table to demonstrate compliance with the Offeror's Company Minimum Requirements in Section 2.1.1.

C) Proposed Personnel and TORFP Staffing
Offeror shall propose exactly four (4) Key Personnel in response to this TORFP. Offeror shall:

1) Complete and provide for each proposed resource Attachment 5A Minimum Qualifications Summary and Attachment 5B Personnel Resume Form.

2) Provide evidence proposed personnel possess the required certifications in accordance with Section 2.1.2 Offeror's Personnel Minimum Qualifications.

3) Provide three (3) references per proposed Key Personnel containing the information listed in Attachment 5B.

4) Provide a Staffing Management Plan that demonstrates how the Offeror will provide resources in addition to the personnel requested in this TORFP, and how the TO Contractor Personnel shall be managed. Include:

    a) Planned team composition by role (**Important! Identify specific names and provide history <u>only</u> for the proposed resources required for evaluation of this TORFP**).
    b) Process and proposed lead time for locating and bringing on board resources that meet TO needs
    c) Supporting descriptions for all labor categories proposed in response to this TORFP
    d) Description of approach for quickly substituting qualified personnel after start of TO.

5) Provide the names and titles of the Offeror's management staff who will supervise the personnel and quality of services rendered under this TO Agreement.

D) MBE, SBE Participation and VSBE Participation

Submit completed MBE documents 2-1A.

E) Subcontractors

Identify all proposed subcontractors, including MBEs, and their roles in the performance of Section 3 - Scope of Work.

F) Overall Offeror team organizational chart

Provide an overall team organizational chart with all team resources available to fulfill the TO scope of work.

G) Master Contractor and Subcontractor Experience and Capabilities

1) Provide up to three examples of engagements or contracts the Master Contractor or subcontractor, if applicable, has completed that were similar to Section 3 - Scope of Work. Include contact information for each client organization complete with the following:

a) Name of organization.

b) Point of contact name, title, e-mail and telephone number (point of contact shall be accessible and knowledgeable regarding experience)

c) Services provided as they relate to Section 3 - Scope of Work.

d) Start and end dates for each example engagement or contract.

e) Current Master Contractor team personnel who participated on the engagement.

f) If the Master Contractor is no longer providing the services, explain why not.

2) State of Maryland Experience: If applicable, the Master Contractor shall submit a list of all contracts it currently holds or has held within the past five years with any entity of the State of Maryland.

For each identified contract, the Master Contractor shall provide the following (if not already provided in sub paragraph 1 above):

a) Contract or task order name

b) Name of organization.

c) Point of contact name, title, e-mail, and telephone number (point of contact shall be accessible and knowledgeable regarding experience)

d) Start and end dates for each engagement or contract. If the Master Contractor is no longer providing the services, explain why not.

e) Dollar value of the contract.

f) Indicate if the contract was terminated before the original expiration date.

g) Indicate if any renewal options were not exercised.

Note - State of Maryland experience can be included as part of Section 2 above as engagement or contract experience. State of Maryland experience is neither required nor given more weight in TO Technical Proposal evaluations.

H) State Assistance

Provide an estimate of expectation concerning participation by State personnel.

I) Confidentiality

A Master Contractor should give specific attention to the identification of those portions of its TO Technical Proposal that it considers confidential, proprietary commercial information or trade secrets, and provide justification why such materials, upon request, should not be disclosed by the State under the Public Information Act, Title 4, of the General Provisions Article of the Annotated Code of Maryland. Master Contractors are advised that, upon request for this information from a third party, the TO Procurement Officer will be required to make an independent determination regarding whether the information may be disclosed.

Offeror shall furnish a list that identifies each Section of the TO Technical Proposal where, in the Offeror's opinion, the Offeror's response should not be disclosed by the State under the Public Information Act.

J) Proposed Facility

Identify Master Contractor's facilities, including address, from which any work will be performed.

K) Additional Submissions

a. As an attachment to the TO Technical Proposal, provide a copy of any software licensing agreement for any software proposed to be licensed to the State under this Task Order (e.g., EULA, Enterprise License Agreements). **A link to manufacturer's site is NOT acceptable.**

4.4.2   TO FINANCIAL PROPOSAL

A) A description of any assumptions on which the Master Contractor's TO Financial Proposal is based (Assumptions shall not constitute conditions, contingencies, or exceptions to the Price Sheet)

B) Attachment 1– Price Sheet

C) Prices shall be valid for 120 days

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 5 - TASK ORDER AWARD PROCESS

5.1   OVERVIEW

The TO Contractor will be selected from among all eligible Master Contractors within the appropriate Functional Area responding to the CATS+ TORFP. In making the TO Agreement award determination, the TO Requesting Agency will consider all information submitted in accordance with Section 4.

5.2   TO PROPOSAL EVALUATION CRITERIA

The following are technical criteria for evaluating a TO Proposal in descending order of importance. Failure to meet the minimum qualifications shall render a TO Proposal not reasonably susceptible for award. If not specified, any sub-criteria have equal weight:

A) The overall experience, capability and references for the Master Contractor as described in the Master Contractor's TO Technical Proposal.

B) The Master Contractor's overall understanding of the TORFP Scope of Work – Section 3. Level of understanding will be determined by the quality and accuracy of the TO Technical Proposal in adherence with Section 4.4.

C) The capability of the proposed resources to perform the required tasks and produce the required deliverables in the TORFP Scope of Work – Section 3. Capability will be determined from each proposed individual's resume, reference checks, and oral presentation (See Section 1.5 Oral Presentations/Interviews).

D) Demonstration of how the Master Contractor plans to staff the task order at the levels set forth in Sections 2.1, 2.2 and 3.1 and also for potential future resource requests.

E) Capability and risk management approach for how the Master Contractor plans to support LTSS System changes to support business needs, compliance and/or scalability, including the transition from the BASE-level to EXPANDED volumes.

F) Completeness and capability of how the Master Contractor's proposed Primary and Secondary Data Centers meet the TORFP requirements, as described in Section 3.6.4, 3.6.5 and 4.4.1.

  1) Completeness and risk management approach of the proposed sample COOP or DR Plan for the Primary and Secondary Data Centers, per Section 4.4.1 (8).

  2) Adherence to published Data Center practices and procedures as evidenced via third-party evaluation, per Section 4.4.1(9).

5.3   SELECTION PROCEDURES

A) TO Proposals will be assessed throughout the evaluation process for compliance with the minimum qualifications listed in Section 2 of this TORFP, and quality of responses to Section 4.4.1 TO Technical Proposal.

B) For all TO Proposals deemed technically qualified, Oral Presentations will be performed

C) For TO Technical Proposals deemed technically qualified, the associated TO Financial Proposal will be opened. All others will be deemed not reasonably susceptible for award and the TO Procurement Officer will notify the Master Contractor it has not been selected to perform the work.

D) Qualified TO Financial Proposal responses will be reviewed and ranked from lowest to highest price proposed.

E) The most advantageous TO Proposal considering both the technical and financial submissions shall be selected for TO award. In making this selection, technical merit has greater weight.

F) All Master Contractors submitting a TO Proposal shall receive written notice from the TO Procurement Officer identifying the awardee.

5.4   COMMENCEMENT OF WORK UNDER A TO AGREEMENT

Commencement of work in response to a TO Agreement shall be initiated only upon:

a. Issuance of a fully executed TO Agreement;

b. Non-Disclosure Agreement (TO Contractor);

c. Purchase Order;

d. Notice to Proceed authorized by the TO Procurement Officer. See Attachment 7 - Notice to Proceed (sample);

e. Proof of Cyber Security insurance (see Section 3.13.1); and,

f. Business Associate Agreement (see Section 1.22) within five (5) Business Days.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

LIST OF ATTACHMENTS

Attachment Label	Attachment Name	Applicable to this TORFP?	Submit with TO Proposal?* (Submit, Do Not Submit, N/A)
Attachment 1	Price Sheet	Applicable	Submit with TO Financial Proposal with password protection
Attachment 2	Minority Business Enterprise Participation (Attachments 1A – 5)	Applicable	Submit with TO Technical Proposal
Attachment 3	Task Order Agreement (TO Agreement)	Applicable	Do Not Submit with TO Proposal
Attachment 4	Conflict of Interest Affidavit and Disclosure	Applicable	Submit with TO Technical Proposal
Attachment 5	Labor Classification Personnel Resume Summary	Applicable	Submit with TO Technical Proposal
Attachment 6	Pre-Proposal Conference Directions	Applicable	Do Not Submit with TO Proposal
Attachment 7	Notice to Proceed (Sample)	Applicable	Do Not Submit with TO Proposal
Attachment 8	Agency Deliverable Product Acceptance Form (DPAF)	Applicable	Do Not Submit with TO Proposal
Attachment 9	Non-Disclosure Agreement (Offeror)	Not Applicable	Do Not Submit with TO Proposal
Attachment 10	Non-Disclosure Agreement (TO Contractor)	Applicable	Do Not Submit with TO Proposal
Attachment 11	TO Contractor Self-Reporting Checklist	Applicable	Do Not Submit with TO Proposal
Attachment 12	Living Wage Affidavit of Agreement	Applicable	Submit with TO Technical Proposal
Attachment 13	Mercury Affidavit	*Not Applicable*	*N/A*
Attachment 14	Veteran Owned Small Business Enterprise Utilization Affidavit	*Not Applicable*	*N/A*
Attachment 15	Certification Regarding Investments in Iran	Applicable	Submit with TO Technical Proposal
Attachment 16	Sample Work Order	Applicable	Do Not Submit with TO Proposal
Attachment 17	Criminal Background Check Affidavit	Applicable	Do Not Submit with TO Proposal
Attachment 18	Incident Response Protocol	Applicable	*N/A*
Attachment 19	Business Associate Agreement	Applicable	Do Not Submit with TO Proposal
Attachment 20	LTSS System Technical Infrastructure Design	Applicable	Do Not Submit with TO Proposal
Attachment 21	Work-from-Home Help Desk Security Policy	Applicable	Do Not Submit with TO Proposal
Attachment 22	TEFT IVR Proposed Call Flow (see separate document)	Applicable	Do Not Submit with TO Proposal

*if not specified in submission instructions, any attachment submitted with response shall be in PDF format and signed

ATTACHMENT 1 PRICE SHEET

PRICE SHEET (FIXED PRICE) FOR CATS+ TORFP # DHMH OPASS 18-17607 M00B8400002

The TO Financial Proposal Form shall contain all price information in the format specified on these pages. Complete the TO Financial Proposal Form only as provided in the TO Financial Proposal Instructions. Do not amend, alter or leave blank any items on the TO Financial Proposal Form. Offerors must submit pricing for the option year. Failure to adhere to any of these instructions may result in the Proposal being determined not reasonably susceptible of being selected for award.

The Fixed Price shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TO Agreement. A year for this Task Order shall be calculated as one calendar year from date of TO Agreement execution.

Fixed Monthly Unit Price services shall start AFTER the Start-up Period has been successfully completed and accepted by the Department, with the remaining months in the first calendar year to be charged at the Base Year 1 rate.

Items in Part III are increases to the Fixed Monthly Unit Price for items in Part II. The items in Part III are estimated additional increments and not guaranteed. On a month-to-month basis, the volumes are evaluated to determine if the increases in Part III are required.

Part I. Firm-Fixed Price

The Firm-Fixed Price is based on Deliverables in 3.8.4.1 – 3.8.4.14.

Description	Reference Sections	Fixed Price	
Start-up Period (Excluding TEFT IVR)	3.6.3, 3.6.7.6(10), 3.8.4.1-14	$	Completed within one hundred fifty (150) calendar days from NTP Date.
(OPTION) TEFT IVR	3.6.3.1, 3.6.5.5(b)	$	Within sixty (60) calendar days from NTP, DHMH shall confirm go / no go for the TEFT IVR.

(I. Deliverable Based Subtotal) = $ _____

Part II A. Fixed Monthly Unit Price

Offeror shall allocate its Fixed Monthly Unit Price for the Operations – Help Desk (3.3, 3.6(C) & 3.6.6.21) component for the TO Technical Proposal. One (1) Fixed Monthly Unit for this item is up to 1,500 Help Desk Inquiries in one (1) calendar month.

The Fixed Monthly Unit Price shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP.

	A	B	C

	Up To Monthly Inquiry Volume	Fixed Monthly Unit Price	Extended Price (B x 12)
Base Year 1	1,500	$	(a) $
Base Year 2	1,500	$	(b) $
Base Year 3	1,500	$	(c) $
Base Year 4	1,500	$	(d) $
Option Year	1,500	$	(e) $
SUBTOTAL	**(a+b+c+d+e)**		**(f) $**

(II A. Fixed Price Subtotal) (f) = $ _____

Part II B. Fixed Monthly Unit Price for BASE-Level Operations Claims

Offeror shall allocate its Fixed Monthly Unit Price for the Operations – Claims (3.3, 3.6(C), & 3.6.6.1) component for the TO Technical Proposal. One (1) Fixed Monthly Unit for this item is up to 1.5 million claims in one (1) calendar month.

The Fixed Monthly Unit Price shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP.

	A	B	C
	Up To Monthly Claims Volume	Fixed Monthly Unit Price	Extended Price (B x 12)
Base Year 1	1.5 Million	$	(a) $
Base Year 2	1.5 Million	$	(b) $
Base Year 3	1.5 Million	$	(c) $
Base Year 4	1.5 Million	$	(d) $
Option Year	1.5 Million	$	(e) $
SUBTOTAL	**(a+b+c+d+e)**		**(f) $**

(II B. Fixed Price Subtotal) (f) = $ _____

Part II C. Fixed Monthly Unit Price

Offeror shall allocate its Fixed Monthly Unit Price for the Operations – Other Services (3.3, 3.6(C), 3.6.6.2, 3.6.6.3, 3.6.6.5 & 3.6.8) component for the TO Technical Proposal.

The Fixed Monthly Unit Price shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP.

	A	B
	Fixed Monthly Unit Price	Extended Price (A x 12)
Base Year 1	$	(a) $
Base Year 2	$	(b) $
Base Year 3	$	(c) $
Base Year 4	$	(d) $
Option Year	$	(e) $
SUBTOTAL	**(a+b+c+d+e)**	**(f) $**

(II C. Fixed Price Subtotal) (f) = $ _____

Part II D. Fixed Monthly Unit Price

Offeror shall allocate its Fixed Monthly Unit Price for the <u>Hosting – IVR (3.3, 3.6(B), 3.6.3.1, 3.6.4, 3.6.5.5)</u> component for the TO Technical Proposal. One (1) Fixed Monthly Unit for this item is up to 600,000 IVR calls in one (1) calendar month.

The Fixed Monthly Unit Price shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP.

	A Up To Monthly IVR Call Volume	B Fixed Monthly Unit Price	C Extended Price (B x 12)
Base Year 1	600,000	$	(a) $
Base Year 2	600,000	$	(b) $
Base Year 3	600,000	$	(c) $
Base Year 4	600,000	$	(d) $
Option Year	600,000	$	(e) $
SUBTOTAL	**(a+b+c+d+e)**		**(f) $**

(II D. Fixed Price Subtotal) (f) = $ _____

Part II E. Fixed Monthly Unit Price for BASE-Level Managed Hosting Services

Offeror shall allocate its Fixed Monthly Unit Price for the <u>Hosting – Managed Services (3.3, 3.6(B), 3.6.4, & 3.6.5)</u> component for the TO Technical Proposal.

The Fixed Monthly Unit Price shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP.

	A Fixed Monthly Unit Price	B Extended Price (A x 12)
Base Year 1	$	(a) $
Base Year 2	$	(b) $
Base Year 3	$	(c) $
Base Year 4	$	(d) $
Option Year	$	(e) $
SUBTOTAL	**(a+b+c+d+e)**	**(f) $**

(II E. Fixed Price Subtotal) (f) = $ _____

Part III A. Increase to the Fixed Monthly Unit Price for Additional Help Desk Inquiries

Offeror shall provide pricing for additional Help Desk inquiries (<u>3.3, 3.6(C) & 3.6.6.21</u>). The Increase to the Fixed Monthly Unit Price for Part III A covers the monthly fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP, for each additional increment of 500 inquiries (from 1 to 500) above the 1,500 inquiries listed in Part II A, above.

For example, if the Contractor received a total of 2,001 Help Desk inquiries for a month, the Contractor would receive the Fixed Monthly Unit Price in Part II A for the first 1,500 calls. Then, the Contractor shall bill for the price of two (2) increments at the Increase to the Fixed Monthly Unit Price listed in Part III A for calls 1,501-2,000 and 2,001 – 2,500.

1 Increment = Additional 500 Help Desk Inquiries per Month	A Fixed Price per Increment	B # increments budget per year	C Extended Price (A x B)
Base Year 1	$	24	(a) $
Base Year 2	$	24	(b) $
Base Year 3	$	24	(c) $
Base Year 4	$	24	(d) $
Option Year	$	24	(e) $
	SUBTOTAL	(a+b+c+d+e)	(f) $

(III A. Fixed Price Subtotal) (f) = $ _____

Part III B. Increase to the Fixed Monthly Unit Price for Additional Claims

Offeror shall provide pricing for additional Claims (3.3, 3.6(C), & 3.6.6.1). The Increase to the Fixed Monthly Unit Price for Part III B covers the monthly fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP, for each additional increment of 100,000 claims (from 1 to 100,000) above the 1.5 Million claims listed in Part II B, above.

For example, if the Contractor received a total of 1,600,001 claims for a month, the Contractor would receive the Fixed Monthly Unit Price in Part II B for the first 1,500,000 claims. Then, the Contractor shall bill for two (2) increments at the Increase to Fixed Monthly Unit Price listed in Part III B for claims 1,500,001-1,600,000 and 1,600,001 – 1,700,000.

However, when the EXPANDED volumes are in effect, per Part V A. Fixed Monthly Unit Price for EXPANDED Managed Hosting Services, the additional claims volumes would begin AFTER the volume goes above 3 Million claims.

1 Increment = Additional 100,000 Claims per Month	A Fixed Price per Increment	B # increments budget per year	C Extended Price (A x B)
Base Year 1	$	48	(a) $
Base Year 2	$	48	(b) $
Base Year 3	$	48	(c) $
Base Year 4	$	48	(d) $
Option Year	$	48	(e) $
	SUBTOTAL	(a+b+c+d+e)	(f) $

(III B. Fixed Price Subtotal) (f) = $ _____

Part III C. Increase to the Fixed Monthly Unit Price for Additional IVR Calls

Offeror shall provide pricing for additional IVR Calls (3.3, 3.6(B), 3.6.3.1, 3.6.4, 3.6.5.5). The Increase to the Fixed Monthly Unit Price for Part III C covers the monthly fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP, for each

additional increment of 60,000 IVR calls (from 1 to 60,000) above the 600,000 IVR Calls listed in Part II D, above.

For example, if the Contractor received a total of 660,001 IVR Calls for a month, the Contractor would receive the Fixed Monthly Unit Price in Part II D for the first 600,000 IVR Calls. Then, the Contractor shall bill for the price of two (2) increments at the Increase to the Fixed Monthly Unit Price listed in Part III C for IVR Calls 600,001-660,000 and 660,001 – 720,000.

1 Increment = Additional 60,000 IVR Calls per Month	A	B	C
	Fixed Price per Increment	# increments budget per year	Extended Price (A x B)
Base Year 1	$	36	(a) $
Base Year 2	$	36	(b) $
Base Year 3	$	36	(c) $
Base Year 4	$	36	(d) $
Option Year	$	36	(e) $
	SUBTOTAL	**(a+b+c+d+e)**	**(f) $**

(III C. Fixed Price Subtotal) (f) = $ _____

THE REMAINDER OF THIS PAGE INTENTIALLY LEFT BLANK.

Part IV. Fixed Price Deliverables for Additional Operations Support Services (See Sections 3.1 (d) & 3.6(D))

Offerors shall provide a proposed hourly rate for the Junior and Senior Network Technician Labor Categories (see CATS+ Section 2.10 Labor Categories and Qualifications). For evaluation purposes, DHMH requires an Annual Hours Budget of 2,000 hours per labor category per year.

	Labor Category	A Annual Hours Budget	B Hourly Rate	C Extended Price (A x B = C)
Base Year 1	Network Technician (Junior)	2000	$	$
	Network Technician (Senior)	2000	$	$
BASE YEAR 1 SUBTOTAL				**(a) $**
Base Year 2	Network Technician (Junior)	2000	$	$
	Network Technician (Senior)	2000	$	$
BASE YEAR 2 SUBTOTAL				**(b) $**
Base Year 3	Network Technician (Junior)	2000	$	$
	Network Technician (Senior)	2000	$	$
BASE YEAR 3 SUBTOTAL				**(c) $**
Base Year 4	Network Technician (Junior)	2000	$	$
	Network Technician (Senior)	2000	$	$
BASE YEAR 4 SUBTOTAL				**(d) $**
Option Year	Network Technician (Junior)	2000	$	$
	Network Technician (Senior)	2000	$	$
OPTION YEAR SUBTOTAL				**(e) $**
SUBTOTAL		20,000	**(a+b+c+ d+e)**	**(f) $**

There is no guarantee of any minimum or maximum number of hours.

(IV. Fixed Price Deliverables for Additional Support Services Subtotal) (f) = $ _____

Part V A. Fixed Monthly Unit Price for EXPANDED Managed Hosting Services

Offeror shall allocate its Fixed Monthly Unit Price for the <u>EXPANDED Managed Hosting Services (3.3, 3.6(B), 3.6.4, & 3.6.5)</u> component for the TO Technical Proposal to assist the Department in determining the reasonableness of the price offered and whether the requirements of the TORFP have been correctly understood. The Fixed Monthly Unit Price should be the <u>INCREMENTAL INCREASE</u> to <u>Part II E. Fixed Monthly Unit Price for BASE-Level Managed Hosting Services</u>.

The Fixed Monthly Unit Price shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP.

	A Fixed Monthly Unit Price	B Extended Price (A x 12)
Base Year 1	$	(a) $
Base Year 2	$	(b) $
Base Year 3	$	(c) $
Base Year 4	$	(d) $
Option Year	$	(e) $
SUBTOTAL	**(a+b+c+d+e)**	**(f) $**

There is no guarantee of any minimum or maximum Expanded Managed Hosting Services.

    (V. Fixed Price Subtotal) (f) =   **$ _____**

Part V B. Fixed Monthly Unit Price for EXPANDED Operations Claims

Offeror shall allocate its Fixed Monthly Unit Price for the <u>EXPANDED Operations – Claims (3.3, 3.6(C), & 3.6.6.1)</u> component for the TO Technical Proposal to assist the Department in determining the reasonableness of the price offered and whether the requirements of the TORFP have been correctly understood. The Fixed Monthly Unit Price should be the <u>INCREMENTAL INCREASE</u> to <u>Part II B. Fixed Monthly Unit Price for BASE-Level Operations Claims</u>. One (1) Fixed Monthly Unit for this item is the additional 1.5 million claims from the BASE-Level, resulting in up to 3 million claims in one (1) calendar month.

The Fixed Monthly Unit Price shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP.

	A Up To Monthly Claims Volume	B Fixed Monthly Unit Price	C Extended Price (B x 12)
Base Year 1	3,000,000	$	(a) $
Base Year 2	3,000,000	$	(b) $
Base Year 3	3,000,000	$	(c) $
Base Year 4	3,000,000	$	(d) $
Option Year	3,000,000	$	(e) $
SUBTOTAL	**(a+b+c+d+e)**	■■■■■■	**(f) $**

    (II B. Fixed Price Subtotal) (f) =   **$ _____**

TO Financial Proposal Summary:

Offeror must enter its subtotals from the indicated Sections of the price form in the indicated rows: Then, sum all amounts and enter the amount in TOTAL PROPOSAL PRICE.

A	B
Part I. Deliverable Based Subtotal Start-up Period	$
Part II A. Fixed Monthly Unit Price Operations – Help Desk Subtotal	$
Part II B. Fixed Monthly Unit Price for BASE-Level Claims Operations Subtotal	$
Part II C. Fixed Monthly Unit Price Operations – Other Services Subtotal	$
Part II D. Fixed Monthly Unit Price Hosting – IVR Subtotal	$
Part II E. Fixed Monthly Unit Price for BASE-Level Managed Hosting Services Subtotal	$
Part III A. Increase to Fixed Monthly Unit Price for Additional Help Desk Inquiries Subtotal	$
Part III B. Increase to Fixed Monthly Unit Price for Additional Claims Subtotal	$
Part III C Increase to Fixed Monthly Unit Price for Additional IVR Calls Subtotal	$
Part IV. Fixed Price Deliverables for Additional Operations Support Services Subtotal	$
Part V A. Fixed Monthly Unit Price for EXPANDED Managed Hosting Services Subtotal	$
Part V B. Fixed Monthly Unit Price for EXPANDED Claims Operations Subtotal	$
TOTAL PROPOSAL PRICE (Sum of Column B)	**$**

The Total Proposal Price shall be used in the ranking of TO Financial Proposals.

Authorized Individual Name

Title

Signature

Company Name

Company Tax ID #

Date

PRICE SHEET FOR OPTIONAL SERVICES (FIXED PRICE)

Optional Services based on the following:

Offeror shall allocate its Fixed Monthly Unit Price for the <u>Operations – Database Support Services (3.3, 3.6(E), 3.6.6.24-33 and 3.8.4.23</u> component for the TO Technical Proposal to assist the Department in determining the reasonableness of the price offered and whether the requirements of the TORFP have been correctly understood.

The Fixed Monthly Unit Price shall be fully loaded, all-inclusive, i.e., include all direct and indirect costs and profits for the Master Contractor to perform under the TORFP.

	A Fixed Monthly Unit Price	**B** Extended Price (A x 12)
Base Year 1	$	(a) $
Base Year 2	$	(b) $
Base Year 3	$	(c) $
Base Year 4	$	(d) $
Option Year	$	(e) $
TOTAL	(a+b+c+d+e)	(f) $

(Fixed Price TOTAL)   **(f) =**   **$ _____**

There is no guarantee that the Department will accept the TO Contractor's proposal for the Optional Services.

_____
Authorized Individual Name

_____
Title

_____
Signature

_____
Company Name

_____
Company Tax ID #

_____
Date

ATTACHMENT 2 MINORITY BUSINESS ENTERPRISE FORMS

The Minority Business Enterprise (MBE) subcontractor participation goal for this solicitation is 25%.

TO CONTRACTOR MINORITY BUSINESS ENTERPRISE REPORTING REQUIREMENTS

CATS+ TORFP # **DHMH OPASS 18-17607 / M00B8400002**

If after reading these instructions you have additional questions or need further clarification, please contact the TO Contract Monitor immediately.

1) As the TO Contractor, you have entered into a TO Agreement with the State of Maryland. As such, your company/firm is responsible for successful completion of all deliverables under the contract, including your commitment to making a good faith effort to meet the MBE participation goal(s) established for TORFP. Part of that effort, as outlined in the TORFP, includes submission of monthly reports to the State regarding the previous month's MBE payment activity. Reporting forms 2-4A (Prime Contractor Paid/Unpaid MBE Invoice Report), 2-4B (MBE Prime Contractor Report) and 2-5 (Subcontractor Paid/Unpaid MBE Invoice Report) are attached for your use and convenience.

2) The TO Contractor must complete a separate Form 2-4A for each MBE subcontractor for each month of the contract and submit one copy to each of the locations indicated at the bottom of the form. The report is due no later than the 15th of the month following the month that is being reported. For example, the report for January's activity is due no later than the 15th of February. With the approval of the TO Contract Monitor, the report may be submitted electronically. Note: Reports are required to be submitted each month, regardless whether there was any MBE payment activity for the reporting month.

3) The TO Contractor is responsible for ensuring that each subcontractor receives a copy of Form 2-5 (e-copy of and/or hard copy). The TO Contractor should make sure that the subcontractor receives all the information necessary to complete the form properly, including all of the information located in the upper right corner of the form. It may be wise to customize Form 2-5 (upper right corner of the form) for the subcontractor. This will help to minimize any confusion for those who receive and review the reports.

4) It is the responsibility of the TO Contractor to make sure that all subcontractors submit reports no later than the 15th of each month**, including reports showing zero MBE payment activity**. Actual payment data is verified and entered into the State's financial management tracking system from the **subcontractor's 2-5 report only**. Therefore, if the subcontractor(s) do not submit 2-5 payment reports, the TO Contractor cannot and will not be given credit for subcontractor payments, regardless of the TO Contactor's proper submission of Form 2-4A. The TO Contract Monitor will contact the TO Contractor if reports are not received each month from either the prime contractor or any of the identified subcontractors.

5) The TO Contractor must promptly notify the TO Contract Monitor if, during the course of the contract, a new MBE subcontractor is utilized. Failure to comply with the MBE contract provisions and reporting requirements may result in sanctions, as provided by COMAR 21.11.03.13.

ATTACHMENT 2 -1A MBE UTILIZATION AND FAIR SOLICITATION AFFIDAVIT & MBE PARTICIPATION SCHEDULE

INSTRUCTIONS

PLEASE READ BEFORE COMPLETING THIS FORM

This form includes Instructions and the MBE Utilization and Fair Solicitation Affidavit & MBE Participation Schedule which must be submitted with the bid/proposal. If the bidder/offeror fails to accurately complete and submit this Affidavit and Schedule with the bid or proposal as required, the Procurement Officer shall deem the bid non-responsive or shall determine that the proposal is not reasonably susceptible of being selected for award.

1.   Contractor shall structure its procedures for the performance of the work required in this Contract to attempt to achieve the minority business enterprise (MBE) subcontractor participation goal stated in the Invitation for Bids or Request for Proposals. Contractor agrees to exercise good faith efforts to carry out the requirements set forth in these Instructions, as authorized by the Code of Maryland Regulations (COMAR) 21.11.03.

2.   MBE Goals and Subgoals: Please review the solicitation for information regarding the Contract's MBE overall participation goals and subgoals. After satisfying the requirements for any established subgoals, the Contractor is encouraged to use a diverse group of subcontractors and suppliers from any/all of the various MBE classifications to meet the remainder of the overall MBE participation goal.

3.   MBE means a minority business enterprise that is certified by the Maryland Department of Transportation ("MDOT"). Only entities certified by MDOT may be counted for purposes of achieving the MBE participation goals. In order to be counted for purposes of achieving the MBE participation goals, the MBE firm, including a MBE prime, must be MDOT-certified for the services, materials or supplies that it is committed to perform on the MBE Participation Schedule.

4.   Please refer to the MDOT MBE Directory at www.mdot.state.md.us to determine if a firm is certified with the appropriate North American Industry Classification System ("NAICS") Code **and** the product/services description (specific product that a firm is certified to provide or specific areas of work that a firm is certified to perform). For more general information about NAICS, please visit www.naics.com. Only those specific products and/or services for which a firm is certified in the MDOT Directory can be used for purposes of achieving the MBE participation goals. **WARNING:** If the firm's NAICS Code is in graduated status, such services/products **may not be counted** for purposes of achieving the MBE participation goals. A NAICS Code is in the graduated status if the term "Graduated" follows the Code in the MDOT MBE Directory.

5.   **Guidelines Regarding MBE Prime Self-Performance.** Please note that when a certified MBE firm participates as a prime contractor on a contract, a procurement agency may count the distinct, clearly defined portion of the work of the contract that the certified MBE firm performs with its own workforce toward fulfilling up, but not more than, to fifty-percent (50%) of the MBE participation goal (overall, including up to one hundred percent (100%) of not more than one of the MBE participation subgoals, if any, established for the contract.

✓   In order to receive credit for self-performance, an MBE prime must list its firm in Section 4A of the MBE Participation Schedule, including the certification category under which the MBE prime is self-performing and include information regarding the work it will self-perform.

- ✓ For the remaining portion of the overall goal and the subgoals, the MBE prime must also identify other certified MBE subcontractors (see Section 4B of the MBE Participation Schedule) used to meet those goals or request a waiver.
- ✓ These guidelines apply to the work performed by the MBE Prime that can be counted for purposes of meeting the MBE participation goals. These requirements do not affect the MBE Prime's ability to self-perform a greater portion of the work in excess of what is counted for purposes of meeting the MBE participation goals.
- ✓ Please note that the requirements to meet the MBE participation overall goal and subgoals are distinct and separate. If the Contract has subgoals, regardless of MBE Prime's ability to self-perform up to 50% of the overall goal (including up to 100% of any subgoal), the MBE Prime must either commit to other MBEs for each of any remaining subgoals or request a waiver. As set forth in **Attachment <<mbeAttachmentNumber>>1-B** Waiver Guidance, the MBE Prime's ability to self-perform certain portions of the work of the Contract will not be deemed a substitute for the good faith efforts to meet any remaining subgoal or the balance of the overall goal.
- ✓ In certain instances where the percentages allocated to MBE participation subgoals add up to more than 50% of the overall goal, the portion of self-performed work that an MBE Prime may count toward the overall goal may be limited to less than 50%. Please refer to GOMA's website (www.goma.maryland.gov) for the MBE Prime Regulations Q&A for illustrative examples.

6.   Subject to items 1 through 5 above, when a certified MBE performs as a participant in a joint venture, a procurement agency may count a portion of the total dollar value of the contract equal to the distinct, clearly-defined portion of the work of the contract that the certified MBE performs with its workforce towards fulfilling the contract goal, and not more than one of the contract subgoals, if any.

7.   As set forth in COMAR 21.11.03.12-1, once the Contract work begins, the work performed by a certified MBE firm, including an MBE prime, can only be counted towards the MBE participation goal(s) if the MBE firm is performing a commercially useful function on the Contract. Please refer to COMAR 21.11.03.12-1 for more information regarding these requirements.

8.   If you have any questions as to whether a firm is certified to perform the specific services or provide specific products, please contact MDOT's Office of Minority Business Enterprise at 1-800-544-6056 or via email to mbe@mdot.state.md.us sufficiently prior to the submission due date.

9.   Worksheet: The percentage of MBE participation, calculated using the percentage amounts for all of the MBE firms listed on the Participation Schedule MUST at least equal the MBE participation goal **and** subgoals (if applicable) set forth in the solicitation. If a bidder/offeror is unable to achieve the MBE participation goal and/or any subgoals (if applicable), the bidder/offeror must request a waiver in Item 1 of the MBE Utilization and Fair Solicitation Affidavit (Attachment 2-1A) or the bid will be deemed not responsive, or the proposal determined to be not susceptible of being selected for award. You may wish to use the Subgoal summary below to assist in calculating the percentages and confirm that you have met the applicable MBE participation goal and subgoals, if any.

Subgoals (if applicable)

Total African American MBE Participation: _____%

Total Asian American MBE Participation: _____%

Total Hispanic American MBE Participation: _____%

Total Women-Owned MBE Participation: _____%

Overall Goal

Total MBE Participation (include all categories):   _____%

ATTACHMENT 2 -1A MBE UTILIZATION AND FAIR SOLICITATION AFFIDAVIT & MBE PARTICIPATION SCHEDULE

This MBE Utilization and Fair Solicitation Affidavit and MBE Participation Schedule **MUST BE** included with the bid/proposal for any solicitation with an MBE goal greater than 0%. If the Bidder/offeror fails to accurately complete and submit this Affidavit and Schedule with the bid or offer as required, the TO Procurement Officer shall deem the bid non-responsive or shall determine that the offer is not reasonably susceptible of being selected for award.

In conjunction with the bid or offer submitted in response to Solicitation No. DHMH OPASS 18-17607 M00B8400002, I affirm the following:

1. MBE Participation (PLEASE CHECK ONLY ONE)

☐   I acknowledge and intend to meet the overall certified Minority Business Enterprise (MBE) participation goal of ____ percent and, if specified in the solicitation, the following subgoals (complete for only those subgoals that apply):

    ____ percent African American-owned MBE firms

    ____ percent Asian American-owned MBE firms

    ____ percent Hispanic American-owned MBE firms

    ____ percent Woman-Owne2-owned MBE firms

    Therefore, I am not seeking a waiver pursuant to COMAR 21.11.03.11.

    Notwithstanding any subgoals established above, the Contractor is encouraged to use a diverse group of subcontractors and suppliers from any/all of the various MBE classifications to meet the remainder of the overall MBE participation goal.

OR

☐   I conclude that I am unable to achieve the MBE participation goal and/or subgoals. I hereby request a waiver, in whole or in part, of the overall goal and/or subgoals. Within 10 working days of receiving notice that our firm is the apparent awardee, I will submit completed Good Faith Efforts Documentation to Support Waiver Request (Attachment 2-1C) and all required waiver documentation in accordance with COMAR 21.11.03.

2.   Additional MBE Documentation

I understand that if I am notified that I am the apparent awardee or as requested by the Procurement Officer, I must submit the following documentation within 10 business days of receiving notice of the potential award or from the date of conditional award (per COMAR 21.11.03.10), whichever is earlier:

(a) Outreach Efforts Compliance Statement (Attachment 2-2);

(b) MBE Subcontractor Project Participation Statement (Attachment 2-3);

(c) Any other documentation, including waiver documentation if applicable, required by the Procurement Officer to ascertain bidder or offeror responsibility in connection with the certified MBE participation goal and subgoals, if any.

I understand that if I fail to return each completed document within the required time, the Procurement Officer may determine that I am not responsible and therefore not eligible for contract award. If the contract has already been awarded, the award is voidable.

3.   Information Provided to MBE firms

State of Maryland- Department of Health and Mental Hygiene

In the solicitation of subcontract quotations or offers, MBE firms were provided not less than the same information and amount of time to respond as were non-MBE firms.

4.   MBE Participation Schedule

Set forth below are the (i) certified MBEs I intend to use, (ii) the percentage of the total Contract amount allocated to each MBE for this project and, (iii) the items of work each MBE will provide under the Contract. I have confirmed with the MDOT database that the MBE firms identified below are performing work activities for which they are MDOT certified.

Prime Contractor: (Firm Name, Address, Phone)	Project Description:
Project Number:	

LIST INFORMATION FOR EACH CERTIFIED MBE FIRM YOU AGREE TO USE TO ACHIEVE THE MBE PARTICIPATION GOAL AND SUBGOALS, IF ANY.

MBE PRIMES: PLEASE COMPLETE BOTH SECTIONS A AND B BELOW.

SECTION A: For MBE Prime Contractors ONLY (including MBE Primes in a Joint Venture)

MBE Prime Firm Name:_____ MBE Certification Number: _____ (If dually certified, check only one box.) ☐ African American-Owned ☐ Hispanic American- Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification	Percentage of total Contract Value to be performed with own forces and counted towards the MBE overall participation goal (up to 50% of the overall goal): _____% Percentage of total Contract Value to be performed with own forces and counted towards the subgoal, if any, for my MBE classification (up to 100% of not more than one subgoal): _____% Description of the Work to be performed with MBE prime's own forces: _____ _____

SECTION B: For all Contractors (including MBE Primes and MBE Primes in a Joint Venture)

MBE Firm Name: _____ MBE Certification Number: _____ (If dually certified, check only one box.) ☐ African American-Owned ☐ Hispanic American- Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification	Percentage of Total Contract to be performed by this MBE: _____% Description of the Work to be Performed: _____ _____ _____ _____
MBE Firm Name: _____ MBE Certification Number: _____ (If dually certified, check only one box.) ☐ African American-Owned ☐ Hispanic American- Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification	Percentage of Total Contract to be performed by this MBE: _____% Description of the Work to be Performed: _____ _____ _____ _____
MBE Firm Name: _____ MBE Certification Number: _____ (If dually certified, check only one box.) ☐ African American-Owned ☐ Hispanic American- Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification	Percentage of Total Contract to be performed by this MBE: _____% Description of the Work to be Performed: _____ _____ _____ _____
MBE Firm Name: _____ MBE Certification Number: _____ (If dually certified, check only one box.) ☐ African American-Owned ☐ Hispanic American- Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification	Percentage of Total Contract to be performed by this MBE: _____% Description of the Work to be Performed: _____ _____ _____ _____

<u>CONTINUE ON SEPARATE PAGE IF NEEDED</u>

I solemnly affirm under the penalties of perjury that I have reviewed the instructions for the MBE MBE Utilization & Fair Solicitation Affidavit and MBE Schedule and that the information included in the Schedule is true to the best of my knowledge, information and belief.

_____   _____

Bidder/Offeror Name   Signature of Authorized Representative

(PLEASE PRINT OR TYPE)

_____   _____

Address   Printed Name and Title

_____   _____

City, State and Zip Code   Date

SUBMIT AS INSTRUCTED IN TORFP

ATTACHMENT 2 -1B WAIVER GUIDANCE

GUIDANCE FOR DOCUMENTING GOOD FAITH EFFORTS TO MEET MBE PARTICIPATION GOALS

In order to show that it has made good faith efforts to meet the Minority Business Enterprise (MBE) participation goal (including any MBE subgoals) on a contract, the bidder/offeror must either (1) meet the MBE Goal(s) and document its commitments for participation of MBE Firms, or (2) when it does not meet the MBE Goal(s), document its Good Faith Efforts to meet the goal(s).

I.   Definitions

MBE Goal(s) – "MBE Goal(s)" refers to the MBE participation goal and MBE participation subgoal(s).

Good Faith Efforts – The "Good Faith Efforts" requirement means that when requesting a waiver, the bidder/offeror must demonstrate that it took all necessary and reasonable steps to achieve the MBE Goal(s), which, by their scope, intensity, and appropriateness to the objective, could reasonably be expected to obtain sufficient MBE participation, even if those steps were not fully successful. Whether a bidder/offeror that requests a waiver made adequate good faith efforts will be determined by considering the quality, quantity, and intensity of the different kinds of efforts that the bidder/offeror has made. The efforts employed by the bidder/offeror should be those that one could reasonably expect a bidder/offeror to take if the bidder/offeror were actively and aggressively trying to obtain MBE participation sufficient to meet the MBE contract goal and subgoals. Mere *pro forma* efforts are not good faith efforts to meet the MBE contract requirements. The determination concerning the sufficiency of the bidder's/offeror's good faith efforts is a judgment call; meeting quantitative formulas is not required.

Identified Firms – "Identified Firms" means a list of the MBEs identified by the procuring agency during the goal setting process and listed in the procurement as available to perform the Identified Items of Work. It also may include additional MBEs identified by the bidder/offeror as available to perform the Identified Items of Work, such as MBEs certified or granted an expansion of services after the procurement was issued. If the procurement does not include a list of Identified Firms, this term refers to all of the MBE Firms (if State-funded) the bidder/offeror identified as available to perform the Identified Items of Work and should include all appropriately certified firms that are reasonably identifiable.

Identified Items of Work – "Identified Items of Work" means the bid items identified by the procuring agency during the goal setting process and listed in the procurement as possible items of work for performance by MBE Firms. It also may include additional portions of items of work the bidder/offeror identified for performance by MBE Firms to increase the likelihood that the MBE Goal(s) will be achieved. If the procurement does not include a list of Identified Items of Work, this term refers to all of the items of work the bidder/offeror identified as possible items of work for performance by MBE Firms and should include all reasonably identifiable work opportunities.

MBE Firms – "MBE Firms" refers to a firm certified by the Maryland Department of Transportation ("MDOT") under COMAR 21.11.03. Only MDOT-certified MBE Firms can participate in the State's MBE Program.

II.   Types of Actions Agency will Consider

The bidder/offeror is responsible for making relevant portions of the work available to MBE subcontractors and suppliers and to select those portions of the work or material needs consistent with the available MBE subcontractors and suppliers, so as to facilitate MBE participation. The following is a list of types of actions the procuring agency will consider as part of the bidder's/offeror's Good Faith Efforts when the bidder/offeror fails to meet the MBE Goal(s). This list is not intended to be a mandatory checklist, nor is it intended to be exclusive or exhaustive. Other factors or types of efforts may be relevant in appropriate cases.

A.   Identify Bid Items as Work for MBE Firms

1.   Identified Items of Work in Procurements

(a) Certain procurements will include a list of bid items identified during the goal setting process as possible work for performance by MBE Firms. If the procurement provides a list of Identified Items of Work, the bidder/offeror shall make all reasonable efforts to solicit quotes from MBE Firms to perform that work.

(b) Bidders/Offerors may, and are encouraged to, select additional items of work to be performed by MBE Firms to increase the likelihood that the MBE Goal(s) will be achieved.

2.   Identified Items of Work by Bidders/Offerors

(a) When the procurement does not include a list of Identified Items of Work or for additional Identified Items of Work, bidders/offerors should reasonably identify sufficient items of work to be performed by MBE Firms.

(b) Where appropriate, bidders/offerors should break out contract work items into economically feasible units to facilitate MBE participation, rather than perform these work items with their own forces. The ability or desire of a prime contractor to perform the work of a contract with its own organization does not relieve the bidder/offeror of the responsibility to make Good Faith Efforts.

B.   Identify MBE Firms to Solicit

1.   MBE Firms Identified in Procurements

(a) Certain procurements will include a list of the MBE Firms identified during the goal setting process as available to perform the items of work. If the procurement provides a list of Identified MBE Firms, the bidder/offeror shall make all reasonable efforts to solicit those MBE firms.

(b)   Bidders/offerors may, and are encouraged to, search the MBE Directory to identify additional MBEs who may be available to perform the items of work, such as MBEs certified or granted an expansion of services after the solicitation was issued.

2.   MBE Firms Identified by Bidders/Offerors

(a) When the procurement does not include a list of Identified MBE Firms, bidders/offerors should reasonably identify the MBE Firms that are available to perform the Identified Items of Work.

(b) Any MBE Firms identified as available by the bidder/offeror should be certified to perform the Identified Items of Work.

C.   Solicit MBEs

1.   Solicit all Identified Firms for all Identified Items of Work by providing written notice. The bidder/offeror should:

(a) provide the written solicitation at least 10 days prior to bid opening to allow sufficient time for the MBE Firms to respond;

(b) send the written solicitation by first-class mail, facsimile, or email using contact information in the MBE Directory, unless the bidder/offeror has a valid basis for using different contact information; and

(c) provide adequate information about the plans, specifications, anticipated time schedule for portions of the work to be performed by the MBE, and other requirements of the contract to assist MBE Firms in responding. (This information may be provided by including hard copies in the written solicitation or by electronic means as described in C.3 below.)

2.   "All" Identified Firms includes the MBEs listed in the procurement and any MBE Firms you identify as potentially available to perform the Identified Items of Work, but it does not include MBE Firms who are no longer certified to perform the work as of the date the bidder/offeror provides written solicitations.

3.   "Electronic Means" includes, for example, information provided via a website or file transfer protocol (FTP) site containing the plans, specifications, and other requirements of the contract. If an interested MBE cannot access the information provided by electronic means, the bidder/offeror must make the information available in a manner that is accessible to the interested MBE.

4.   Follow up on initial written solicitations by contacting MBEs to determine if they are interested. The follow up contact may be made:

(a) by telephone using the contact information in the MBE Directory, unless the bidder/offeror has a valid basis for using different contact information; or

(b) in writing *via* a method that differs from the method used for the initial written solicitation.

5.   In addition to the written solicitation set forth in C.1 and the follow up required in C.4, use all other reasonable and available means to solicit the interest of MBE Firms certified to perform the work of the contract. Examples of other means include:

(a) attending any pre-bid meetings at which MBE Firms could be informed of contracting and subcontracting opportunities; and

(b) if recommended by the procurement, advertising with or effectively using the services of at least two minority focused entities or media, including trade associations, minority/women community organizations, minority/women contractors' groups, and local, state, and federal minority/women business assistance offices listed on the MDOT Office of Minority Business Enterprise website.

D.   Negotiate With Interested MBE Firms

Bidders/Offerors must negotiate in good faith with interested MBE Firms.

1.   Evidence of negotiation includes, without limitation, the following:

(a) the names, addresses, and telephone numbers of MBE Firms that were considered;

(b) a description of the information provided regarding the plans and specifications for the work selected for subcontracting and the means used to provide that information; and

(c) evidence as to why additional agreements could not be reached for MBE Firms to perform the work.

2.   A bidder/offeror using good business judgment would consider a number of factors in negotiating with subcontractors, including MBE subcontractors, and would take a firm's price and capabilities as well as contract goals into consideration.

3.   The fact that there may be some additional costs involved in finding and using MBE Firms is not in itself sufficient reason for a bidder's/offeror's failure to meet the contract MBE goal(s), as long as such costs are reasonable. Factors to take into consideration when determining whether a MBE Firm's quote is excessive or unreasonable include, without limitation, the following:

(a)   the dollar difference between the MBE subcontractor's quote and the average of the other subcontractors' quotes received by the bidder/offeror;

(b) the percentage difference between the MBE subcontractor's quote and the average of the other subcontractors' quotes received by the bidder/offeror;

(c) the percentage that the MBE subcontractor's quote represents of the overall contract amount;

(d) the number of MBE firms that the bidder/offeror solicited for that portion of the work;

(e) whether the work described in the MBE and Non-MBE subcontractor quotes (or portions thereof) submitted for review is the same or comparable; and

(f) the number of quotes received by the bidder/offeror for that portion of the work.

4.   The above factors are not intended to be mandatory, exclusive, or exhaustive, and other evidence of an excessive or unreasonable price may be relevant.

5.   The bidder/offeror may not use its price for self-performing work as a basis for rejecting a MBE Firm's quote as excessive or unreasonable.

6.   The "average of the other subcontractors' quotes received" by the bidder/offeror refers to the average of the quotes received from all subcontractors. Bidder/offeror should attempt to receive quotes from at least three subcontractors, including one quote from a MBE and one quote from a Non-MBE.

7.   A bidder/offeror shall not reject a MBE Firm as unqualified without sound reasons based on a thorough investigation of the firm's capabilities. For each certified MBE that is rejected as unqualified or that placed a subcontract quotation or offer that the bidder/offeror concludes is not acceptable, the bidder/offeror must provide a written detailed statement listing the reasons for this conclusion. The bidder/offeror also must document the steps taken to verify the capabilities of the MBE and Non-MBE Firms quoting similar work.

(a) The factors to take into consideration when assessing the capabilities of a MBE Firm, include, but are not limited to the following: financial capability, physical capacity to perform, available personnel and equipment, existing workload, experience performing the type of work, conduct and performance in previous contracts, and ability to meet reasonable contract requirements.

(b) The MBE Firm's standing within its industry, membership in specific groups, organizations, or associations and political or social affiliations (for example union vs. non-union employee status) are not legitimate causes for the rejection or non-solicitation of bids in the efforts to meet the project goal.

E.   Assisting Interested MBE Firms

When appropriate under the circumstances, the decision-maker will consider whether the bidder/offeror:

1.   made reasonable efforts to assist interested MBE Firms in obtaining the bonding, lines of credit, or insurance required by the procuring agency or the bidder/offeror; and

2.   made reasonable efforts to assist interested MBE Firms in obtaining necessary equipment, supplies, materials, or related assistance or services.

III.   Other Considerations

In making a determination of Good Faith Efforts the decision-maker may consider engineering estimates, catalogue prices, general market availability and availability of certified MBE Firms in the area in which the work is to be performed, other bids or offers and subcontract bids or offers substantiating significant variances between certified MBE and Non-MBE costs of participation, and their impact on the overall cost of the contract to the State and any other relevant factors.

The decision-maker may take into account whether a bidder/offeror decided to self-perform subcontract work with its own forces, especially where the self-performed work is Identified Items of Work in the procurement. The decision-maker also may take into account the performance of other bidders/offerors in meeting the contract. For example, when the apparent successful bidder/offeror fails to meet the contract goal, but others meet it, this reasonably raises the question of whether, with additional reasonable efforts, the apparent successful bidder/offeror could have met the goal. If the apparent successful bidder/offeror fails to meet the goal, but meets or exceeds the average MBE participation obtained by other bidders/offerors, this, when viewed in conjunction with other factors, could be evidence of the apparent successful bidder/offeror having made Good Faith Efforts.

IV.   Documenting Good Faith Efforts

At a minimum, a bidder/offeror seeking a waiver of the MBE Goal(s) or a portion thereof must provide written documentation of its Good Faith Efforts, in accordance with COMAR 21.11.03.11, within 10 business days after receiving notice that it is the apparent awardee. The written documentation shall include the following:

A.   Items of Work (Complete Good Faith Efforts Documentation Attachment 2-1C, Part 1)

A detailed statement of the efforts made to select portions of the work proposed to be performed by certified MBE Firms in order to increase the likelihood of achieving the stated MBE Goal(s).

B.   Outreach/Solicitation/Negotiation

1.   The record of the bidder's/offeror's compliance with the outreach efforts prescribed by COMAR 21.11.03.09C(2)(a). (Complete Outreach Efforts Compliance Statement – Attachment 2-2).

2.   A detailed statement of the efforts made to contact and negotiate with MBE Firms including:

(a) the names, addresses, and telephone numbers of the MBE Firms who were contacted, with the dates and manner of contacts (letter, fax, email, telephone, etc.) **(Complete Good Faith Efforts Attachment 2-1C Part 2, and submit letters, fax cover sheets, emails, etc. documenting solicitations)**; and

(b) a description of the information provided to MBE Firms regarding the plans, specifications, and anticipated time schedule for portions of the work to be performed and the means used to provide that information.

C.   Rejected MBE Firms (Complete Good Faith Efforts Attachment 2-1C, Part 3)

1.   For each MBE Firm that the bidder/offeror concludes is not acceptable or qualified, a detailed statement of the reasons for the bidder's/offeror's conclusion, including the steps taken to verify the capabilities of the MBE and Non-MBE Firms quoting similar work.

2.   For each certified MBE Firm that the bidder/offeror concludes has provided an excessive or unreasonable price, a detailed statement of the reasons for the bidder's/offeror's conclusion, including the quotes received from all MBE and Non-MBE firms bidding on the same or comparable work. **(Include copies of all quotes received.)**

3.   A list of MBE Firms contacted but found to be unavailable. This list should be accompanied by a MBE Unavailability Certificate (see Exhibit A to this Part 1) signed by the MBE contractor or a statement from the bidder/offeror that the MBE contractor refused to sign the MBE Unavailability Certificate.

D.   Other Documentation

1.   Submit any other documentation requested by the Procurement Officer to ascertain the bidder's/offeror's Good Faith Efforts.

2.   Submit any other documentation the bidder/offeror believes will help the Procurement Officer ascertain its Good Faith Efforts.

Exhibit A
MBE Subcontractor Unavailability Certificate

1. It is hereby certified that the firm of _____

(Name of Minority firm)

located at _____

(Number)   (Street)

_____

(City)   (State)   (Zip)

was offered an opportunity to bid on Solicitation No. _____

in _____ County by_____

(Name of Prime Contractor's Firm)

****

2._____ (Minority Firm), is either unavailable for the
work/service or unable to prepare a bid for this project for the following reason(s):

_____

_____

_____

_____   _____   _____

Signature of Minority Firm's MBE Representative   **Title**   **Date**

_____   _____

MDOT Certification #   Telephone #

****

3. To be completed by the prime contractor if Section 2 of this form is <u>not</u> completed by the minority firm.

To the best of my knowledge and belief, said Certified Minority Business Enterprise is either unavailable
for the work/service for this project, is unable to prepare a bid, or did not respond to a request for a price
proposal and has not completed the above portion of this submittal.

_____   _____   _____

Signature of Prime Contractor   **Title**   **Date**

ATTACHMENT 2 -1C MBE ATTACHMENT
GOOD FAITH EFFORTS DOCUMENTATION TO SUPPORT WAIVER REQUEST

Page __ of ___

Prime Contractor:	Project Description:
DHMH OPASS 18-17607 M00B8400002:	

Parts 1, 2, and 3 must be included with this certificate along with all documents supporting your waiver request.

I affirm that I have reviewed Attachment 2-1B, Waiver Guidance. I further affirm under penalties of perjury that the contents of Parts 1, 2, and 3 of this Attachment 2-1C Good Faith Efforts Documentation Form are true to the best of my knowledge, information, and belief.

_____   _____

Company Name   Signature of Representative

_____   _____

Address   Printed Name and Title

_____   _____

City, State and Zip Code   Date

GOOD FAITH EFFORTS DOCUMENTATION TO SUPPORT WAIVER REQUEST

Part 1 – Identified items of work bidder/offeror made available to MBE firms

Page __ of ___

Prime Contractor:	Project Description:
DHMH OPASS 18-17607 M00B8400002:	

Identify those items of work that the bidder/offeror made available to MBE Firms. This includes, where appropriate, those items the bidder/offeror identified and determined to subdivide into economically feasible units to facilitate the MBE participation. For each item listed, show the anticipated percentage of the total contract amount. It is the bidder's/offeror's responsibility to demonstrate that sufficient work to meet the goal was made available to MBE Firms, and the total percentage of the items of work identified for MBE participation equals or exceeds the percentage MBE goal set for the procurement. Note: If the procurement includes a list of bid items identified during the goal setting process as possible items of work for performance by MBE Firms, the bidder/offeror should make all of those items of work available to MBE Firms or explain why that item was not made available. If the bidder/offeror selects additional items of work to make available to MBE Firms, those additional items should also be included below.

Identified Items of Work	Was this work listed in the procurement?	Does bidder/ offeror normally self-perform this work?	Was this work made available to MBE Firms? If no, explain why?
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes □ No	□ Yes □ No
	□ Yes □ No	□ Yes No	□ Yes □ No

☐ Please check if Additional Sheets are attached.

GOOD FAITH EFFORTS DOCUMENTATION TO SUPPORT WAIVER REQUEST

Part 2 – identified MBE firms and record of solicitations

Page __ of ___

Prime Contractor:	Project Description:
DHMH OPASS 18-17607 M00B8400002:	

Identify the MBE Firms solicited to provide quotes for the Identified Items of Work made available for MBE participation. Include the name of the MBE Firm solicited, items of work for which bids/quotes were solicited, date and manner of initial and follow-up solicitations, whether the MBE provided a quote, and whether the MBE is being used to meet the MBE participation goal. MBE Firms used to meet the participation goal must be included on the MBE Participation Schedule. Note: If the procurement includes a list of the MBE Firms identified during the goal setting process as potentially available to perform the items of work, the bidder/offeror should solicit all of those MBE Firms or explain why a specific MBE was not solicited. If the bidder/offeror identifies additional MBE Firms who may be available to perform Identified Items of Work, those additional MBE Firms should also be included below. Copies of all written solicitations and documentation of follow-up calls to MBE Firms must be attached to this form. This list should be accompanied by a Minority Contractor Unavailability Certificate signed by the MBE contractor or a statement from the bidder/offeror that the MBE contractor refused to sign the Minority Contractor Unavailability Certificate (see Exhibit A to MBE Attachment 2-1B). If the bidder/offeror used a Non-MBE or is self-performing the identified items of work, Part 4 must be completed.

Name of Identified MBE Firm & MBE Classification	Describe Item of Work Solicited	Initial Solicitation Date & Method	Follow-up Solicitation Date & Method	Details for Follow-up Calls	Quote Rec'd	Quote Used	Reason Quote Rejected
Firm Name: **MBE Classification (Check only if requesting waiver of MBE subgoal.)** ☐ African American-Owned ☐ Hispanic American- Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification		Date: ☐ Mail ☐ Facsimile ☐ Email	Date: ☐ Phone ☐ Mail ☐ Facsimile ☐ Email	Time of Call: Spoke With: ☐ Left Message	☐ Yes ☐ No	☐ Yes ☐ No	☐ Used Other MBE ☐ Used Non-MBE ☐ Self-performing
Firm Name: **MBE Classification (Check only if requesting waiver of MBE subgoal.)** ☐ African American-Owned ☐ Hispanic American- Owned ☐ Asian American-Owned ☐ Women-Owned ☐ Other MBE Classification		Date: ☐ Mail ☐ Facsimile ☐ Email	Date: ☐ Phone ☐ Mail ☐ Facsimile ☐ Email	Time of Call: Spoke With: ☐ Left Message	☐ Yes ☐ No	☐ Yes ☐ No	☐ Used Other MBE ☐ Used Non-MBE ☐ Self-performing

☐ Please check if Additional Sheets are attached.

GOOD FAITH EFFORTS DOCUMENTATION TO SUPPORT WAIVER REQUEST

Part 3 – additional information regarding rejected MBE quotes

Page __ of ___

Prime Contractor:	Project Description:
DHMH OPASS 18-17607 M00B8400002:	

This form must be completed if Part 1 indicates that a MBE quote was rejected because the bidder/offeror is using a Non-MBE or is self-performing the Identified Items of Work. Provide the Identified Items Work, indicate whether the work will be self-performed or performed by a Non-MBE, and if applicable, state the name of the Non-MBE. Also include the names of all MBE and Non-MBE Firms that provided a quote and the amount of each quote.

Describe Identified Items of Work Not Being Performed by MBE (Include spec/ Section number from bid)	Self-performing or Using Non-MBE (Provide name)	Amount of Non-MBE Quote	Name of Other Firms who Provided Quotes & Whether MBE or Non-MBE	Amount Quoted	Indicate Reason Why MBE Quote Rejected & Briefly Explain
	□ Self-performing □ Using Non-MBE _____	$_____	_____ □ MBE □ Non-MBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE _____	$_____	_____ □ MBE □ Non-MBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE _____	$_____	_____ □ MBE □ Non-MBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE _____	$_____	_____ □ MBE □ Non-MBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE _____	$_____	_____ □ MBE □ Non-MBE	$_____	□ Price □ Capabilities □ Other
	□ Self-performing □ Using Non-MBE _____	$_____	_____ □ MBE □ Non-MBE	$_____	□ Price □ Capabilities □ Other

☐ Please check if Additional Sheets are attached.

ATTACHMENT 2 -2 MBE ATTACHMENT
OUTREACH EFFORTS COMPLIANCE STATEMENT

Complete and submit this form within 10 working days of notification of apparent award or actual award, whichever is earlier.

In conjunction with the bid/proposal submitted in response to Solicitation No. DHMH OPASS 18-17607 M00B8400002, I state the following:

1. Bidder/Offeror identified subcontracting opportunities in these specific work categories: _____

_____

2. Attached to this form are copies of written solicitations (with bidding/proposal instructions) used to solicit certified MBE firms for these subcontract opportunities.

3. Bidder/Offeror made the following attempts to personally contact the solicited MDOT-certified MBE firms: _____

_____

4. **Please Check One:**

□ This project does not involve bonding requirements.
□ Bidder/Offeror assisted MDOT-certified MBE firms to fulfill or seek waiver of bonding requirements.
(DESCRIBE EFFORTS): _____

_____

5. **Please Check One:**

□ Bidder/Offeror did attend the pre-bid/pre-proposal conference.
□ No pre-bid/pre-proposal meeting/conference was held.
□ Bidder/Offeror did not attend the pre-bid/pre-proposal conference.

_____   _____
Company Name   Signature of Representative

_____   _____
Address   Printed Name and Title

_____   _____
City, State and Zip Code   Date

ATTACHMENT 2 -3A MBE ATTACHMENT
MBE SUBCONTRACTOR PROJECT PARTICIPATION CERTIFICATION

Please complete and submit one form for each certified MBE firm listed on the MBE Participation Schedule (Attachment 2-1A) within 10 Working Days of notification of apparent award. If the Bidder/Offeror fails to return this affidavit within the required time, the Procurement Officer may determine that the Bidder/Offeror is not responsible and therefore not eligible for Contract award.

Provided that _____ (Prime Contractor's Name) is awarded the State contract in conjunction with Solicitation No. _____, such Prime Contractor intends to enter into a subcontract with _____(Subcontractor's Name) committing to participation by the MBE firm _____ (MBE Name) with MDOT Certification Number _____ which will receive at least $_____ which equals to___% of the Total Contract Amount for performing the following products/services for the Contract:

NAICS CODE	WORK ITEM, SPECIFICATION NUMBER, LINE ITEMS OR WORK CATEGORIES (IF APPLICABLE)	DESCRIPTION OF SPECIFIC PRODUCTS AND/OR SERVICES

Each of the Contractor and Subcontractor acknowledges that, for purposes of determining the accuracy of the information provided herein, the Procurement Officer may request additional information, including, without limitation, copies of the subcontract agreements and quotes. Each of the Contractor and Subcontractor solemnly affirms under the penalties of perjury that: (i) the information provided in this MBE Subcontractor Project Participation Affidavit is true to the best of its knowledge, information and belief, and (ii) has fully complied with the State Minority Business Enterprise law, State Finance and Procurement Article §14-308(a)(2), Annotated Code of Maryland which provides that, except as otherwise provided by law, a contractor may not identify a certified minority business enterprise in a Bid/Proposal and:

(1)   fail to request, receive, or otherwise obtain authorization from the certified minority business enterprise to identify the certified Minority Business Enterprise in its Bid/Proposal;

(2)   fail to notify the certified Minority Business Enterprise before execution of the Contract of its inclusion of the Bid/Proposal;

(3)   fail to use the certified Minority Business Enterprise in the performance of the Contract; or

(4)   pay the certified Minority Business Enterprise solely for the use of its name in the Bid/Proposal.

PRIME CONTRACTOR
Signature of Representative:

_____

Printed Name and Title:

_____

Firm's Name:
_____

Federal Identification Number:
_____

Address:
_____
_____

Telephone:
_____

Date:
_____

SUBCONTRACTOR
Signature of Representative:

_____

Printed Name and Title:

_____

Firm's Name:
_____

Federal Identification Number:
_____

Address:
_____
_____

Telephone:
_____

Date:
_____

ATTACHMENT 2 -3B MBE ATTACHMENT

MBE PRIME PROJECT PARTICIPATION CERTIFICATION

Please complete and submit this form to attest each specific item of work that your MBE firm has listed on the MBE participation schedule (Attachment 2-1A) for purposes of meeting the MBE participation goals. This form must be submitted within 10 Working Days of notification of apparent award. If the Bidder/offeror fails to return this affidavit within the required time, the Procurement Officer may determine that the Bidder/offeror is not responsible and therefore not eligible for Contract award.

Provided that _____ (Prime Contractor's Name) with Certification Number _____ is awarded the State contract in conjunction with Solicitation No. _____, such MBE Prime Contractor intends to perform with its own forces at least $_____ which equals to___% of the Total Contract Amount for performing the following products/services for the Contract:

NAICS CODE	WORK ITEM, SPECIFICATION NUMBER, LINE ITEMS OR WORK CATEGORIES (IF APPLICABLE) For Construction Projects, General Conditions must be listed separately.	DESCRIPTION OF SPECIFIC PRODUCTS AND/OR SERVICES	VALUE OF THE WORK

MBE PRIME CONTRACTOR

Signature of Representative:

_____

Printed Name and Title:

_____

Firm's Name:
_____

Federal Identification Number:
_____

Address:
_____
_____

Telephone:
_____

Date:

This form must be completed monthly by the prime contractor.

ATTACHMENT 2 -4A MBE PRIME CONTRACTOR PAID/UNPAID MBE INVOICE REPORT

DHMH – OHS
Minority Business Enterprise Participation

Prime Contractor Paid/Unpaid MBE Invoice Report

Report #: _____ Reporting Period (Month/Year): _____ **Report is due to the MBE Officer by the 15th of the month following the month the services were provided.** **Note: Please number reports in sequence**	Contract #: _____ Contracting Unit: _____ Contract Amount: _____ MBE Subcontract Amt: _____ Project Begin Date: _____ Project End Date: _____ Services Provided: _____

Prime Contractor:	Contact Person:	
Address:		
City:	State:	ZIP:
Phone:	FAX: Email:	
MBE Subcontractor Name:	Contact Person:	
Phone:	FAX:	
Subcontractor Services Provided:		

List all payments made to MBE subcontractor above during this reporting period:
      Invoice#   Amount
1.
2.
3.
4.
Total Dollars Paid: $_____
	List dates and amounts of any outstanding invoices:
	      Invoice # Amount
	1.
	2.
	3.
	4.
	Total Dollars Unpaid:
	$_____

**If more than one MBE subcontractor is used for this contract, you must use separate 2-4A forms.
Information regarding payments that the MBE prime will use for purposes of meeting the MBE participation goals must be reported separately in Attachment 2-4B.
**Return one copy (hard or electronic) of this form to the following addresses (electronic copy with signature and date is preferred):

_____Contract Monitor
_____Contracting Unit
(Department)

_____
_____ mailto:

Signature:_____ Date:_____

             (Required)

<mark>*This form must be completed monthly by MBE subcontractor*</mark>

ATTACHMENT 2 *SAMPLE* MBE 2-5 SUBCONTRACTOR PAID/UNPAID MBE INVOICE REPORT

Minority Business Enterprise Participation

Subcontractor Paid/Unpaid MBE Invoice Report

Report#: ____ Reporting Period (Month/Year): _____ **Report is due by the 15th of the month following the month the services were performed.**	Contract # Contracting Unit: MBE Subcontract Amount: Project Begin Date: Project End Date: Services Provided:

MBE Subcontractor Name:

MDOT Certification #:

Contact Person: Email:

Address:

City: State: ZIP:

Phone: FAX:

Subcontractor Services Provided:

List all payments received from Prime Contractor during reporting period indicated above.	List dates and amounts of any unpaid invoices over 30 days old.
Invoice Amount Date 1. 2. 3. 4. Total Dollars Paid: $_____	Invoice Amount Date 1. 2. 3. 4. Total Dollars Unpaid: $_____

Prime Contractor: Contact Person:

**Return one copy of this form to the following address (electronic copy with signature & date is preferred):

_____Contract Monitor
_____Contracting Unit
DHMH – OHS
_____
_____ mailto:

Signature:_____ Date:_____
                 (Required)

ATTACHMENT 2 -4B MBE PRIME CONTRACTOR REPORT

DHMH – OHS

Minority Business Enterprise Participation

MBE Prime Contractor Report

MBE Prime Contractor:	Contract #: _____
Certification Number:	Contracting Unit: _____
Report #: _____	Contract Amount: _____
Reporting Period (Month/Year): _____	Total Value of the Work to the Self-Performed for
Report is due to the MBE Officer by the 15th of the month following the month the services were provided.	purposes of Meeting the MBE participation goal/subgoals: _____
Note: Please number reports in sequence	Project Begin Date: _____
	Project End Date: _____

Contact Person:		
Address:		
City:	State:	ZIP:
Phone:	Fax:	E-mail:

INVOICE NUMBER	VALUE OF THE WORK	NAICS CODE	DESCRIPTION OF SPECIFIC PRODUCTS AND/OR SERVICES

Return one copy (hard or electronic) of this form to the following addresses (electronic copy with signature and date is preferred):

Signature:_____ Date:_____

_____Contract Monitor
_____Contracting Unit
(Department)
_____
_____
_____
_____
Signature:_____ Date:_____

(Required)

<mark>*This form must be completed monthly by MBE subcontractor*</mark>

ATTACHMENT 2 -5 SUBCONTRACTOR PAID/UNPAID MBE INVOICE REPORT

Minority Business Enterprise Participation

Subcontractor Paid/Unpaid MBE Invoice Report

Report#: _____ Reporting Period (Month/Year): _____ **Report is due by the 15th of the month following the month the services were performed.**	Contract # Contracting Unit: MBE Subcontract Amount: Project Begin Date: Project End Date: Services Provided:

MBE Subcontractor Name:		
MDOT Certification #:		
Contact Person:	Email:	
Address:		
City:	State:	ZIP:
Phone:	FAX:	
Subcontractor Services Provided:		

List all payments received from Prime Contractor during reporting period indicated above.	List dates and amounts of any unpaid invoices over 30 days old.
Invoice Amount Date 1. 2. 3. 4. Total Dollars Paid: $_____	Invoice Amount Date 1. 2. 3. 4. Total Dollars Unpaid: $_____

Prime Contractor: _____ Contact Person: _____

**Return one copy of this form to the following address (electronic copy with signature & date is preferred):

_____Contract Monitor
_____Contracting Unit
DHMH – OHS

_____
_____ mailto:

Signature:_____ Date:_____
            (Required)

ATTACHMENT 3 TASK ORDER AGREEMENT

CATS+ TORFP# DHMH OPASS 18-17607 M00B8400002 OF MASTER CONTRACT #060B2490023

This Task Order Agreement ("TO Agreement") is made this day of Month, 20XX by and between _____(TO Contractor) and the STATE OF MARYLAND, Department of Health and Mental Hygiene (DHMH).

IN CONSIDERATION of the mutual promises and the covenants herein contained and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions. In this TO Agreement, the following words have the meanings indicated:

    a) "Agency" means DHMH, as identified in the CATS+ TORFP # DHMH OPASS 18-17607 M00B8400002.

    b) "CATS+ TORFP" means the Task Order Request for Proposals # DHMH OPASS 18-17607 M00B8400002, dated MONTH DAY, YEAR, including any addenda and amendments.

    c) "Master Contract" means the CATS+ Master Contract between the Maryland Department of Information Technology and TO Contractor dated April 22, 2013.

    d) "TO Procurement Officer" means Queen Davis. The Agency may change the TO Procurement Officer at any time by written notice.

    e) "TO Agreement" means this signed TO Agreement between DHMH and TO Contractor.

    f) "TO Contractor" means the CATS+ Master Contractor awarded this TO Agreement, whose principal business address is _____.

    g) "TO Contract Monitor" means Jane Holman. The Agency may change the TO Contract Monitor at any time by written notice to the TO Contractor.

    h) "TO Technical Proposal" means the TO Contractor's technical response to the CATS+ TORFP dated date of TO Technical Proposal.

    i) "TO Financial Proposal" means the TO Contractor's financial response to the CATS+ TORFP dated date of TO Financial Proposal.

    j) "TO Proposal" collectively refers to the TO Technical Proposal and TO Financial Proposal.

2. Scope of Work

2.1 This TO Agreement incorporates all of the terms and conditions of the Master Contract and shall not in any way amend, conflict with or supersede the Master Contract.

2.2 The TO Contractor shall, in full satisfaction of the specific requirements of this TO Agreement, provide the services set forth in Section 3 of the CATS+ TORFP. These services shall be provided in accordance with the Master Contract, this TO Agreement, and the following Exhibits, which are attached and incorporated herein by reference. If there is any conflict among the Master Contract, this TO Agreement, and these Exhibits, the terms of the Master Contract shall govern. If there is any conflict between this TO Agreement and any of these Exhibits, the following order of precedence shall determine the prevailing provision:

    a) The TO Agreement,

    b) Exhibit A – CATS+ TORFP

    c) Exhibit B – TO Technical Proposal

    d) Exhibit C – TO Financial Proposal

2.3   The TO Procurement Officer may, at any time, by written order, make changes in the work within the general scope of the TO Agreement. No other order, statement or conduct of the TO Procurement Officer or any other person shall be treated as a change or entitle the TO Contractor to an equitable adjustment under this Section. Except as otherwise provided in this TO Agreement, if any change under this Section causes an increase or decrease in the TO Contractor's cost of, or the time required for, the performance of any part of the work, whether or not changed by the order, an equitable adjustment in the TO Agreement price shall be made and the TO Agreement modified in writing accordingly. The TO Contractor must assert in writing its right to an adjustment under this Section within thirty (30) days of receipt of written change order and shall include a written statement setting forth the nature and cost of such claim. No claim by the TO Contractor shall be allowed if asserted after final payment under this TO Agreement. Failure to agree to an adjustment under this Section shall be a dispute under the Disputes clause of the Master Contract. Nothing in this Section shall excuse the TO Contractor from proceeding with the TO Agreement as changed.

3.   Time for Performance

Unless terminated earlier as provided in the Master Contract, the TO Contractor shall provide the services described in the TO Proposal and in accordance with the CATS+ TORFP on receipt of a Notice to Proceed from the TO Contract Monitor. The term of this TO Agreement is for a period of four (4) years commencing on the date the TO Agreement is fully executed and terminating on Month Day, Year. At the sole option of the State, this TO Agreement may be extended for one (1) additional, one (1) year period for a total TO Agreement period ending on Month, Day, Year.

4.   Consideration and Payment

4.1   The consideration to be paid the TO Contractor shall not exceed $_____. Any work performed by the TO Contractor in excess of the not-to-exceed ceiling amount of the TO Agreement without the prior written approval of the TO Contract Monitor is at the TO Contractor's risk of non-payment.

4.2   Payments to the TO Contractor shall be made as outlined Section 3 of the CATS+ TORFP, but no later than thirty (30) days after the Agency's receipt of a proper invoice for services provided by the TO Contractor, acceptance by the Agency of services provided by the TO Contractor, and pursuant to the conditions outlined in Section 4 of this Agreement.

4.3   Each invoice for services rendered must include the TO Contractor's Federal Tax Identification Number which is _____. Charges for late payment of invoices other than as prescribed by Title 15, Subtitle 1, of the State Finance and Procurement Article, Annotated Code of Maryland, as from time-to-time amended, are prohibited. Invoices must be submitted to the Agency TO Contract Monitor unless otherwise specified herein.

4.4   In addition to any other available remedies, if, in the opinion of the TO Procurement Officer, the TO Contractor fails to perform in a satisfactory and timely manner, the TO Procurement Officer may refuse or limit approval of any invoice for payment, and may cause payments to the TO Contractor to be reduced or withheld until such time as the TO Contractor meets performance standards as established by the TO Procurement Officer.

IN WITNESS THEREOF, the parties have executed this TO Agreement as of the date hereinabove set forth.

TO Contractor Name

_____   _____
By: Type or Print TO Contractor POC   Date

Witness: _____

STATE OF MARYLAND, DHMH

_____   _____
By: Queen Davis, TO Procurement Officer   Date

Witness: _____

Approved for form and legal sufficiency this _____ day of _____ 20___.

_____
Assistant Attorney General

ATTACHMENT 4 CONFLICT OF INTEREST AFFIDAVIT AND DISCLOSURE

A)   "Conflict of interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the State, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage.

B)   "Person" has the meaning stated in COMAR 21.01.02.01B(64) and includes a bidder, offeror, contractor, consultant, or subcontractor or subconsultant at any tier, and also includes an employee or agent of any of them if the employee or agent has or will have the authority to control or supervise all or a portion of the work for which a bid or offer is made.

C)   The bidder or offeror warrants that, except as disclosed in §D, below, there are no relevant facts or circumstances now giving rise or which could, in the future, give rise to a conflict of interest.

D)   The following facts or circumstances give rise or could in the future give rise to a conflict of interest (explain in detail—attach additional sheets if necessary):

E)   The bidder or offeror agrees that if an actual or potential conflict of interest arises after the date of this affidavit, the bidder or offeror shall immediately make a full disclosure in writing to the procurement officer of all relevant facts and circumstances. This disclosure shall include a description of actions which the bidder or offeror has taken and proposes to take to avoid, mitigate, or neutralize the actual or potential conflict of interest. If the contract has been awarded and performance of the contract has begun, the Contractor shall continue performance until notified by the procurement officer of any contrary action to be taken.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date:_____   By:_____

                                  (Authorized Representative and Affiant)

ATTACHMENT 5 LABOR CLASSIFICATION PERSONNEL RESUME SUMMARY
(INSTRUCTIONS)

1) For this TORFP,

   a) Master Contractors shall comply with all personnel requirements defined under the Master Contract RFP 060B2490023.

   b) Master Contractors shall propose the CATS+ Labor Category that best fits each proposed. A Master Contractor may only propose against labor categories in the Master Contractor's CATS+ Master Contract Financial Proposal.

   c) A Master Contractor's entire TO Technical Proposal will be deemed not susceptible for award if any of the following occurs:

      i) Failure to follow these instructions.

      ii) Failure to propose a resource for each job title or labor category identified in the TORFP as a required submission.

      iii) Failure of any proposed resource to meet minimum requirements as listed in this TORFP and in the CATS+ Master Contract.

      iv) Placing content on the Minimum Qualifications Summary that is not also on the Personnel Resume Form. *The function of the Minimum Qualifications Summary is to aid the agency to make a minimum qualification determination. Information on the Minimum Qualification Summary must correspond with information on the Personnel Resume form and shall not contain additional content not found on the other form.*

   d) Complete and sign the **Minimum Qualifications Summary** (Attachment 5A) and the **Personnel Resume Form** (Attachment 5B) for each resource proposed. Alternate resume formats are not allowed.

      i) The **Minimum Qualifications Summary** demonstrates the proposed resource meets minimum qualifications for the labor category, as defined in the CATS+ Master Contract RFP Section 2.10, and any additional minimum requirements stated in this TORFP. For each minimum qualification, indicate the location on the Personnel Resume Form (5B) demonstrating meeting this requirement.

      Only include the experience relevant to meeting a particular minimum qualification. Every skill must be linked to specific work experience and/or education. *The Minimum Qualification Summary shall not contain content that cannot be correlated to the Personnel Resume form.*

      Every experience listed on the Minimum Qualifications Resume Summary must be explicitly listed with start and stop dates. Where there is a time requirement such as three months' experience, you must provide the dates from and to showing an amount of time that equals or exceeds the mandatory time requirement; in this case, three months. Note: Overlapping time periods shall only count once against a specific minimum qualification (i.e., a minimum qualification may not be met by listing two examples occurring during the same time period.).

ii) The **Personnel Resume Form** provides resumes in a standard format. Additional information may be attached to each Personnel Resume Summary if it aids a full and complete understanding of the individual proposed.

ATTACHMENT 5   5A – MINIMUM QUALIFICATIONS SUMMARY

CATS+ TORFP # DHMH OPASS 18-17607 M00B8400002

All content on this form must also be on the Personnel Resume Form.
ONLY include information on this summary that supports meeting a minimum qualification.

Proposed Individual's Name and Company/Sub-Contractor:	List how the proposed individual meets each requirement by including a reference to relevant entries in Form 5B
LABOR CATEGORY TITLE – (INSERT CATS+ LABOR CATEGORY NAME)	
Education: Insert the education description from the CATS+ Master Contract RFP from Section 2.10 for the applicable labor category	(Identify school or institution Name; Address; Degree obtained and dates attended.)
Generalized Experience: Insert the generalized experience description from the CATS+ Master Contract RFP from Section 2.10 for the applicable labor category Provide dates in the format of MM/YY to MM/YY	(Identify specific work experiences from the resume that illustrate compliance with the Master Contract RFP Labor Category requirements for Generalized Experience.) <table><tr><td>FROM</td><td>TO</td><td>Job Title and Company</td></tr><tr><td>Match to Form 5B:</td><td colspan=2><insert cross-reference(s) to the full description on Form 5B></td></tr></table>
Specialized Experience: Insert the specialized experience description from the CATS+ Master Contract RFP from Section 2.10 for the applicable labor category Provide dates in the format of MM/YY to MM/YY	(Identify specific work experiences from the resume that illustrate compliance with the Master Contract RFP Labor Category requirements for Specialized Experience.) <table><tr><td>FROM</td><td>TO</td><td>Job Title and Company</td></tr><tr><td>Match to Form 5B:</td><td colspan=2><insert cross-reference to the full description on Form 5B></td></tr></table>
TORFP Additional Requirements Minimum qualifications and required certifications as defined in Section 2.1 of this TORFP. Provide dates in the format of MM/YY to MM/YY	

The information provided on this form for this labor class is true and correct to the best of my knowledge (Signatures must be included):

Master Contractor Representative:

_____   _____
Signature   Date

Proposed Individual:

_____   _____
Signature   Date

ATTACHMENT 5   5B – PERSONNEL RESUME FORM

CATS+ TORFP # DHMH OPASS 18-17607 M00B8400002

Instructions: Submit one resume form for each resource proposed. Do not submit other resume formats. Fill out each box as instructed. Failure to follow the instructions on the instructions page and in TORFP may result in the TO Proposal being considered not susceptible for award.

Resource Name:
Master Contractor: <insert Master Contractor name>   Sub-Contractor (if applicable):
Proposed CATS+ Labor Category:
Job Title (As listed in TORFP):

Education / Training (start with most recent degree / certificate)

Institution Name / City / State	Degree / Certification	Year Completed	Field Of Study
<add lines as needed>			

Relevant Work Experience*

Describe work experience relevant to the Duties / Responsibilities and Minimum Qualifications described in Section 3 of the TORFP. Start with the most recent experience first; do not include experience not relevant to the scope of this TORFP; use Employment History below for full employment history. Enter dates as MM/YY – MM/YY.   Add lines as needed.

[Organization] [Title / Role] [Period of Employment / Work (MM/YY – MM/YY)] [Location] [Contact Person (Optional if current employer)] [Technologies Used]	Description of Work (recommended: organize work descriptions to address minimum qualifications and other requirements)
[Organization] [Title / Role] [Period of Employment / Work MM/YY – MM/YY] [Location] [Contact Person] [Technologies Used]	Description of Work (recommended: organize work descriptions to address minimum qualifications and other requirements)

*Fill out each box. Do not enter "see resume" as a response.

A) References for Proposed Resource (if requested in the TORFP)

List persons the State may contact as employment references. Add lines as needed.

Reference Number:	1
Date From:	<mm/yy>
Date To:	<mm/yy>
Organization Name:	<insert organization name>
Contact Name:	<insert contact>

Contact Phone:	<insert phone>
Contact e-mail:	<insert e-mail>
Details:	<insert details>

The information provided on this form for this labor class is true and correct to the best of my knowledge (Signatures must be included):

Master Contractor Representative:

_____   _____
Signature   Date

Proposed Individual:

_____   _____
Signature   Date

Instruction: Sign each form.

ATTACHMENT 6 PRE-PROPOSAL CONFERENCE DIRECTIONS

There is a private parking garage directly across the street from 201W. Preston St. Building.

FROM THE NORTH OR SOUTH ON I-95

Take the exit for Route I-395 (Downtown Baltimore), staying in the right lane. Continue going straight using the Martin Luther King, Jr. Blvd. off-ramp. Go approximately two (2) miles and turn left at Eutaw Street. Make the next right onto Preston Street. About halfway down the block on the left is a paid visitor's parking lot. The O'Conor Building is across the street (tan building).

FROM THE NORTH ON I-83

Follow I-83 to the North Avenue exit. Make a left onto North Avenue. Immediately after you cross the bridge, make a right onto Howard Street. Proceed on Howard Street for almost a half-mile and make a right onto Preston Street (Armory on right comer). Take the second right to the paid visitor's parking lot. The O'Conor Building is across the street (tan building).

FROM THE WEST ON I-70

Take I-70 East to I-695 South toward Glen Burnie. Follow I-695 South to I-95 North. Follow I-95 to the exit for Route I-395 North. Take the exit for Route I-395 (Downtown Baltimore), staying in the right lane. Continue going straight using the Martin Luther King, Jr. Blvd. off-ramp. Go approximately two (2) miles and turn left at Eutaw Street. Make the next right onto Preston Street. About halfway down the block on the left is a paid visitor's parking lot. The O'Conor Building is across the street (tan building).

FROM ANNAPOLIS AND VICINITY ON I-97

Follow I-97 North toward Baltimore. Exit at the Baltimore Beltway (I-695) West toward Towson. Continue on I-695 to I-95 North. Take the exit for Route I-395 (Downtown Baltimore), staying in the right lane. Continue going straight using the Martin Luther King, Jr. Blvd. off-ramp. Go approximately two (2) miles and turn left at Eutaw Street. Make the next right onto Preston Street. About halfway down the block on the left is a paid visitor's parking lot. The O'Conor Building is across the street (tan building).

BALTIMORE METRO

The Baltimore Metro runs from Charles Center to Owings Mills. Get off the Subway at the State Center stop. Take the escalator, or elevator, to the top, and you will be on West Preston Street.

LIGHT RAIL

A light rail line connects Timonium, Baltimore and Glen Burnie. Get off of the Light rail at the Cultural Center Station.

ATTACHMENT 7 NOTICE TO PROCEED (SAMPLE)

Month Day, Year

TO Contractor Name

TO Contractor Mailing Address

Re: CATS+ DHMH OPASS 18-17607 M00B8400002 (TORFP #): DHMH OPASS 18-17607 M00B8400002

Dear TO Contractor Contact:

This letter is your official Notice to Proceed as of Month Day, Year, for the above-referenced Task Order Agreement. Mr. / Ms. _____ of DHMH will serve as the TO Contract Monitor and your contact person on this Task Order. He / She can be reached at telephone _____.

Enclosed is an original, fully executed Task Order Agreement and purchase order.

Sincerely,

Queen Davis

Task Order Procurement Officer

Enclosures (2)

cc: Jane Holman, TO Contract Monitor

Procurement Liaison Office, Department of Information Technology

Project Oversight Office, Department of Information Technology

ATTACHMENT 8 AGENCY DELIVERABLE PRODUCT ACCEPTANCE FORM

Agency Name: DHMH

Solicitation Title: LTSS O&M

TO Contract Monitor: (410) 767-1294

To: TO Contractor Name

The following deliverable, as required by DHMH OPASS 18-17607 M00B8400002 (TORFP #): DHMH OPASS 18-17607 M00B8400002 has been received and reviewed in accordance with the TORFP.

Title of deliverable: _____

TORFP Contract Reference Number: Section # _____

Deliverable Reference ID # _____

This deliverable:

☐   Is accepted as delivered.

☐   Is rejected for the reason(s) indicated below.

REASON(S) FOR REJECTING DELIVERABLE:

OTHER COMMENTS:

_____   _____

TO Contract Monitor Signature   Date Signed

ATTACHMENT 9 NON-DISCLOSURE AGREEMENT (OFFEROR)

THIS ATTACHMENT DOES NOT APPLY TO THIS TORFP.

ATTACHMENT 10 NON-DISCLOSURE AGREEMENT (TO CONTRACTOR)

THIS NON-DISCLOSURE AGREEMENT ("Agreement") is made as of this ___ day of _____, 20__, by and between the State of Maryland ("the State"), acting by and through its DHMH, (the "Department"), and _____ ("TO Contractor"), a corporation with its principal business office located at _____ and its principal office in Maryland located at _____.

RECITALS

WHEREAS, the TO Contractor has been awarded a Task Order Agreement (the "TO Agreement") for LTSS O&M TORFP No. DHMH OPASS 18-17607 M00B8400002 dated _____, (the "TORFP") issued under the Consulting and Technical Services procurement issued by the Department, Project Number 060B2490023; and

WHEREAS, in order for the TO Contractor to perform the work required under the TO Agreement, it will be necessary for the State to provide the TO Contractor and the TO Contractor's employees and agents (collectively the "TO Contractor's Personnel") with access to certain confidential information regarding _____ (the "Confidential Information").

NOW, THEREFORE, in consideration of being given access to the Confidential Information in connection with the TORFP and the TO Agreement, and for other good and valuable consideration, the receipt and sufficiency of which the parties acknowledge, the parties do hereby agree as follows:

1.   Regardless of the form, format, or media on or in which the Confidential Information is provided and regardless of whether any such Confidential Information is marked as such, Confidential Information means (1) any and all information provided by or made available by the State to the TO Contractor in connection with the TO Agreement and (2) any and all personally identifiable information (PII) (including but not limited to personal information as defined in Md. Ann. Code, State Govt. § 10-1301(c)) and protected health information (PHI) that is provided by a person or entity to the TO Contractor in connection with this TO Agreement. Confidential Information includes, by way of example only, information that the TO Contractor views, takes notes from, copies (if the State agrees in writing to permit copying), possesses or is otherwise provided access to and use of by the State in relation to the TO Agreement.

2.   TO Contractor shall not, without the State's prior written consent, copy, disclose, publish, release, transfer, disseminate, use, or allow access for any purpose or in any form, any Confidential Information except for the sole and exclusive purpose of performing under the TO Agreement. TO Contractor shall limit access to the Confidential Information to the TO Contractor's Personnel who have a demonstrable need to know such Confidential Information in order to perform under the TO Agreement and who have agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information. The names of the TO Contractor's Personnel are attached hereto and made a part hereof as Exhibit A. Each individual whose name appears on Exhibit A shall execute a copy of this Agreement and thereby be subject to the terms and conditions of this Agreement to the same extent as the TO Contractor. TO Contractor shall update Exhibit A by adding additional names as needed, from time to time.

3.   If the TO Contractor intends to disseminate any portion of the Confidential Information to non-employee agents who are assisting in the TO Contractor's performance of the TORFP or who will otherwise have a role in performing any aspect of the TORFP, the TO Contractor shall first obtain the written consent of the State to any such dissemination. The State may grant, deny, or condition any such consent, as it may deem appropriate in its sole and absolute subjective discretion.

4.   TO Contractor hereby agrees to hold the Confidential Information in trust and in strictest confidence, to adopt or establish operating procedures and physical security measures, and to take all other measures necessary to protect the Confidential Information from inadvertent release or disclosure to unauthorized third parties and to prevent all or any portion of the Confidential Information from falling into the public domain or into the possession of persons not bound to maintain the confidentiality of the Confidential Information.

5.   TO Contractor shall promptly advise the State in writing if it learns of any unauthorized use, misappropriation, or disclosure of the Confidential Information by any of the TO Contractor's Personnel or the TO Contractor's former Personnel. TO Contractor shall, at its own expense, cooperate with the State in seeking injunctive or other equitable relief against any such person(s).

6.   TO Contractor shall, at its own expense, return to the Department, all Confidential Information in its care, custody, control or possession upon request of the Department or on termination of the TO Agreement.

7. A breach of this Agreement by the TO Contractor or by the TO Contractor's Personnel shall constitute a breach of the Master Contract Agreement between the TO Contractor and the State.

8. TO Contractor acknowledges that any failure by the TO Contractor or the TO Contractor's Personnel to abide by the terms and conditions of use of the Confidential Information may cause irreparable harm to the State and that monetary damages may be inadequate to compensate the State for such breach. Accordingly, the TO Contractor agrees that the State may obtain an injunction to prevent the disclosure, copying or improper use of the Confidential Information. The TO Contractor consents to personal jurisdiction in the Maryland State Courts. The State's rights and remedies hereunder are cumulative and the State expressly reserves any and all rights, remedies, claims and actions that it may have now or in the future to protect the Confidential Information and/or to seek damages from the TO Contractor and the TO Contractor's Personnel for a failure to comply with the requirements of this Agreement. In the event the State suffers any losses, damages, liabilities, expenses, or costs (including, by way of example only, attorneys' fees and disbursements) that are attributable, in whole or in part to any failure by the TO Contractor or any of the TO Contractor's Personnel to comply with the requirements of this Agreement, the TO Contractor shall hold harmless and indemnify the State from and against any such losses, damages, liabilities, expenses, and/or costs.

9. TO Contractor and each of the TO Contractor's Personnel who receive or have access to any Confidential Information shall execute a copy of an agreement substantially similar to this Agreement and the TO Contractor shall provide originals of such executed Agreements to the State.

10. The parties further agree that:

   a) This Agreement shall be governed by the laws of the State of Maryland;

   b) The rights and obligations of the TO Contractor under this Agreement may not be assigned or delegated, by operation of law or otherwise, without the prior written consent of the State;

   c) The State makes no representations or warranties as to the accuracy or completeness of any Confidential Information;

   d) The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement;

   e) Signatures exchanged by facsimile are effective for all purposes hereunder to the same extent as original signatures; and

   f) The Recitals are not merely prefatory but are an integral part hereof.

TO Contractor/TO Contractor's Personnel: **DHMH:**

Name:_____   Name: _____

Title:_____   Title:_____

Date: _____   Date: _____

EXHIBIT A – FOR THE NONDISCLOSURE AGREEMENT (TO CONTRACTOR)

TO CONTRACTOR'S EMPLOYEES AND AGENTS WHO WILL BE GIVEN ACCESS TO THE
CONFIDENTIAL INFORMATION

Printed Name and Address
of Employee or Agent   Signature   Date

_____   _____   _____

_____   _____   _____

_____   _____   _____

_____   _____   _____

_____   _____   _____

ATTACHMENT 11 TO CONTRACTOR SELF-REPORTING CHECKLIST

The purpose of this checklist is for CATS+ Master Contractors to self-report on adherence to procedures for task orders (TO) awarded under the CATS+ Master Contract. Requirements for TO management can be found in the CATS+ Master Contract RFP and at the TORFP level. The Master Contractor is requested to complete and return this form by the Checklist Due Date below. Master Contractors may attach supporting documentation as needed. Please send the completed checklist and direct any related questions to contractoversight.doit@maryland.gov with the TO number in the subject line.

Master Contractor:	
Master Contractor Contact / Phone:	
Procuring State Agency Name:	
TO Title:	
TO Number:	
TO Type (Fixed Price, T&M, or Both):	
Checklist Issue Date:	
Checklist Due Date:	

Section 1 – Task Orders with Invoices Linked to Deliverables

A) Was the original TORFP (Task Order Request for Proposals) structured to link invoice payments to distinct deliverables with specific acceptance criteria?
Yes ☐   No ☐   (If no, skip to Section 2.)

B) Do TO invoices match corresponding deliverable prices shown in the accepted Financial Proposal?
Yes ☐   No ☐   (If no, explain why)

C) Is the deliverable acceptance process being adhered to as defined in the TORFP?
Yes ☐   No ☐   (If no, explain why)

Section 2 – Task Orders with Invoices Linked to Time, Labor Rates and Materials

A) If the TO involves material costs, are material costs passed to the agency without markup by the Master Contractor?
Yes ☐   No ☐   (If no, explain why)

B) Are labor rates the same or less than the rates proposed in the accepted Financial Proposal?
Yes ☐   No ☐   (If no, explain why)

C) Is the Master Contractor providing timesheets or other appropriate documentation to support invoices?
Yes ☐   No ☐   (If no, explain why)

Section 3 – Substitution of Personnel

A) Has there been any substitution of personnel?
Yes ☐   No ☐   (If no, skip to Section 4.)

B) Did the Master Contractor request each personnel substitution in writing?
Yes ☐   No ☐   (If no, explain why)

C) Does each accepted substitution possess equivalent or better education, experience and qualifications than incumbent personnel?
Yes ☐   No ☐   (If no, explain why)

Was the substitute approved by the agency in writing?
Yes ☐   No ☐   (If no, explain why)

Section 4 – MBE Participation

A) What is the MBE goal as a percentage of the TO value?   % (If there is no MBE goal, skip to Section 5)
B) Are MBE reports 2-4A, 2-4B, and 2-5 submitted monthly? Yes ☐   No ☐   (If no, explain why)
C) What is the actual MBE percentage to date? (divide the dollar amount paid to date to the MBE by the total amount paid to date on the TO)   % (Example - $3,000 was paid to date to the MBE subcontractor; $10,000 was paid to date on the TO; the MBE percentage is 30% (3,000 ÷ 10,000 = 0.30))
Is this consistent with the planned MBE percentage at this stage of the project? Yes ☐   No ☐   (If no, explain why)
Has the Master Contractor expressed difficulty with meeting the MBE goal? Yes ☐   No ☐ (If yes, explain the circumstances and any planned corrective actions)

Section 5 – TO Change Management

A) Is there a written change management procedure applicable to this TO? Yes ☐   No ☐   (If no, explain why)

B) Does the change management procedure include the following?
 	
    Yes ☐   No ☐   Sections for change description, justification, and sign-off
    Yes ☐   No ☐   Sections for impact on cost, scope, schedule, risk and quality (i.e., the impact of change on satisfying TO requirements)
    Yes ☐   No ☐   A formal group charged with reviewing / approving / declining changes (e.g., change control board, steering committee, or management team)

C) Have any change orders been executed? Yes ☐   No ☐ (If yes, explain expected or actual impact on TO cost, scope, schedule, risk and quality)
D) Is the change management procedure being followed? Yes ☐   No ☐   (If no, explain why)

SUBMIT AS INSTRUCTED IN TORFP.

ATTACHMENT 12 LIVING WAGE AFFIDAVIT OF AGREEMENT

Contract No. _____

Name of Contractor _____

Address_____

City_____ State_____ Zip Code_____

If the Contract is Exempt from the Living Wage Law

The Undersigned, being an authorized representative of the above named Contractor, hereby affirms that the Contract is exempt from Maryland's Living Wage Law for the following reasons: (check all that apply)

__ Bidder/Offeror is a nonprofit organization

__ Bidder/Offeror is a public service company

__ Bidder/Offeror employs 10 or fewer employees and the proposed contract value is less than $500,000

__ Bidder/Offeror employs more than 10 employees and the proposed contract value is less than $100,000

If the Contract is a Living Wage Contract

A.   The Undersigned, being an authorized representative of the above named Contractor, hereby affirms our commitment to comply with Title 18, State Finance and Procurement Article, Annotated Code of Maryland and, if required, to submit all payroll reports to the Commissioner of Labor and Industry with regard to the above stated contract. The Bidder/Offeror agrees to pay covered employees who are subject to living wage at least the living wage rate in effect at the time service is provided for hours spent on State contract activities, and to ensure that its Subcontractors who are not exempt also pay the required living wage rate to their covered employees who are subject to the living wage for hours spent on a State contract for services. The Contractor agrees to comply with, and ensure its Subcontractors comply with, the rate requirements during the initial term of the contract and all subsequent renewal periods, including any increases in the wage rate established by the Commissioner of Labor and Industry, automatically upon the effective date of the revised wage rate.

B.   _____(initial here if applicable) The Bidder/Offeror affirms it has no covered employees for the following reasons (check all that apply):

__ All employee(s) proposed to work on the State contract will spend less than one-half of the employee's time during every work week on the State contract;

__ All employee(s) proposed to work on the State contract will be 17 years of age or younger during the duration of the State contract; or

__ All employee(s) proposed to work on the State contract will work less than 13 consecutive weeks on the State contract.

The Commissioner of Labor and Industry reserves the right to request payroll records and other data that the Commissioner deems sufficient to confirm these affirmations at any time.

Name of Authorized Representative: _____

Signature of Authorized Representative _____

Date: _____ Title: _____

Witness Name (Typed or Printed): _____

Witness Signature and Date: _____

ATTACHMENT 13 MERCURY AFFIDAVIT

THIS ATTACHMENT DOES NOT APPLY TO THIS TORFP.

ATTACHMENT 14 VETERAN SMALL BUSINESS ENTERPRISE PARTICIPATION (VSBE) FOR STATE OF MARYLAND

THIS ATTACHMENT DOES NOT APPLY TO THIS TORFP.

ATTACHMENT 15 CERTIFICATION REGARDING INVESTMENTS IN IRAN

Authority: State Finance & Procurement, §§17-701 – 17-707, Annotated Code of Maryland [Chapter 447, Laws of 2012.]

List: The Investment Activities in Iran list identifies companies that the Board of Public Works has found to engage in investment activities in Iran; those companies may not participate in procurements with a public body in the State. "Engaging in investment activities in Iran" means:

A. Providing goods or services of at least $20 million in the energy sector of Iran; or
B. For financial institutions, extending credit of at least $20 million to another person for at least 45 days if the person is on the Investment Activities In Iran list and will use the credit to provide goods or services in the energy of Iran.

The Investment Activities in Iran list is located at: www.bpw.state.md.us

Rule: A company listed on the Investment Activities In Iran list is ineligible to bid on, submit a proposal for, or renew a contract for goods and services with a State Agency or any public body of the State. Also ineligible are any parent, successor, subunit, direct or indirect subsidiary of, or any entity under common ownership or control of, any listed company.

NOTE: This law applies only to new contracts and to contract renewals. The law does not require an Agency to terminate an existing contract with a listed company.

CERTIFICATION REGARDING INVESTMENTS IN IRAN

The undersigned certifies that, in accordance with State Finance & Procurement Article, §17-705:

(i) it is not identified on the list created by the Board of Public Works as a person engaging in investment activities in Iran as described in §17-702 of State Finance & Procurement; and

(ii) it is not engaging in investment activities in Iran as described in State Finance & Procurement Article, §17-702.

The undersigned is unable make the above certification regarding its investment activities in Iran due to the following activities:

Name of Authorized Representative: _____

Signature of Authorized Representative: _____

Date: _____ Title: _____

Witness Name (Typed or Printed): _____

Witness Signature and Date: _____

ATTACHMENT 16 SAMPLE WORK ORDER

WORK ORDER	Work Order #	Contract #

This Work Order is issued under the provisions of the Task Order. The services authorized are within the scope of services set forth in the *Purpose* of the Work Order.

Purpose

Statement of Work
Requirements *(Uniquely number each requirement):*

Deliverable(s), Acceptance Criteria and Due Date(s) (*Uniquely number each Deliverable):*

Deliverables are subject to review and approval by DHMH prior to payment.
(Attach additional sheets if necessary)

Start Date		End Date	

Cost

Description for Task(s) / Deliverable(s) / Item(s)	Quantity (if applicable)	Item Price	Estimate Total
1.		$	$
2.		$	$
*Include WBS, schedule and response to requirements.	DHMH shall pay an amount not to exceed		**$**

Contractor	Agency Approval
(Signature) Contractor Authorized Representative (Date)	(Signature) TO Contract Monitor (Date)

POC	(Print Name)	TO Contract Monitor	Jane Holman
Telephone No.		Telephone No.	(410) 767-1294
E-mail:		E-mail:	Jane.Holman@maryland.gov

ATTACHMENT 17 CRIMINAL BACKGROUND CHECK AFFIDAVIT

AUTHORIZED REPRESENTATIVE

I HEREBY AFFIRM THAT:

I am the _____(Title) and the duly authorized representative of _____(Master Contractor) and that I possess the legal authority to make this Affidavit on behalf of myself and the business for which I am acting.

I hereby affirm that _____ has complied with Section 2.4, Security Requirements of the Department of Information Technology's Consulting Technical Services Master Contract Number 060B2490023 (CATS+) hereto as Exhibit A.

I hereby affirm that the _____ has provided the Maryland Department of Health and Mental Hygiene with a summary of the security clearance results for all of the candidates that will be working on Task Order LTSS O&M OPASS 18-17607 / M00B8400002 and all of these candidates have successfully passed all of the background checks required under Section 2.4.3.2 of the CATS + Master Contract. Master Contractors hereby agrees to provide security clearance results for any additional candidates at least seven (7) days prior to the date the candidate commences work on this Task Order.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

_____

Master Contractor

_____

Typed Name

_____

Signature

_____

Date

ATTACHMENT 18 INCIDENT RESPONSE PROTOCOL

1. The TO Contractor agrees to abide by all applicable federal, State and local laws concerning information security and comply with current State and agency information security policy, currently found at http://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf. TO Contractor shall limit access to and possession of Sensitive Data to only employees whose responsibilities reasonably require such access or possession and shall train such employees on the Confidentiality obligations set forth herein.

2. The TO Contractor agrees to notify DHMH when any TO Contractor's system that may access, process, or store State data or Work Product is subject to unintended access or attack. Unintended access or attack includes compromise by a computer malware, malicious search engine, credential compromise or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures.

3. The TO Contractor further agrees to notify DHMH within twenty-four (24) hours of the discovery of the unintended access or attack by providing notice via written or electronic correspondence to the TO Contract Monitor, DHMH chief information officer and DHMH chief information security officer.

4. The TO Contractor agrees to notify DHMH within two (2) hours if there is a threat to the TO Contractor's product as it pertains to the use, disclosure, and security of DHMH's data.

5. If an unauthorized use or disclosure of any Sensitive Data occurs, the TO Contractor must provide written notice to DHMH within one (1) business day after TO Contractor's discovery of such use or disclosure and thereafter all information the State (or DHMH) requests concerning such unauthorized use or disclosure.

6. The TO Contractor, within one (1) day of discovery, shall report to DHMH any improper or non-authorized use or disclosure of Sensitive Data. The TO Contractor's report shall identify:

    (a) the nature of the unauthorized use or disclosure;

    (b) the Sensitive Data used or disclosed,

    (c) who made the unauthorized use or received the unauthorized disclosure;

    (d) what the TO Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and

    (e) what corrective action the TO Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

    (f) The TO Contractor shall provide such other information, including a written report, as reasonably requested by the State.

7. The TO Contractor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of PII, PHI or other event requiring notification. In the event of a breach of any of the TO Contractor's security obligations or other event requiring notification under applicable law, the TO Contractor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the State (or DHMH) and its officials and employees from and against any claims, damages, or other harm related to such security obligation breach or other event requiring the notification.

8. This Section shall survive expiration or termination of the TO Agreement.

ATTACHMENT 19 BUSINESS ASSOCIATE AGREEMENT

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement") is made by and between the **Office of Health Services**, a unit of the Maryland Department of Health and Mental Hygiene (herein referred to as "Covered Entity") and _____ (Insert Name of Contractor) (hereinafter known as "Business Associate"). Covered Entity and Business Associate shall collectively be known herein as the "Parties."

WHEREAS, Covered Entity has a business relationship with Business Associate that is memorialized in a separate agreement (the "Underlying Agreement") pursuant to which Business Associate may be considered a "business associate" of Covered Entity as defined in the Health Insurance Portability and Accountability Act of 1996 including all pertinent privacy regulations (45 C.F.R. Parts 160 and 164) and security regulations (45 C.F.R. Parts 160, 162, and 164), as amended from time to time, issued by the U.S. Department of Health and Human Services as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111–5) (collectively, "HIPAA"); and

WHEREAS, the nature of the contractual relationship between Covered Entity and Business Associate may involve the exchange of Protected Health Information ("PHI") as that term is defined under HIPAA; and

WHEREAS, for good and lawful consideration as set forth in the Underlying Agreement, Covered Entity and Business Associate enter into this Agreement for the purpose of ensuring compliance with the requirements of HIPAA and the Maryland Confidentiality of Medical Records Act (Md. Ann. Code, Health-General §§ 4-301 *et seq.*) ("MCMRA"); and

WHEREAS, this Agreement supersedes and replaces any and all Business Associate Agreements the Covered Entity and Business Associate may have entered into prior to the date hereof;

NOW THEREFORE, the premises having been considered and with acknowledgment of the mutual promises and of other good and valuable consideration herein contained, the Parties, intending to be legally bound, hereby agree as follows:

DEFINITIONS.

    A.   <u>Catch-all definition</u>. The following terms used in this Agreement, whether capitalized or not, shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

    B.   <u>Specific definitions</u>:

1. <u>Business Associate</u>. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean (Insert Name of Contractor).

2. <u>Covered Entity</u>. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to the party to this agreement, shall mean Office of Health Services.

3. <u>HIPAA Rules</u>. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and Part 164.

4. <u>Protected Health Information ("PHI")</u>. Protected Health Information or "PHI" shall generally have the same meaning as the term "protected health information" at 45 C.F.R. § 160.103.

PERMITTED USES AND DISCLOSURES OF PHI BY BUSINESS ASSOCIATE.

A. Business Associate may only use or disclose PHI as necessary to perform the services set forth in the Underlying Agreement or as required by law.

B. Business Associate agrees to make uses and disclosures and requests for PHI consistent with Covered Entity's policies and procedures regarding minimum necessary use of PHI.

C. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity.

D. Business Associate may, if directed to do so in writing by Covered Entity, create a limited data set, as defined at 45 CFR 164.514(e)(2) , for use in public health, research, or health care operations. Any such limited data sets shall omit any of the identifying information listed in 45 CFR § 164.514(e)(2). Business Associate will enter into a valid, HIPAA-compliant Data Use Agreement, as described in 45 CFR § 164.514(e)(4), with the limited data set recipient. Business Associate will report any material breach or violation of the data use agreement to Covered Entity immediately after it becomes aware of any such material breach or violation.

E. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration, or legal responsibilities of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

F. The Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI of an Individual pursuant to §§13405(d)(1) and (2) of the HITECH Act. This prohibition

does not apply to the State's payment of Business Associate for its performance pursuant to the Underlying Agreement.

G. The Business Associate shall comply with the limitations on marketing and fundraising communications provided in §13406 of the HITECH Act in connection with any PHI of Individuals.

DUTIES OF BUSINESS ASSOCIATE RELATIVE TO PHI.

A. Business Associate agrees that it will not use or disclose PHI other than as permitted or required by the Agreement or as Required by Law;

B. Business Associate agrees to use appropriate administrative, technical and physical safeguards to protect the privacy of PHI.

C. Business Associate agrees to use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement;

D. 1. Business Associate agrees to Report to Covered Entity any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including breaches of unsecured PHI as required by 45 C.F.R. § 164.410, and any Security Incident of which it becomes aware without reasonable delay, and in no case later than fifteen calendar days after the use or disclosure;

2. If the use or disclosure amounts to a breach of unsecured PHI, the Business Associate shall ensure its report:

A. Is made to Covered Entity without unreasonable delay and in no case later than fifteen (15) calendar days after the incident constituting the Breach is first known, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. For purposes of clarity for this Section III.D.1, Business Associate must notify Covered Entity of an incident involving the acquisition, access, use or disclosure of PHI in a manner not permitted under 45 C.F.R. Part E within fifteen (15) calendar days after an incident even if Business Associate has not conclusively determined within that time that the incident constitutes a Breach as defined by HIPAA;

B. Includes the names of the Individuals whose Unsecured PHI has been, or is reasonably believed to have been, the subject of a Breach;

C. Is in substantially the same form as **ATTACHMENT 22** attached hereto; and

D. Includes a draft letter for the Covered Entity to utilize to notify the affected Individuals that their Unsecured PHI has been, or is reasonably believed to have been, the subject of a Breach that includes, to the extent possible:

i)   A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

ii)   A description of the types of Unsecured PHI that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, disability code, or other types of information that were involved);

iii)   Any steps the affected Individuals should take to protect themselves from potential harm resulting from the Breach;

iv)   A brief description of what the Covered Entity and the Business Associate are doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches; and

v)   Contact procedures for the affected Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

E.   To the extent permitted by the Underlying Agreement, Business Associate may use agents and subcontractors. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2) shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information, Business Associate must enter into Business Associate Agreements with subcontractors as required by HIPAA;

F.   Business Associate agrees it will make available PHI in a designated record set to the Covered Entity, or, as directed by the Covered Entity, to an individual, as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524, including, if requested, a copy in electronic format;

G.   Business Associate agrees it will make any amendment(s) to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526;

H.   Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to the Covered Entity or, as directed by the Covered Entity, to an individual, as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.528;

I.   To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s);

J.   Business Associate agrees to make its internal practices, books, and records, including PHI, available to the Covered Entity and/or the Secretary for purposes of determining compliance with the HIPAA Rules.

K.   Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

IV.   TERM AND TERMINATION

A.   <u>Term</u>. The Term of this Agreement shall be effective as of the effective date of the Contract entered into following the solicitation for **LONG TERM SUPPORTS AND SERVICES SYSTEM (LTSS) Operations & Maintenance (O&M)**, Solicitation # **DHMH OPASS 15-14386**, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or the PHI created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, in accordance with the termination provisions in this Section IV, or on the date the Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner. If it is impossible to return or destroy all of the PHI provided by Covered Entity to Business Associate, or the PHI created or received by Business Associate on behalf of Covered Entity, Business Associate's obligations under this contract shall be ongoing with respect to that information, unless and until a separate written agreement regarding that information is entered into with Covered Entity.

B.   <u>Termination for Cause</u>. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall:

    1.   Provide an opportunity for Business Associate to cure the breach or end the violation and, if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, terminate this Agreement; or

    2.   Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and Covered entity determines or reasonably believes that cure is not possible.

C.   <u>Effect of Termination</u>.

    1.   Upon termination of this Agreement, for any reason, Business Associate shall return or, if agreed to by Covered Entity, destroy all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business Associate shall retain no copies of the PHI. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

    2.   Should Business Associate make an intentional or grossly negligent Breach of PHI in violation of this Agreement or HIPAA or an intentional or grossly negligent disclosure of information protected by the MCMRA, Covered Entity shall have the right to immediately terminate any contract, other than this Agreement, then in force between the Parties, including the Underlying Agreement.

D.   <u>Survival.</u> The obligations of Business Associate under this Section shall survive the termination of this agreement.

V.   CONSIDERATION

Business Associate recognizes that the promises it has made in this Agreement shall, henceforth, be detrimentally relied upon by Covered Entity in choosing to continue or commence a business relationship with Business Associate.

VI.   REMEDIES IN EVENT OF BREACH

Business Associate hereby recognizes that irreparable harm will result to Covered Entity, and to the business of Covered Entity, in the event of breach by Business Associate of any of the covenants and assurances contained in this Agreement. As such, in the event of breach of any of the covenants and assurances contained in Sections II or III above, Covered Entity shall be entitled to enjoin and restrain Business Associate from any continued violation of Sections II or III. Furthermore, in the event of breach of Sections II or III by Business Associate, Covered Entity is entitled to reimbursement and indemnification from Business Associate for Covered Entity's reasonable attorneys' fees and expenses and costs that were reasonably incurred as a proximate result of Business Associate's breach. The remedies contained in this Section VI shall be in addition to, not in lieu of, any action for damages and/or any other remedy Covered Entity may have for breach of any part of this Agreement or the Underlying Agreement or which may be available to Covered Entity at law or in equity.

VII.   MODIFICATION; AMENDMENT

This Agreement may only be modified or amended through a writing signed by the Parties and, thus, no oral modification or amendment hereof shall be permitted. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the HIPAA rules and any other applicable law.

VIII.   INTERPRETATION OF THIS AGREEMENT IN RELATION TO OTHER AGREEMENTS BETWEEN THE PARTIES

Should there be any conflict between the language of this Agreement and any other contract entered into between the Parties (either previous or subsequent to the date of this Agreement), the language and provisions of this Agreement shall control and prevail unless the parties specifically refer in a subsequent written agreement to this Agreement by its title and date and specifically state that the provisions of the later written agreement shall control over this Agreement.

IX.   COMPLIANCE WITH STATE LAW

The Business Associate acknowledges that by accepting the PHI from Covered Entity, it becomes a holder of medical information under the MCMRA and is subject to the provisions of that law. If the HIPAA Privacy or Security Rules and the MCMRA conflict regarding the degree of protection provided for PHI, Business Associate shall comply with the more restrictive protection requirement.

X.   MISCELLANEOUS

A.   <u>Ambiguity</u>. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules.

B.   <u>Regulatory References</u>. A reference in this Agreement to a Section in the HIPAA Rules means the Section as in effect or as amended.

C.   <u>Notice to Covered Entity</u>. Any notice required under this Agreement to be given Covered Entity shall be made in writing to:

Ramiek James, Esq.
Privacy Officer and Compliance Analyst
Department of Health & Mental Hygiene
Office of the Inspector General
201 W. Preston Street, Floor 5
Baltimore, MD 21201-2301
Phone: (410) 767-5411

D.   <u>Notice to Business Associate</u>. Any notice required under this Agreement to be given Business Associate shall be made in writing to:

Address: _____

                   _____

Attention: _____

Phone: _____

E.   <u>Survival</u>. Any provision of this Agreement which contemplates performance or observance subsequent to any termination or expiration of this contract shall survive termination or expiration of this Agreement and continue in full force and effect.

F.   <u>Severability</u>. If any term contained in this Agreement is held or finally determined to be invalid, illegal, or unenforceable in any respect, in whole or in part, such term shall be severed from this Agreement, and the remaining terms contained herein shall continue in full force and effect, and shall in no way be affected, prejudiced, or disturbed thereby.

G.   <u>Terms</u>. All of the terms of this Agreement are contractual and not merely recitals and none may be amended or modified except by a writing executed by all parties hereto.

H.   <u>Priority</u>. This Agreement supersedes and renders null and void any and all prior written or oral undertakings or agreements between the parties regarding the subject matter hereof.

IN WITNESS WHEREOF and acknowledging acceptance and agreement of the foregoing, the Parties affix their signatures hereto.

COVERED ENTITY: **BUSINESS ASSOCIATE:**

By: _____   By: _____

Name: _____   Name: _____

Title: _____   Title: _____

Date: _____   Date: _____

Rev. 08/01/2013

ATTACHMENT K-1

FORM OF NOTIFICATION TO COVERED ENTITY OF
BREACH OF UNSECURED PHI

This notification is made pursuant to Section III.2.D(3) of the Business Associate Agreement between **Office of Health Services**, a unit of the Maryland Department of Health and Mental Hygiene (DHMH), and
_____ (Business Associate).

Business Associate hereby notifies DHMH that there has been a breach of unsecured (unencrypted) protected health information (PHI) that Business Associate has used or has had access to under the terms of the Business Associate Agreement.

Description of the breach:
_____
_____

Date of the breach: _____ Date of discovery of the breach: _____

Does the breach involve 500 or more individuals? Yes/No   If yes, do the people live in multiple states? Yes/No

Number of individuals affected by the breach:
_____

Names of individuals affected by the breach: (attach list)

The types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code):
_____

_____

Description of what Business Associate is doing to investigate the breach, to mitigate losses, and to protect against any further breaches:
_____

_____

Contact information to ask questions or learn additional information:

Name: _____

Title: _____

Address: _____

Email Address: _____

Phone Number: _____

Rev. 08/01/2013

ATTACHMENT 20 LTSS SYSTEM TECHNICAL INFRASTRUCTURE DESIGN

20.1   Introduction

This document is an extract of a design document describing the proposed requirements to facilitate the Maryland Long-Term Services and Support (LTSS) System. DHMH's incumbent O&M contractor, Conduent (formerly Xerox), and its subcontractors, TierPoint, GANTECH and CSI, developed the To-be Technical Infrastructure Design for the purpose of supporting the LTSS System's future needs. The current LTSS System's technical infrastructure has been deemed unable to support the future business needs and it cannot be incrementally expanded to the degree necessary. Therefore, this design document specifies a completely new LTSS System technical infrastructure based on the lessons learned from the current infrastructure. The design included input from DHMH's LTSS Project technical personnel and the incumbent Software Development Task Order (TO) Contractor (FEi Systems).

This design is intended to allow for a scalable implementation (i.e. BASE-level then EXPANDED), or a one-time implementation at the EXPANDED level, whichever is best for DHMH at the time the decision is made. Therefore, the *BASE-level LTSS System Requirements* are presented that support the minimum volumes to support the initial business needs. Additional technical infrastructure requirements are addressed in the Section titles *EXPANDED to Support LTSS System and Business Growth*.

NOTES:
1.) References in this document to Xerox, Tierpoint, GANTECH, CSI or any other vendor should be ignored. These vendors appear in the diagrams because they developed the design based on the resources they could provide to meet the requirements.
2.) The Integrated Voice Response (IVR) component reflects current-state for ISAS. DHMH is currently developing additional IVR capabilities that are to be delivered by the TO Contractor. These to-be capabilities are reflected in the TEFT IVR design referenced in Section 20.4.4.2.

20.2   Architecture Overview

LTSS is hosted at a Primary Data Center. Two Cisco FlexPod computing architectures are located at the facility, composed of Cisco Unified Computing System (UCS) servers. The servers use Cisco Nexus network switching and NetApp storage.

The LTSS Technical Infrastructure Design provides full redundancy in all production VMs as well as blue and green stacks in the Primary Data Center to minimize downtime.

20.2.1   Security Overview

Access control readers are placed on the racks to physically secure the servers. This configuration provides a layer of audit and control. Only authorized individuals are allowed on the data center floor. This is managed by physical security services in the data centers.

The physical security services include:

- Manned 24 hours a day, 7 days a week, 365 days a year
- Access restricted to authorized client personnel and data center employees

- Axis IP-based interior and exterior surveillance cameras
- Entrance and exit controlled by Host Intrusion Detection (HID) contact-less access cards
- Cabinet access controlled by combination dial system
- Biometric hand-scan
- Mantraps

20.2.2   COTS Overview

TO Contractor shall provide the required COTS software identified with an asterisk (*) below. For all other COTS software, the TO Contractor may propose an equivalent alternative.

- Microsoft Windows Server Data Center Edition*
- Microsoft SQL Server Standard (includes SSRS reporting services)*
- RavenDB Standard Plus and Enterprise editions*
- IBM Sterling Connect:Direct Standard Edition w/Secure +*
- VMware vSphere Enterprise Plus*
- vCloud Suite
- Veeam Availability Suite v9
- Shavlik Protect
- SolarWinds Network Performance Monitor*
- SolarWinds Application Performance Monitor*
- Zenoss Enterprise
- Microsoft Operations Management 2016*
- BlazeMeter
- Splunk
- Ndatalign

20.2.3   Disaster Recovery Overview

In the event of a disaster, the Primary Data Center is supported with replication in the Secondary Data Center (also referred to as the disaster recovery site). The Secondary Data Center has the features required to meet security, functionality, and availability requirements. At the Secondary Data Center, an identical FlexPod infrastructure is provisioned, with replication enabled from the Primary Data Center.

20.3   LTSS Architecture

20.3.1   BASE-level LTSS System Requirements

20.3.1.1   Infrastructure Design

The infrastructure design is a FlexPod architecture consisting of Cisco Unified Computing, Cisco consolidated networking, NetApp storage, and VMware virtualization.

20.3.1.2   Compute and Virtualization

The Primary Data Center consists of nine (9) Cisco UCS 5108 chassis for redundancy, each populated with six (6) Cisco B200 M4 blades. Each blade consists of 40 CPU cores and 256GB RAM, which has been sized to meet the defined LTSS System requirements. The Primary Data Center hosts three (3) application stacks (green, blue, and pre-production) as well as a management stack. Each chassis has three blades for production (green, blue), one for Pre-Production, and two for management.

The Primary Data Center provides a computing environment consisting of three (3) VMware Clusters. The clusters are provisioned as Production, Pre-production, and Management. The Production environment consists of LTSS System modules, all with Green and Blue stacks to minimize outages. Pre-production is a sandboxed environment, consisting of a previous backup of the Production environment. The environment operates exactly as the Production environment, including performance, except that accessibility is offered via Network Address Translation to prevent IP (Internet Protocol) Address conflicts with the Production environment. The data and configurations remain identical with their roles in Production, as of the latest backup.

The Secondary Data Center is an identical infrastructure to provide a standby site that serves the LTSS System in the event of maintenance downtime or disaster recovery of the Primary Data Center. The Secondary Data Center performs replication of data from the Primary Data Center. The Secondary Data Center consists of five (5) Cisco UCS 5108 chassis for redundancy, each populated with six (6) Cisco B200 M4 blades for a total of 18 blades, divided into two (2) clusters (Prod Green, Management). Each blade consists of 40 CPU cores and 256GB RAM that have been sized to meet the defined LTSS System requirements.

The design includes a VMware vSphere hypervisor for the LTSS System. VMware vSphere is the industry-leading server virtualization platform and offers the most robust enterprise features for maximum performance and uptime of server resources. VMware's vCenter is the de facto management platform.

The Primary Data Center consists of three (3) VMware HA clusters. The VMware HA clusters are split across the thirty-six (36) blades operating on six (6) chassis. This design allows for server failure, or an entire chassis failure, in the environment with automatic built in failover and continued full capacity to operate. This configuration provides redundancy across all clusters, enabling LTSS technical infrastructure to provide higher availability and level of service across the entire environment. Multiple local layers of redundancy and failover serve to eliminate all single points of failure and allow for multiple hardware failures without reducing availability.

This design concept evenly distributes the production load among six separate chassis and three VMware HA Clusters to provide high availability in the event of a hardware failure, VMware Distributed Resource Scheduling (DRS) failure, or both. Six chassis allow for future growth of computing resources and additional resource clusters that can offer even higher levels of service, availability, and capacity.

The Production and Pre-production environments reside on separate vLANs (networks) and separate VRFs (router systems) to keep each environment separate and unique. Hosting Production and Pre-production on the same hardware and computing environment reduces inconsistencies in the environment and provides a more trusted path to Production.

The Secondary Data Center provides a Green-only Production environment, also with failure redundancy across the three chassis. Pre-production is not a requirement for the Secondary Data Center, as it is unlikely that DHMH would perform software releases while in a disaster recovery situation.

20.3.1.3   Storage

The design calls for NetApp AFF 8080 and NetApp FAS8080 Network Attached Storage systems, running the NetApp clustered Data ONTAP v9 operating System. This configuration allows all controllers in each data center to operate as clusters that can be easily maintained and offer high availability and enhanced performance. The storage systems are primarily all-flash systems with solid-state drives to maximize performance and availability for the active data in the LTSS System, with archived data on spinning disks. Spinning disks alone will not work due to the input/output (IO) contention seen on NetApp, which has a FlashPool.

All-flash systems benefit performance by removing components that cause IO contention at the disks, which then cascades throughout the storage infrastructure. Flash disks or solid state drives (SSDs) do not use the single head, single write stream model. They can write in parallel to the disks, decreasing the time needed for a single write operation and multiplying the speed increase by the number of simultaneous writes each disk can perform.

The all-flash optimized system's storage efficiency capabilities allow for better use of the disks and add value by increasing the usable capacity. The NetApp all-flash systems offer this increase in efficiency for flash storage, as well as the capability to perform inline de-duplication without affecting performance. This ensures that the data written is not duplicated and increases the efficiency of the system by reducing the amount of used data before it uses space on the disks, eliminating the need for the storage system to run jobs for de-duplication and data hygiene.

The solution uses an additional cluster containing a NetApp FAS HA (high availability fabric attached storage) pair that serves as the low-cost, low-speed, SATA (serial) storage attached to the virtual environment to provide near line storage for archival systems. The Primary Data Center hosts four NetApp AFF 8080 all-flash High Availability Controller Pairs with approximately 500TB of usable storage and 500,000 IOPS (IO operations per second) of available bandwidth across the NAS (network storage system). The controllers on the NetApp AFF 8080 Systems are configured in two (2) clusters of two (2) HA pairs, or four (4) Controllers/Nodes. This allows the workload to be distributed across the available hardware. The clustering of the filers allows for uniform configurations and performance across the environments.

The four all-flash filers are provisioned into two (2) clustered data ONTAP storage clusters, each containing two (2) NetApp Filers/HA pairs. The Primary Data Center also hosts one NetApp FAS8080 Storage, with disk shelves containing SATA disks. The controllers on the

FAS8080 are made into a separate storage cluster, available to the virtual infrastructure by archive or near line database disks. The storage systems are available to all VMware hosts via NFS. ISCSI will not be active, but it is configured the use iSCSI is needed in the environment. The clusters are provisioned into two physically and logically separate SAN/NAS fabrics, each containing 2 NetApp nodes, each with two (2) controller modules for HA purposes. The four total NetApp nodes at each site are configured in two (2) clusters, one for each environment, Production, and Pre-production. The Management Environment, which contains all the servers and services that are critical to support the LTSS System, shares a NetApp cluster with Pre-production.

Both storage clusters are accessible by only the hosts, VMs, and devices that are a part of the particular enclave. The second cluster is provisioned to host Pre-production, and Management systems.

The storage system offers equal performance within all hosts and are controlled by VMware's storage IO controls, in order to ensure that critical servers can use as much IO as necessary via SIOC (controller), VAAI API, QoS (quality of service) of the network, and UCS Fabric, as well as the virtual network. This capability also enables enhanced visibility into the storage IO of the systems and their components, with performance counters that would not be available otherwise. SIOC provides granular control of resources to enable application performance testing in the Pre-production environment while running the Management stack in parallel, allowing Pre-Production to use the IO before Management.

The Secondary Data Center hosts a NetApp infrastructure similar to the Primary Data Center, reduced in size but not performance, to ensure minimal downtimes, reduce management overhead, and perform disaster recovery or failover without reducing business continuity, and limit downtime. The storage solution comprises three AFF8080s, each with two all-flash disk shelves, and two FAS8080s with two spinning-disk shelves.

The storage systems are integrated into the Veeam backup solution to enable Veeam control as well as archiving of NetApp snapshots. The storage system is capable of encrypting data at rest, if requested. The flash memory SSDs can provide encryption at FIPS 140-2 level 2, with no effect on performance. Key management is not provided by this system, but can be built to handle the encryption keys, PKI for all internal and external certificate needs, and cryptography.

20.3.1.4   Backups

The design uses Veeam software for backups and DR functions. The backup solution comprises a Cisco UCS C3260 Medium Chassis, with approximately 448TB of on board storage, to store backups locally, minimizing RTO and RPO times and enabling fast local recovery of files, volumes, snapshots, VMs, Active Directory Objects, SQL Objects, and more. One Cisco UCS C3260 Chassis at each site is responsible for maintaining a local copy of the sites backups and a copy of the opposite site's backup repository, to enable rebuilding in the event of a catastrophic disaster at either site. Backups require replicating between the primary and secondary location on a near real-time basis to be defined within the service level agreements (SLAs).

The RavenDB databases are replicated using the RavenDB native replication and monitored in real-time to ensure that replication events are flagged and addressed. The only components not handled by Veeam Backup and Recovery or NetApp snapshots are the RavenDB servers, since they are not third-party friendly for backups. This prevents VMware, Veeam, NetApp Snapshots, or other systems from causing data integrity issues or data inconsistencies in the databases.

The SQL Server databases are replicated using SQL Replication and backed up using Veeam's SQL Integration, after which all backups are de-duplicated, compressed, and encrypted for storage at the local site. After all backups have completed, they are replicated to the Secondary Data Center using Veeam Backup Replication, or Backup Shipping, and retained for up to three days. RavenDB database backups are completed using the RavenDB native backup tool and backed up to a local drive. After the native backup, the virtual machines are backed up using Veeam Snapshot Integration on the NetApp Storage system, and then compressed, de-duplicated, and encrypted. The RavenDB backups are stored as an incremental backup and retained for one year.

All other systems are backed up using Veeam, with the policies and retention periods are defined for each server type separately and documented appropriately.

Backup Strategy and Schedule:

Occurrence	Retention	Type	Local or Offsite	Systems
Hourly (every four hrs.)	24 hours	Storage Snapshot	Local	All Systems
Daily RavenDB	72 hours	Native Back Up, then VM backup	Local	All RavenDB Servers
RavenDB Backup Shipping	28 Days	RavenDB Native Backup (Compressed), shipped to another site, via Veeam backup of disk	Off Site	All DB Servers
Daily	7 days	NetApp Storage Snapshot	Local	All Production Servers
Daily Forever Incremental, forward				
Daily Forever Incremental Backup	Unlimited, but constrained by usable storage.	Veeam Forever Incremental backups of each NetApp volume's daily storage snapshot	Local	All Production Servers

Occurrence	Retention	Type	Local or Offsite	Systems
Site Repository, and Backup Shipping to adjacent site	7 copies of the repository at the adjacent site.	Veeam Backup and Recovery – Backup shipping, and library	Local Backups and Repo copy to mirror appliance at opposite site. WAN Accelerated transfer, encrypted in flight, and at rest.	Veeam Backup and Recovery database, repository, and backups and as well as anything needed for a BMR of the Source Veeam Appliance
Weekly	4 Weeks	Veeam Backup and Recovery – Full Backup	Local & Offsite	All Servers
Monthly	36 Months	Snap Vault	Off-Site	RavenDB and SQL Servers

20.3.1.5   Networking

The Primary Data Center consists of two (2) Cisco ASA 5525 firewalls, six (6) Nexus 9K C92160YC-X switches, two (2) Cisco Nexus C9236C switches, two (2) Catalyst 3650-48TD-L switches, two (2) Cisco ASR 1001-X routers, one (1) Catalyst 3650-24TD-L switches for management, two (2) F5 BIG-IP LTM-4000S load balancers, and two (2) Cisco UCS 6332 UP Fabric Interconnects.

Internet and Wide Area Networking

Communication between the Primary and Secondary Data Centers is provided through an encrypted VPN connection between the ASA 5525 firewalls at both data centers. The connection is two (2) one gigabit per second circuits, allowing up to 250Mbps encrypted throughput per circuit using the ASA 5525 firewalls. This connection is used only as a backup, because the ASR 1001-X routers provide the requested encrypted throughput.

Internet access is provided by a "blended" Internet solution, which is a mix of high-speed Internet feeds from several Internet carriers for redundancy. The Internet bandwidth available to the LTSS System is 1000Mbps. Two copper Ethernet ports are provided by the data center, terminating on two separate Cisco 3650 switches for hardware and connectivity diversity.

Two Cisco ASA 5525-X firewalls, configured as an active/standby failover pair, serve as the Internet edge devices. These firewalls secure the LTSS System from the Internet and allow selected inbound and outbound access to the Internet in accordance with the project requirements. Site-to-site IPsec VPN tunnels to third parties and VPN client access enable remote management of the environment.

Local Area Networking

Two Cisco Nexus C9236C switches serve as the "core" switches, or backbone of the infrastructure. These switches are Layer-3 enabled and perform all inter-VLAN routing functions. Two 100Gbps EtherChannel Layer-2 trunks connect the two C9236C switches and four 40Gbps EtherChannel Layer-2 trunks connect the C9236C's to the Nexus C92160YC-X switches in the FlexPod environment. These trunks are used to tag all required VLANs to the virtual systems in use.

All switch-to-switch connections comprise bundles of 40 GB copper twinax Ethernet cabling. All switching hardware is redundant, with redundant cabling in place. Cisco's Rapid Per-VLAN Spanning Tree and Virtual Port Channel protocols are used for fast recovery from LAN switching hardware failure and for the best use of available switching bandwidth.

Two Cisco Catalyst 3650-48TD-L switches are used as multipurpose switches, providing Layer-2 connectivity for WAN and security devices and any LAN devices requiring 1Gbps copper ports. The 3650 switches share VLANs with each other and with the Nexus core switches using 10 GB connections.

F5 Big-IP LTM-4000S balancers load balance incoming IVR traffic to the IVR pool of web servers.

Disaster Recovery Networking

The disaster recovery (DR) data center, located at the Secondary Data Center, closely resembles the network topology of the Production environment. The hardware consists of two (2) Cisco ASA 5525 firewalls, four (4) Nexus 9K C92160YC-X switches, two (2) Cisco Nexus C9236C switches, two (2) Catalyst 3650-48TD-L switches, two (2) Cisco ASR 1001-X routers, one (1) Catalyst 3650-24TD-L switches for management, two (2) F5 BIG-IP LTM-4000S load balancers, and two (2) Cisco UCS 6332 UP Fabric Interconnects. All Layer-2 trunks, VLANs, and connections among devices match Production for easy server replication. Server and Network management VLANs route between sites for ease of management and failover. All communication between the Primary and the Secondary location go through a 1GB Ethernet Circuit provided by the data center. This communication is encrypted using a pair of Cisco ASR 1001-X routers. For additional redundancy, the ASA FWs create a VPN between sites if the circuit or equipment ever fails. Client VPN access to the DR environment for remote management and DR readiness testing is provided by the Cisco ASA firewalls.

20.3.2 EXPANDED to Support LTSS System and Business Growth

In order to meet the demands expected in the five-year timeframe, expansion of compute and storage nodes beyond the BASE-level is required, though overall the architecture layout is expected to remain the same. The overall design remains the same in terms of redundancy and scope for each datacenter. Listed below is the additional hardware required for the EXPANDED LTSS System.

20.3.2.1   Compute nodes

The size of the Primary Data Center is expected to expand as follows:

- The number of chassis is expected to expand from 6 to 9.
- The number of blades is expected to expand from 36 to 54.

The size of the Secondary Data Center is expected to expand as follows:

- The number of chassis is expected to expand from 3 to 5.
- The number of blades is expected to expand from 18 to 30.

20.3.2.2   Storage

The size of the Primary Data Center is expected to expand as follows:

- The number of all-flash disk shelves expected to be required will expand from 12 to 16
- The number of spinning disk shelves expected to be required will expand from 8 to 16

The size of the Secondary Data Center is expected to expand as follows:

- The number of all-flash disk shelves expected to be required will expand from 6 to 8
- The number of spinning disk shelves expected to be required will expand from 4 to 8

20.3.3   LTSS Software

The technical infrastructure design uses all identified software that the LTSS System requires for operation. LTSS compiled code is stored in a managed code repository that is versioned upon new or changed binaries. The compiled code is uploaded to the SFTP server by the Software Development TO Contractor. The server is located within the DMZ in the LTSS Production environment. The Software Development TO Contractor will be provided with credentials to the SFTP server to upload the application code.

20.4   LTSS Architecture and System Diagrams

20.4.1   LTSS Infrastructure Diagrams

LTSS Infrastructure Diagram for BASE-Level Requirements
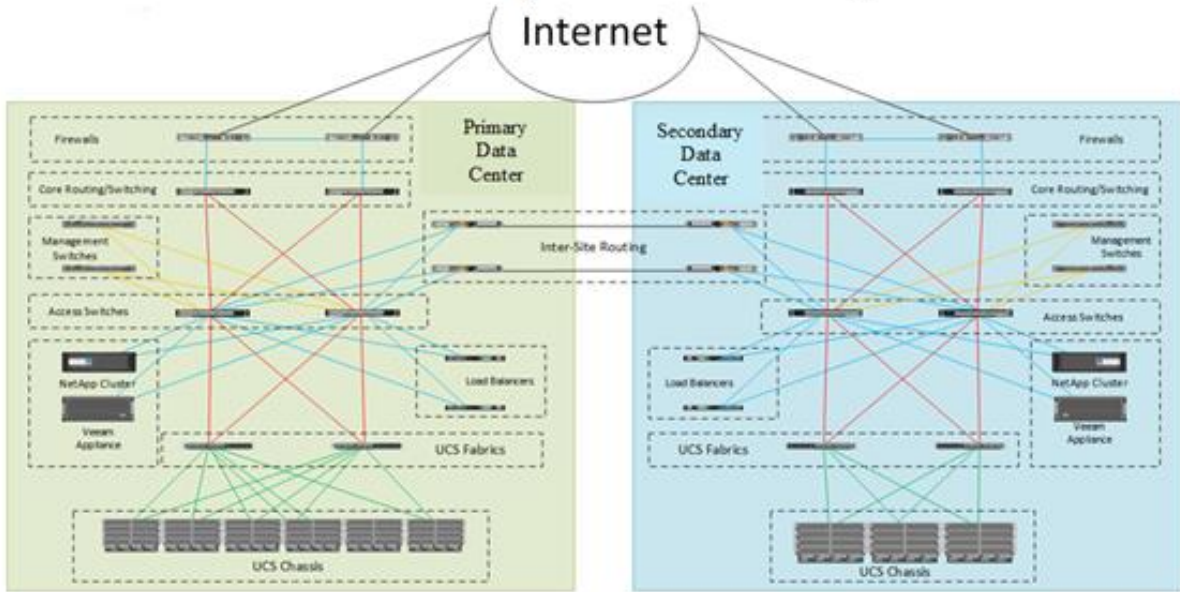
LTSS Infrastructure Diagram for EXPANDED Requirements
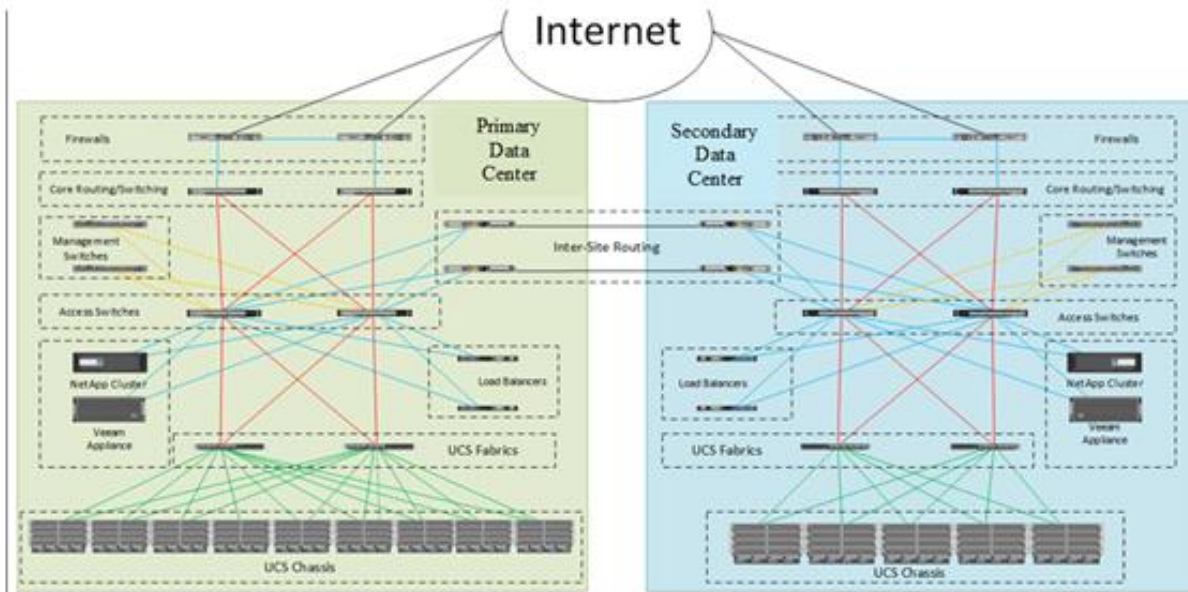
20.4.2   LTSS Hosting Facilities Server Hosting Diagram
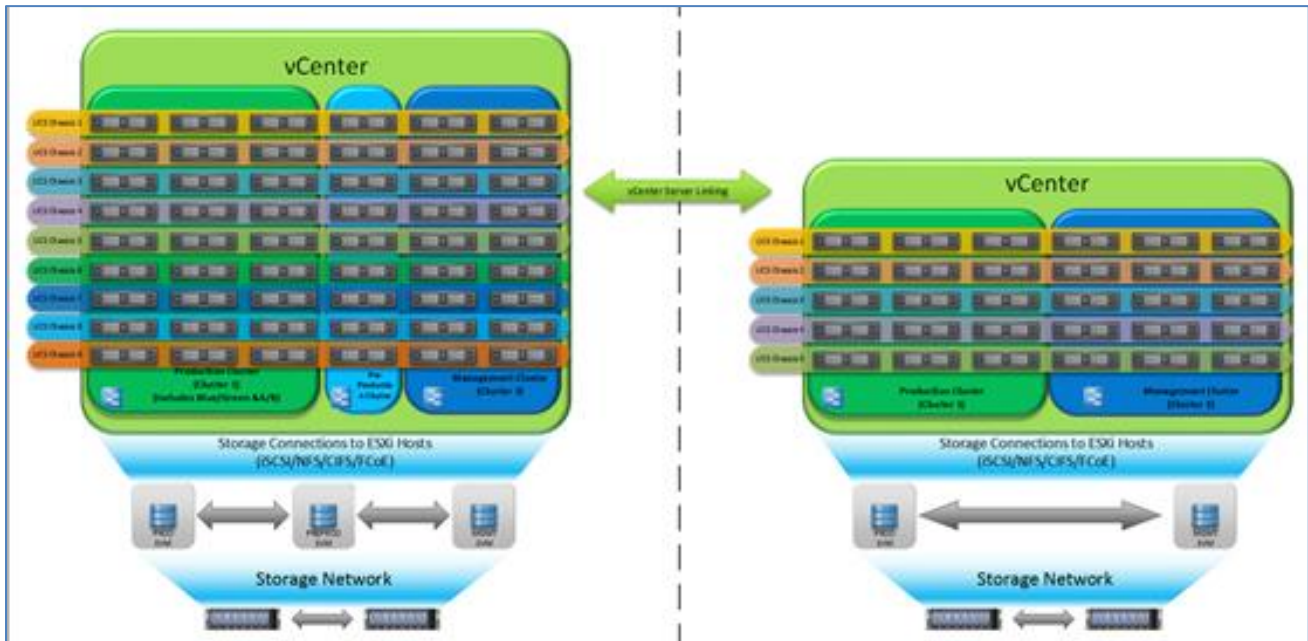
20.4.3   LTSS Application Layer Server Diagram
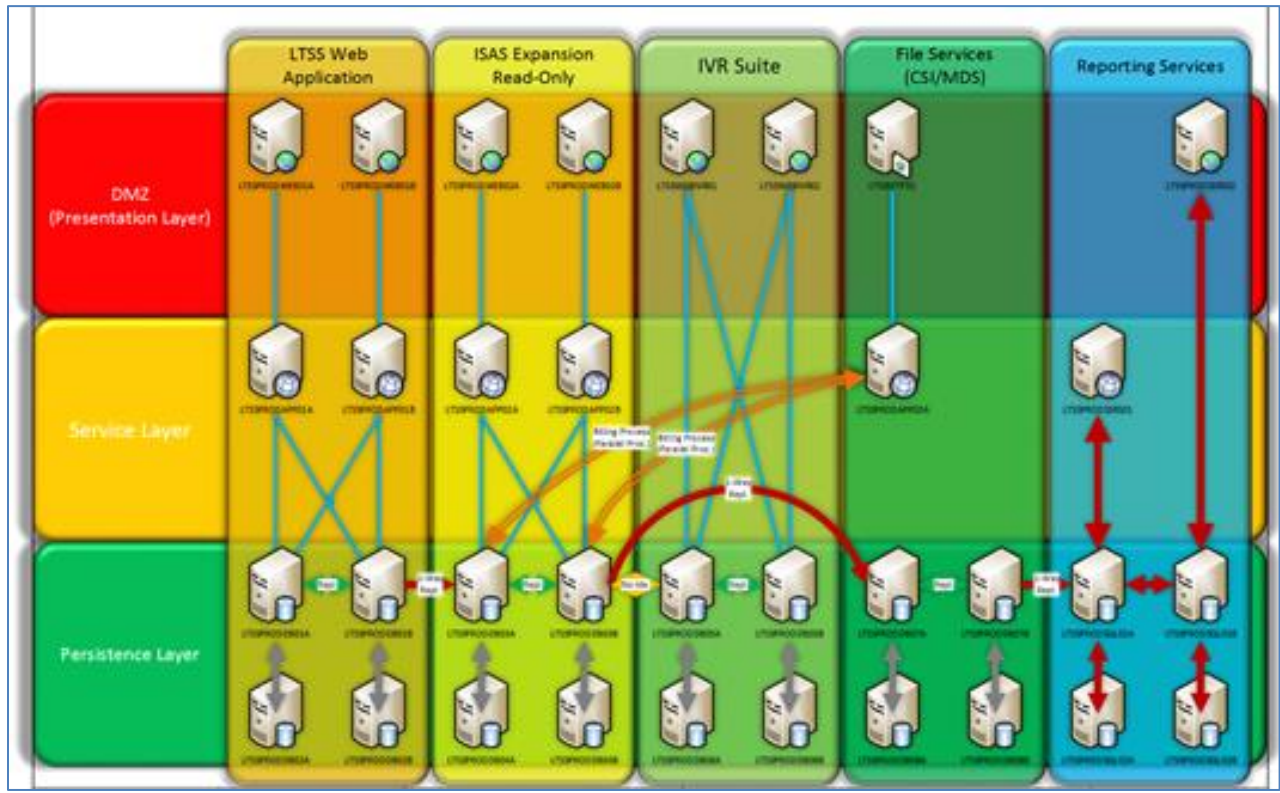
20.4.4   LTSS IVR Server Diagram (Current)

The following ISAS IVR Diagram (20.4.4.1) is the CURRENT solution provided by the current O&M contractor. DHMH is currently developing additional IVR capabilities, including the TEFT IVR (20.4.4.2), which is in the design phase and is planned to be implemented by the TO Contractor during the Start-up Period. DHMH expects the O&M TO Contractor to work collaboratively with the Department, current O&M contractor and the Software Development TO Contractor to expand the IVR to support future DHMH business needs.

20.4.4.1   ISAS IVR Design
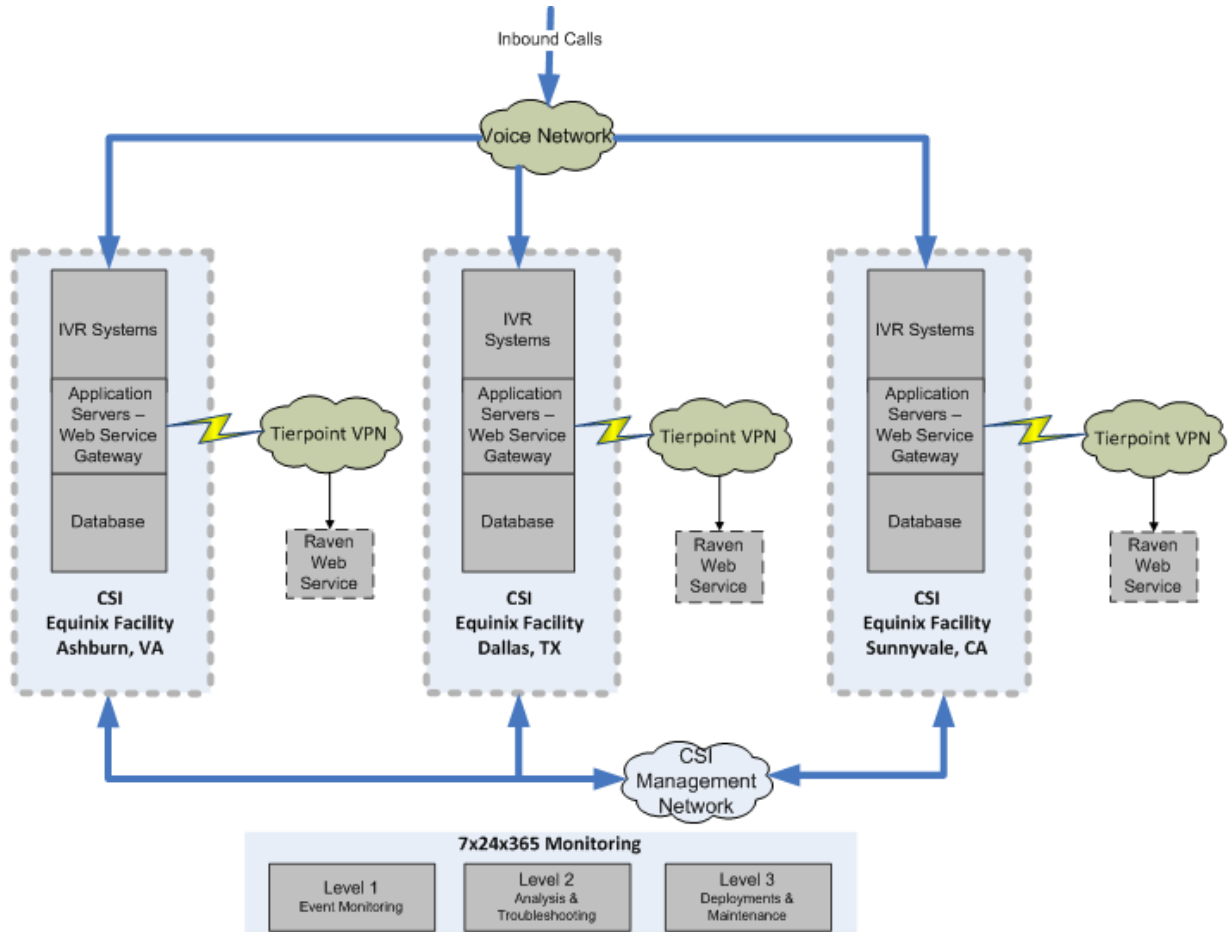
20.4.4.2   TEFT IVR Design

Refer to the attached call flow design document (Attachment 22 TEFT IVR Proposed Call Flow).

20.5   Systems Monitoring

Zenoss and Solarwinds provide enterprise level monitoring for the LTSS System. Both Platforms are IT management systems and monitoring software suites that enable organizations to identify and resolve IT infrastructure problems before they affect critical business processes. An instance within the LTSS architecture monitors the environment locally and reports back to the centralized Service Desk, providing a single pane view of the current state of operations. Monitoring is performed using a VPN connection from the LTSS System to the data center. The monitoring platforms' design empowers the Service Desk to be proactive in their support of DHMH.

20.6   Patch Management

Shavlik provides industry-proven advanced level patch management for the LTSS System. The LTSS System benefits from Shavlik's advanced capabilities, which allow patching of operating systems, Microsoft applications, non-Microsoft applications, including some third party applications.

Every server running within the LTSS System's architecture has a local Shavlik Protect Agent. A VPN connection to the Shavlik enterprise instance allows the centralized Service Desk and system administrators to patch the LTSS Systems proactively. Patching occurs on a monthly maintenance schedule. The Pre-production environment is patched first to fully test approved patches. After testing is complete in the Pre-production environment, the same patches are deployed to the Production environment. Patches are fully tested within Pre-production before deployment to Production. All patches are approved using the change management process.

20.7   Maintenance Scheduling

The LTSS System has standard maintenance on an approved monthly schedule. Systems and devices receive their standard updates and patches during one maintenance window. A second maintenance window is used for application-specific updates, upgrades, code changes, etc.

Off-schedule maintenance windows are provided for emergency releases. The O&M TO Contractor is required to request approval and scheduling from DHMH for emergency maintenance.

20.8   Monitoring

All infrastructure and network equipment is monitored 24x7x365 with SOPs for escalation of issues. The O&M TO Contractor's incident management platform sends automated notifications to selected personnel as an incident is identified, created, updated and resolved.

20.9   Security

The LTSS System provides layered security using a defensive in-depth approach. Security includes physical, network, and system level security. In addition, a secondary security resource provides continual monitoring of logs, alerts, and events.

20.9.1 LTSS Physical Security

Access control readers are placed on the racks to physically secure the servers. This configuration provides audit and control. Only authorized individuals are allowed on the data center floor, managed with the physical security services at the data center. The physical security services include:

- Manned 24 hours a day, 7 days a week, 365 days a year
- Access restricted to authorized TO Contractor personnel and data center employees
    - Client personnel are escorted through the facility either by:
        o Data center employees
        o Authorized TO Contractor personnel
- Axis IP-based interior and exterior surveillance cameras
- Entrance and exit controlled by HID contact-less access cards
- Cabinet access controlled by combination dial system
- Biometric Hand-scan
- Mantraps

20.9.2 LTSS Network Security

20.9.2.1 Firewall Hardware Platform

The Cisco ASA 5525-X firewall is the primary security device. The 5525-X supports up to 5Gbps of stateful inspection throughput, 1Gbps of VPN encryption throughput, up to 5,000 site-to-site VPN peers, and 250 simultaneous remote client VPN users. Two Cisco ASA 5525-X firewalls, configured as an active/standby failover pair, serve as the Internet edge devices. These firewalls secure the LTSS environment from the Internet and allow selected inbound/outbound access to the Internet in accordance with the LTSS System requirements.

20.9.2.2 Firewall Security Zones

Three security zones are initially configured: Outside, DMZ, and Inside:

- Outside Zone
    - This zone connects directly to the Internet. No traffic is allowed from the Internet into the ASA unless explicitly configured within firewall rules. Examples of traffic that are allowed from the Internet include:
        o Incoming connections from the hosted IVR system
        o Traffic from VPN tunnels to third parties
        o Remote access traffic from administrators of the LTSS System.
- DMZ (Demilitarized) Zone
    - Hosts requiring direct incoming access from the Internet are placed in the DMZ. The firewall allows specific Internet traffic into the DMZ to reach the public-facing LTSS servers, and the firewall specifically allows traffic from the public facing servers to reach back-end servers and databases on the inside network.

Traffic is not allowed directly from the Internet to a server on the inside zone.

- Inside Zone
  - This zone comprises all systems and applications in the most secure network behind the firewall. The bulk of the applications, devices, and systems sit in this zone, including:
    - o Database servers
    - o Active directory
    - o Storage
    - o Network management devices
  - Hosts on the inside network have explicit rules allowing them to communicate with the DMZ and allowing required traffic out to the Internet, including web browsing, network time protocol, FTP, and email.

Traffic in different security zones is separated by VLANs. Hosts in VLANs belonging to different security zones are forwarded first to the firewall, then pass through the firewall's security mechanisms to communicate with each other.

20.9.2.3 Network/Security Device Access Control

Access control to Cisco network and security devices are provided with a combination of a RADIUS (Remote Authentication Dial-In User Service) server and user accounts configured in the Active Directory servers in the virtual environment. The network and security devices pass login authentication to a Windows RADIUS server, and the RADIUS server checks the credentials against Active Directory. Password expiration and complexity rules for user accounts are implemented according to best practices. Emergency local accounts are configured on all network and security devices in the event the RADIUS and/or Active Directory servers are unavailable.

20.9.2.4 Virtual Private Networking

Site-to-site IPsec VPN tunnels to third parties and VPN client access for remote management of the environment are provided by the ASA firewalls.

- Site-to-Site VPN
  - The Cisco ASA firewalls provide VPN access to entities requiring permanent "always-on" access to the LTSS environment. Examples include:
    - o VPN tunnel to security operations center
    - o VPN tunnel to network operations center
    - o VPN tunnel to DHMH headquarters
  - These VPN tunnels use IPsec/AES tunnel encryption over the 500Mbps Internet feed provided by the data center.
- Remote Access Client VPN
  - The Cisco ASA firewalls provide client VPN access so individual users can log

in directly into the LTSS environment from a computer. Examples include:

- o Remote user login for day-to-day network and system administration
- o Remote user login for disaster recovery readiness testing
- o Remote user login for auditing purposes
- − This service is provided by Cisco's AnyConnect VPN software, installed directly on the remote computer. The computer then initiates a VPN tunnel to the firewall for secure access into the environment.

20.9.2.5   Intrusion Detection and Intrusion Prevention Services

IDS/IPS functions are provided by Cisco's FirePOWER software, which comes prepackaged with the ASA platform. The IDS/IPS service helps protect the environment from malware attacks and provide reputation- and category-based URL filtering for protection against suspicious web traffic. The ASA is configured to send alerts to the security operations center. The SOC receives threat alarms and recommends corrective actions to the network and security engineers.

20.9.2.6   Logging and Monitoring

All network and security devices are configured to send their SysLog events for storage on a logging server in the environment. The data on the SysLog server are queried by the network operations center (NOC) or SOC or rolled up into event correlation software for analysis.

All network and security devices are configured with Simple Network Management Protocol (SNMP) for monitoring up/down status, network bandwidth, CPU, and memory. SNMP statistics are collected by the SNMP server located in the network operations center. Network alarms Alerts are sent to NOC staff, and statistics are queried and presented in a report format. Where possible, SNMPv3 is used for a higher level of security.

20.9.2.7   Baseline Device Configuration

All network and security devices are configured with industry-standard, best-practice security settings, including:

- Disabling of services not in use
- Password encryption
- Access control lists
- Session idle timers
- Device authentication
- Secure network management

20.9.3   LTSS System Security

All LTSS System servers in the hosted environment have multiple layers of security implemented at a system level. Anti-virus software is installed, monitored, and continually updated on all hosted servers. All systems are scanned and patched with the latest security updates and patches monthly.

All LTSS System-hosted servers are hardened at the operating system level to provide a further layer of security. All user accounts and access are limited at the server level to implement a need-to-have access level approach.

20.9.4   LTSS Security Monitoring

All devices and servers within the LTSS System's hosted environment are continually analyzed and monitored by a separate security resource. The security resource provides continual monitoring of logs, alerts, and events.

20.10   Health Insurance Portability and Accountability Act (HIPAA) Compliance

The LTSS System's hosted environment is secure, with multiple established processes and procedures for continual monitoring of systems and the environment to protect LTSS Systems and data. The LTSS System's hosting environment is NIST 800-53 compliant, HIPAA compliant, and IRS 1075 compliant.

20.11   Database Replication

The RavenDB replicates in the Primary Data Center site to supporting databases and failover databases as defined within the LTSS System's architecture. A secondary replication is implemented between the primary RavenDB server and a hot DR RavenDB server at the Secondary Data Center site. This replication takes place over the replication circuit between the Primary Data Center and Secondary Data Center dedicated to the LTSS System. This replication prevents any dirty database copies or restorations in the event of a disaster recovery of the RavenDB. Replication is configured to meet the SLAs defined within the contract.

20.12   Certificate Expiration Date Tracking

All LTSS System server, device, or system certificates are tracked throughout the duration of the contract. Upon operational hosting of the production environment, an inventory is performed to track all applicable of the LTSS System's certificates and their respective expiration dates. This initial inventory is provided to DHMH in order to have a complete inventory of all LTSS certificates and their dates of expiration. The O&M TO Contractor shall review inventory monthly in order to ensure that all certificates within the LTSS System's architecture are processed for renewal well before a certificate has expired. This proactive approach ensures a higher level of availability for the LTSS System.

20.13   Appendix A – Engineering Assumptions

20.13.1   Compute Infrastructure

The following assumptions were made for the purpose of engineering the compute resources design:

ID	Compute Component Level	Assumption
1	Site	Both sites (Primary and Secondary Data Centers) will need capacity to host the entire LTSS System infrastructure in the event of a disaster, or outage affecting the other site.
2	Environments/ Enclaves	The environments will include a Production and Management environment for both sites. And a Pre-production environment in the Primary Data Center.
3	Environments/ Enclaves	The Pre-production environment will need to mirror the Production environment in all aspects.
4	Environments/ Enclaves	The Pre-production environment needs to be a copy of the Production environment that is accessible via Network Address Translation and separated via different Distributed vSwitches
5	Compute CPU Resources	The compute CPU resource is based on the projected transaction amounts.
6	Compute Memory Resources	The compute memory resource is based on the projected transaction amounts.
7	Hosts	The number of hosts is required to ensure high availability and to scale out resources for distribution across the infrastructure.
8	Clusters	The different environments require separation at the cluster level to prevent migrating Pre-production data to Production.
9	HA/DRS	The high availability is required to accommodate hardware failure on any one component of the infrastructure.

20.13.2   Storage Infrastructure

The following assumptions were made for the purpose of engineering the storage infrastructure design:

ID	Storage Component	Assumption
1	Connectivity	The storage system will only be used by the VMware Hypervisor and ESXi Hosts via NFS.
2	Latency	The latency times will need to be less than or equal to one millisecond to prevent the storage from reducing system performance.
3	Load Distribution	The application servers are able to distribute load across more than one server to maximize performance.

ID	Storage Component	Assumption
4	High Availability	The system will need to accommodate a failure of at least two hardware components at any given time while maintaining availability.
5	Environments	The system must have a separate storage environment for pre-production.
6	Encryption	The system will not need to provide encryption for data at rest.
7	Replication	The system will not need to replicate data between sites

20.13.3   Backup Infrastructure

The following assumptions were made for the purpose of engineering the backup infrastructure design:

ID	Backups Component	Assumption
1	Encryption	The system will not need to encrypt data at rest.
2	Speed	The speed of the backups will need be fast enough to complete backups within a determined by amount of time that is allotted specifically for backups each night.
3	Restores	The system must be able to restore files, virtual machines, application data, and storage snapshots.
4	Replication	The backups will need to be replicated to the adjacent site for DR purposes in the event of a disaster.

20.13.4   Application Infrastructure

The following assumptions were made for the purpose of engineering the application infrastructure design:

ID	Application Component	Assumption
1	Presentation Layer	The application presentation or web servers are scaled out in a linear manner in accordance with the usage projections.
2	Presentation Layer	The application presentation layer is developed to scale out across multiple servers.
3	Service Layer	The service layer or application servers are scaled out in a linear manner.
4	Service Layer	The application service layer servers will scale out across multiple servers and stacks
5	Database Layer	The database layer or database servers are scaled out in a linear manner in accordance with the usage projections.
6	Database Layer	The application database layer servers will scale out across multiple servers.
7	Database Layer	The database layer will perform replication of application data between application stacks and sites.

20.14   Appendix B – Design Document Diagrams

20.14.1   LTSS WAN Topology Diagram
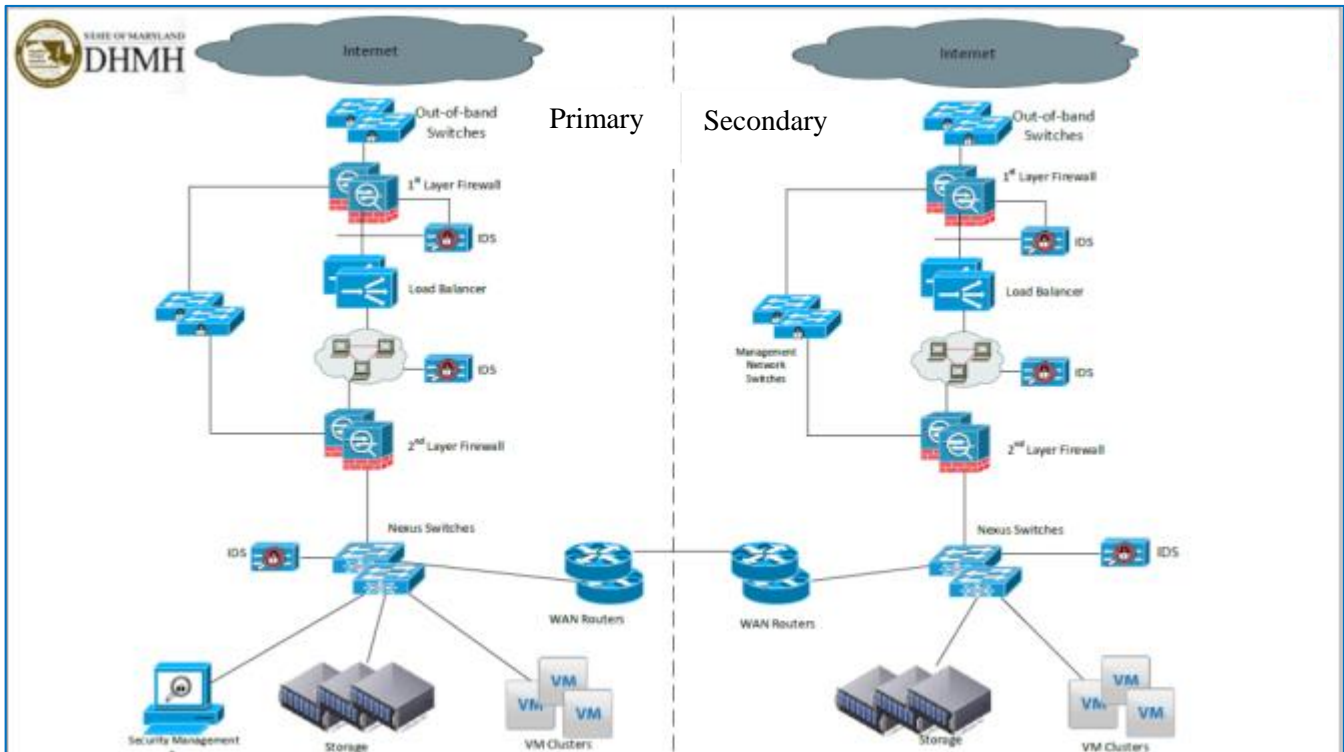
20.14.2   LTSS Network Fault Tolerance Diagram
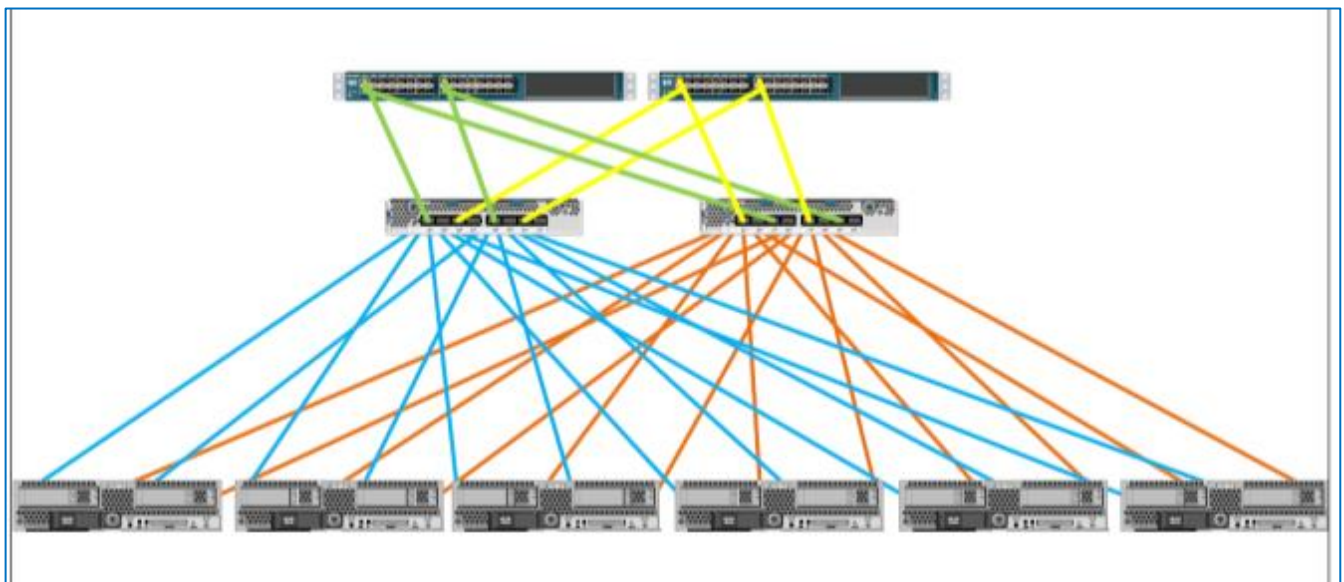
20.14.3   LTSS Virtual NIC Uplink Policy Diagram
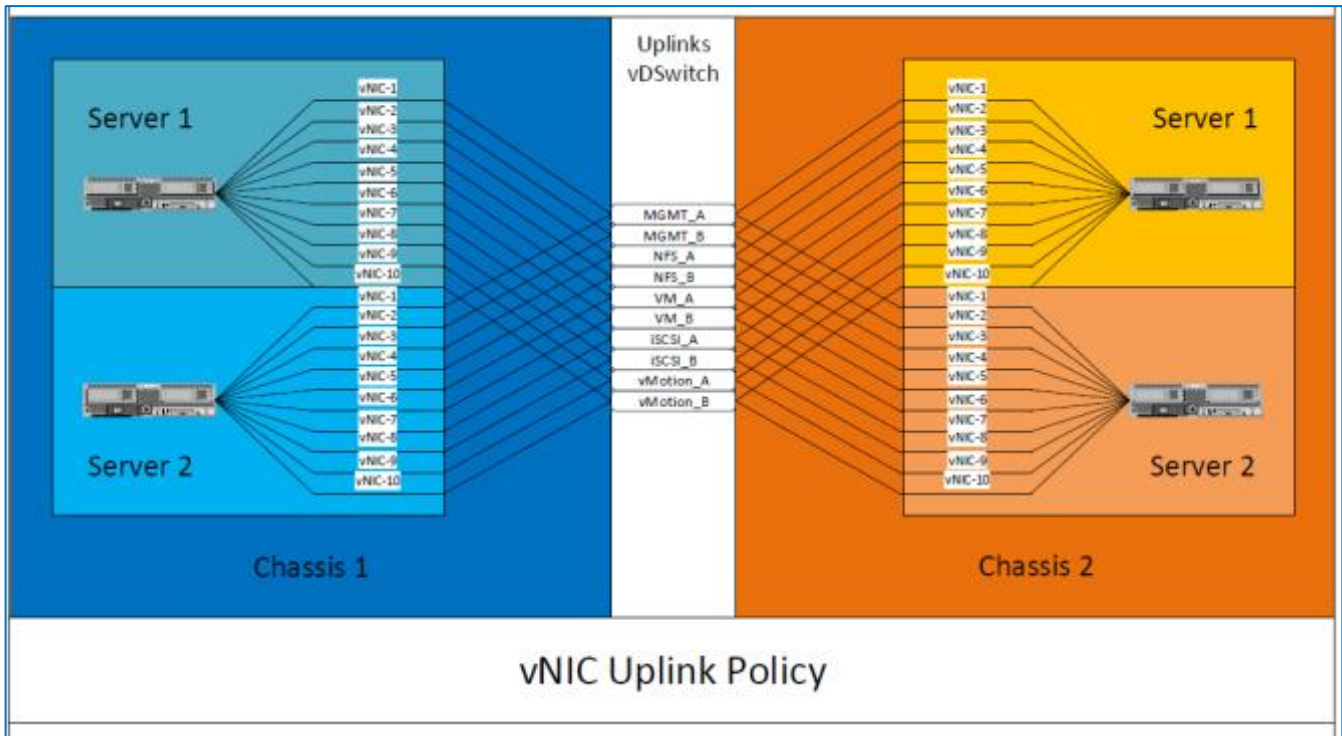
20.15 Appendix C – LTSS Server Listing

20.15.1   Primary Data Center

Primary Data Center					
ID	BASE or EXPANDED	Environment	Layer	Role	Application
1	BASE	Prod Green	Presentation	WEB	LTSS/DDA
		Prod Green	Presentation	WEB	LTSS/DDA
		Prod Green	Presentation	WEB	LTSS/DDA
		Prod Green	Presentation	WEB	LTSS/DDA
2	EXPANDED	Prod Green	Presentation	WEB	LTSS/DDA
		Prod Green	Presentation	WEB	LTSS/DDA
3	BASE	Prod Green	Presentation	WEB	P.P.
		Prod Green	Presentation	WEB	P.P.
4	BASE	Prod Green	Presentation	WEB	SSRS
		Prod Green	Presentation	WEB	SSRS
		Prod Green	Presentation	WEB	SSRS
		Prod Green	Presentation	APP	SSRS-Ad hoc-Legacy
		Prod Green	Presentation	APP	SSRS-Ad hoc-Legacy
5	BASE	Prod Green	Presentation	WEB	SSO
		Prod Green	Presentation	WEB	SSO
6	BASE	Prod Green	Service	APP	LTSS/DDA
		Prod Green	Service	APP	LTSS/DDA
		Prod Green	Service	APP	LTSS/DDA
		Prod Green	Service	APP	LTSS/DDA
7	EXPANDED	Prod Green	Service	APP	LTSS/DDA
		Prod Green	Service	APP	LTSS/DDA
8	BASE	Prod Green	Service	APP	P.P.
		Prod Green	Service	APP	P.P.
		Prod Green	Service	APP	IVR
		Prod Green	Service	APP	IVR
		Prod Green	Service	BATCH	BILLING
		Prod Green	Service	BATCH	BILLING
9	EXPANDED	Prod Green	Service	BATCH	BILLING
		Prod Green	Service	BATCH	BILLING
10	BASE	Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
11	EXPANDED	Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert

ID	BASE or EXPANDED	Environment	Layer	Role	Application
Primary Data Center						

ID	BASE or EXPANDED	Environment	Layer	Role	Application
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
12	BASE	Prod Green	Persistence	RavenDB	IVR & Billing
		Prod Green	Persistence	RavenDB	IVR & Billing
13	EXPANDED	Prod Green	Persistence	RavenDB	IVR & Billing
		Prod Green	Persistence	RavenDB	IVR & Billing
14	BASE	Prod Green	Persistence	RavenDB	Raven ETL DB
		Prod Green	Persistence	RavenDB	Raven ETL DB
15	EXPANDED	Prod Green	Persistence	RavenDB	Raven ETL DB
		Prod Green	Persistence	RavenDB	Raven ETL DB
16	BASE	Prod Green	Persistence	SQL	SQL AG Group 1
		Prod Green	Persistence	SQL	SQL AG Group 1
17	EXPANDED	Prod Green	Persistence	SQL	SQL AG Group 1
		Prod Green	Persistence	SQL	SQL AG Group 1
		Prod Green	Persistence	SQL	SQL AG Group 1
		Prod Green	Persistence	SQL	SQL AG Group 1
18	BASE	Prod Green	Persistence	SQL	SQL AG Group 2
		Prod Green	Persistence	SQL	SQL AG Group 2
19	EXPANDED	Prod Green	Persistence	SQL	SQL AG Group 2
		Prod Green	Persistence	SQL	SQL AG Group 2
20	BASE	Prod Blue	Presentation	WEB	LTSS/DDA
		Prod Blue	Presentation	WEB	LTSS/DDA
		Prod Blue	Presentation	WEB	LTSS/DDA
		Prod Blue	Presentation	WEB	LTSS/DDA
21	EXPANDED	Prod Blue	Presentation	WEB	LTSS/DDA
		Prod Blue	Presentation	WEB	LTSS/DDA
22	BASE	Prod Blue	Presentation	WEB	P.P.
		Prod Blue	Presentation	WEB	P.P.
23	BASE	Prod Blue	Presentation	WEB	SSRS
		Prod Blue	Presentation	WEB	SSRS
		Prod Blue	Presentation	WEB	SSRS
24	BASE	Prod Blue	Presentation	APP	SSRS-Ad hoc-Legacy
		Prod Blue	Presentation	APP	SSRS-Ad hoc-Legacy
25	BASE	Prod Blue	Presentation	WEB	SSO
		Prod Blue	Presentation	WEB	SSO
26	BASE	Prod Blue	Service	APP	LTSS/DDA
		Prod Blue	Service	APP	LTSS/DDA
		Prod Blue	Service	APP	LTSS/DDA
		Prod Blue	Service	APP	LTSS/DDA
27	EXPANDED	Prod Blue	Service	APP	LTSS/DDA

ID	BASE or EXPANDED	Environment	Layer	Role	Application
Primary Data Center				
		Prod Blue	Service	APP	LTSS/DDA
28	BASE	Prod Blue	Service	APP	P.P.
		Prod Blue	Service	APP	P.P.
29	BASE	Prod Blue	Service	APP	IVR
		Prod Blue	Service	APP	IVR
30	BASE	Prod Blue	Service	BATCH	BILLING
		Prod Blue	Service	BATCH	BILLING
31	EXPANDED	Prod Blue	Service	BATCH	BILLING
		Prod Blue	Service	BATCH	BILLING
32	BASE	Prod Blue	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Blue	Persistence	RavenDB	LTSS/Audit/File/Alert
33	EXPANDED	Prod Blue	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Blue	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Blue	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Blue	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Blue	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Blue	Persistence	RavenDB	LTSS/Audit/File/Alert
34	BASE	Prod Blue	Persistence	RavenDB	IVR & Billing
		Prod Blue	Persistence	RavenDB	IVR & Billing
35	EXPANDED	Prod Blue	Persistence	RavenDB	IVR & Billing
		Prod Blue	Persistence	RavenDB	IVR & Billing
36	BASE	Prod Blue	Persistence	RavenDB	Raven ETL DB
		Prod Blue	Persistence	RavenDB	Raven ETL DB
37	EXPANDED	Prod Blue	Persistence	RavenDB	Raven ETL DB
		Prod Blue	Persistence	RavenDB	Raven ETL DB
38	BASE	Prod Blue	Persistence	SQL	SQL AG Group 1
		Prod Blue	Persistence	SQL	SQL AG Group 1
39	EXPANDED	Prod Blue	Persistence	SQL	SQL AG Group 1
		Prod Blue	Persistence	SQL	SQL AG Group 1
		Prod Blue	Persistence	SQL	SQL AG Group 1
		Prod Blue	Persistence	SQL	SQL AG Group 1
40	BASE	Prod Blue	Persistence	SQL	SQL AG Group 2
		Prod Blue	Persistence	SQL	SQL AG Group 2
41	EXPANDED	Prod Blue	Persistence	SQL	SQL AG Group 2
		Prod Blue	Persistence	SQL	SQL AG Group 2
42	BASE	Pre-prod	Presentation	WEB	LTSS/DDA
43	BASE	Pre-prod	Presentation	WEB	P.P.
44	BASE	Pre-prod	Presentation	WEB	SSRS
		Pre-prod	Presentation	WEB	SSRS

		Primary Data Center			
ID	BASE or EXPANDED	Environment	Layer	Role	Application
45	BASE	Pre-prod	Presentation	APP	SSRS-Ad hoc-Legacy
46	BASE	Pre-prod	Presentation	WEB	SSO
47	BASE	Pre-prod	Service	APP	LTSS/DDA
48	BASE	Pre-prod	Service	APP	P.P.
49	BASE	Pre-prod	Service	APP	IVR
50	BASE	Pre-prod	Service	BATCH	BILLING
51	BASE	Pre-prod	Persistence	RavenDB	LTSS/Audit/File/Alert
52	BASE	Pre-prod	Persistence	RavenDB	IVR & Billing
53	BASE	Pre-prod	Persistence	RavenDB	Raven ETL DB
54	BASE	Pre-prod	Persistence	SQL	SQL AG Group 1
55	BASE	Pre-prod	Persistence	SQL	SQL AG Group 2
56	BASE	Management	Active Directory	AD-FR	AD
		Management	Active Directory	AD-FR	AD
57	BASE	Management	Active Directory	AD-PROD	AD
		Management	Active Directory	AD-PROD	AD
58	BASE	Management	Active Directory	AD-PREP	AD
		Management	Active Directory	AD-PREP	AD
59	BASE	Management	Monitoring Tools	NAGIOS	MONITORING
		Management	Monitoring Tools	NAGIOS	MONITORING
60	BASE	Management	Monitoring Tools	SolarWinds	MONITORING
		Management	Monitoring Tools	SolarWinds	MONITORING
61	BASE	Management	Monitoring Tools	Zenoss	MONITORING
		Management	Monitoring Tools	Zenoss	MONITORING
62	BASE	Management	Backups	Veeam	BACKUPS
		Management	Backups	Veeam	BACKUPS
63	BASE	Management	Storage	NetAppOCUM	STORAGE-MGMT
64	BASE	Management	Storage	NetAppOCPM	STORAGE-MGMT
65	BASE	Management	Storage	NetAppOCMC	STORAGE-MGMT
		Management	Storage	NetAppOCMC	STORAGE-MGMT
66	BASE	Management	Storage	NetAppVSA	STORAGE-MGMT

			Primary Data Center		
ID	**BASE or EXPANDED**	**Environment**	**Layer**	**Role**	**Application**
67	BASE	Management	Cisco UCS	Cisco One	UCS-MGMT
68	BASE	Management	Cisco UCS	Cisco UCS Dir	UCS-MGMT
69	BASE	Management	Cisco UCS	Cisco ACI	UCS-MGMT
70	BASE	Management	Cisco UCS	Cisco UCS Mgr	UCS-MGMT
71	BASE	Management	Cisco UCS	Cisco UCS Mgr	UCS-MGMT
72	BASE	Management	SMTP	SMTP	Mail Sender
		Management	SMTP	SMTP	Mail Sender
73	BASE	Management	File Services	Secure FTP	Secure File transfer
		Management	File Services	Secure FTP	Secure File transfer
74	BASE	Management	File Services	FTP	Insecure FTP
		Management	File Services	FTP	Insecure FTP
75	BASE	Management	Configuration Management	Puppet	Config Mgmt
		Management	Configuration Management	Puppet	Config Mgmt
		Management	Configuration Management	Puppet	Config Mgmt
		Management	Configuration Management	Puppet	Config Mgmt
		Management	Configuration Management	Puppet	Config Mgmt
76	BASE	Management	Management Servers	Management	General Management
		Management	Management Servers	Management	General Management
		Management	Management Servers	Management	General Management
		Management	Management Servers	Management	General Management
		Management	Management Servers	Management	General Management
		Management	Management Servers	Management	General Management
		Management	Management Servers	Management	General Management
77	BASE	Management	Patching	Shavlik	Patching
		Management	Patching	Shavlik	Patching
78	BASE	Management	Vmware	vCenter	VM Mgmt
79	BASE	Management	Vmware	VC Orchestrator	VM Mgmt
80	BASE	Management	Vmware	vRealize	VM Mgmt

Primary Data Center					
ID	**BASE or EXPANDED**	**Environment**	**Layer**	**Role**	**Application**
81	BASE	Management	Vmware	vCloud Ops	VM Mgmt
82	BASE	Management	AlienVault	AlienVault Server	Security
		Management	AlienVault	AlienVault Sensor	Security
83	BASE	Management	AlienVault	AlienVault Database	Security
84	BASE	Management	IDS	DMZ IDS	Security
85	BASE	Management	IDS	MGMT IDS	Security
86	BASE	Management	IDS	Internal IDS	Security
87	BASE	Management	Vipre	AntiVirus	Security

20.15.1   Secondary Data Center

Secondary Data Center					
ID	**BASE / EXPANDED**	**Environment**	**Layer**	**Role**	**Application**
1	BASE	Prod Green	Presentation	WEB	LTSS/DDA
		Prod Green	Presentation	WEB	LTSS/DDA
		Prod Green	Presentation	WEB	LTSS/DDA
		Prod Green	Presentation	WEB	LTSS/DDA
2	EXPANDED	Prod Green	Presentation	WEB	LTSS/DDA
		Prod Green	Presentation	WEB	LTSS/DDA
3	BASE	Prod Green	Presentation	WEB	P.P.
		Prod Green	Presentation	WEB	P.P.
4	BASE	Prod Green	Presentation	WEB	SSRS
		Prod Green	Presentation	WEB	SSRS
		Prod Green	Presentation	WEB	SSRS
5	BASE	Prod Green	Presentation	APP	SSRS-Ad hoc-Legacy
		Prod Green	Presentation	APP	SSRS-Ad hoc-Legacy
6	BASE	Prod Green	Presentation	WEB	SSO
		Prod Green	Presentation	WEB	SSO
7	BASE	Prod Green	Service	APP	LTSS/DDA
		Prod Green	Service	APP	LTSS/DDA
		Prod Green	Service	APP	LTSS/DDA
		Prod Green	Service	APP	LTSS/DDA
8	EXPANDED	Prod Green	Service	APP	LTSS/DDA
		Prod Green	Service	APP	LTSS/DDA
9	BASE	Prod Green	Service	APP	P.P.
		Prod Green	Service	APP	P.P.
10	BASE	Prod Green	Service	APP	IVR
		Prod Green	Service	APP	IVR

ID	BASE / EXPANDED	Environment	Layer	Role	Application
Secondary Data Center					
11	BASE	Prod Green	Service	BATCH	BILLING
		Prod Green	Service	BATCH	BILLING
12	EXPANDED	Prod Green	Service	BATCH	BILLING
		Prod Green	Service	BATCH	BILLING
13	BASE	Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
14	EXPANDED	Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
		Prod Green	Persistence	RavenDB	LTSS/Audit/File/Alert
15	BASE	Prod Green	Persistence	RavenDB	IVR & Billing
		Prod Green	Persistence	RavenDB	IVR & Billing
16	EXPANDED	Prod Green	Persistence	RavenDB	IVR & Billing
		Prod Green	Persistence	RavenDB	IVR & Billing
17	BASE	Prod Green	Persistence	RavenDB	Raven ETL DB
		Prod Green	Persistence	RavenDB	Raven ETL DB
18	EXPANDED	Prod Green	Persistence	RavenDB	Raven ETL DB
		Prod Green	Persistence	RavenDB	Raven ETL DB
19	BASE	Prod Green	Persistence	SQL	SQL AG Group 1
		Prod Green	Persistence	SQL	SQL AG Group 1
20	EXPANDED	Prod Green	Persistence	SQL	SQL AG Group 1
		Prod Green	Persistence	SQL	SQL AG Group 1
		Prod Green	Persistence	SQL	SQL AG Group 1
		Prod Green	Persistence	SQL	SQL AG Group 1
21	BASE	Prod Green	Persistence	SQL	SQL AG Group 2
		Prod Green	Persistence	SQL	SQL AG Group 2
22	EXPANDED	Prod Green	Persistence	SQL	SQL AG Group 2
		Prod Green	Persistence	SQL	SQL AG Group 2
23	BASE	Management	Active Directory	AD-FR	AD
		Management	Active Directory	AD-FR	AD
24	BASE	Management	Active Directory	AD-PROD	AD
		Management	Active Directory	AD-PROD	AD
25	BASE	Management	Monitoring Tools	NAGIOS	MONITORING

ID	BASE / EXPANDED	Environment	Layer	Role	Application
		Secondary Data Center			
		Management	Monitoring Tools	NAGIOS	MONITORING
26	BASE	Management	Monitoring Tools	SolarWinds	MONITORING
		Management	Monitoring Tools	SolarWinds	MONITORING
27	BASE	Management	Monitoring Tools	Zenoss	MONITORING
		Management	Monitoring Tools	Zenoss	MONITORING
28	BASE	Management	Backups	Veeam	BACKUPS
		Management	Backups	Veeam	BACKUPS
29	BASE	Management	Storage	NetAppOCUM	STORAGE-MGMT
30	BASE	Management	Storage	NetAppOCPM	STORAGE-MGMT
31	BASE	Management	Storage	NetAppOCMC	STORAGE-MGMT
32	BASE	Management	Storage	NetAppVSA	STORAGE-MGMT
33	BASE	Management	Cisco UCS	Cisco One	UCS-MGMT
34	BASE	Management	Cisco UCS	Cisco UCS Dir	UCS-MGMT
35	BASE	Management	Cisco UCS	Cisco ACI	UCS-MGMT
36	BASE	Management	Cisco UCS	Cisco UCS Mgr	UCS-MGMT
37	BASE	Management	Cisco UCS	Cisco UCS Mgr	UCS-MGMT
38	BASE	Management	SMTP	SMTP	Mail Sender
39	BASE	Management	File Services	Secure FTP	Secure File transfer
40	BASE	Management	File Services	FTP	Insecure FTP
41	BASE	Management	Configuration Management	Puppet	Config Mgmt
		Management	Configuration Management	Puppet	Config Mgmt
		Management	Configuration Management	Puppet	Config Mgmt
42	BASE	Management	Management Servers	Management	General Management
		Management	Management Servers	Management	General Management
		Management	Management Servers	Management	General Management
		Management	Management Servers	Management	General Management
43	EXPANDED	Management	Management Servers	Management	General Management
44	BASE	Management	Patching	Shavlik	Patching

		Secondary Data Center			
ID	**BASE / EXPANDED**	**Environment**	**Layer**	**Role**	**Application**
45	BASE	Management	Vmware	vCenter	VM Mgmt
46	BASE	Management	Vmware	VC Orchestrator	VM Mgmt
47	BASE	Management	Vmware	vRealize	VM Mgmt
48	BASE	Management	Vmware	vCloud Ops	VM Mgmt
49	BASE	Management	AlienVault	AlienVault Server	Security
50	BASE	Management	AlienVault	AlienVault Sensor	Security
51	BASE	Management	AlienVault	AlienVault Database	Security
52	BASE	Management	IDS	DMZ IDS	Security
53	BASE	Management	IDS	MGMT IDS	Security
54	BASE	Management	IDS	Internal IDS	Security
55	BASE	Management	Vipre	AntiVirus	Security

20.16 Appendix D – Itemized Component List

Compute, Storage and software components for environment configuration and environment maintenance	
Category	**Minimum Requirements**
Compute Node for Flexpod systems	Low Core / Socket density - Minimums(E5v4,2.3 GHz,Sockets 2,Cores 28, Threads 56, CPU cache 70mb,Max RAM 1,536GB)
Compute Node for Flexpod systems	Moderate Core / Socket density - Minimums(E7v4,2.2 GHz,Sockets 2,Cores 48, Threads 96, CPU cache 120mb,Max RAM 1,536GB)
Compute Node for Flexpod systems	High Core / Socket density - Minimums(E5v4,2.2 GHz,Sockets 4,Cores 88, Threads 176, CPU cache 220mb,Max RAM 2,304GB)
Compute Node for Flexpod systems	High Speed Processor / mid cores - Minimums(E7v2,3.4 GHz,Sockets 4,Cores 24, Threads 48, CPU cache 150mb,Max RAM 6,144GB)
Memory for Flexpod systems	64 GB Stick High Speed - Min. Speed: 2400MHz
Memory for Flexpod systems	32 GB Stick High Speed - Min. Speed: 2400MHz
Memory for Flexpod systems	16 GB Stick High Speed - Min. Speed: 2400MHz
Memory for Flexpod systems	8 GB Stick High Speed - Min. Speed: 2400MHz
Memory for Flexpod systems	64 GB Stick Moderate Speed- Min. Speed: 1600MHz
Memory for Flexpod systems	32 GB Stick Moderate Speed- Min. Speed: 1600MHz
Memory for Flexpod systems	16 GB Stick Moderate Speed- Min. Speed: 1600MHz
Memory for Flexpod systems	8 GB Stick Moderate Speed- Min. Speed: 1600MHz
Memory for Flexpod systems	64 GB Stick Low Speed - Min. Speed: 1066MHz
Memory for Flexpod systems	32 GB Stick Low Speed - Min. Speed: 1066MHz
Memory for Flexpod systems	16 GB Stick Low Speed - Min. Speed: 1066MHz
Memory for Flexpod systems	8 GB Stick Low Speed - Min. Speed: 1066MHz
Standalone Rackmount server/computer non-blade	Web server w/ SFF Drive support - Minimums(E5-2600v4,2.3 GHz,Sockets 2,Cores 28, Threads 56, CPU cache 70mb,Max RAM 128GB)
Standalone Rackmount server/computer non-blade	Application Server w/ SFF Drive support - Minimums(E5-2600v4,2.4 GHz,Sockets 2,Cores 44, Threads 88, CPU cache 110mb,Max RAM 256GB)
Standalone Rackmount server/computer non-blade	Database Server w/ SFF Drive support - Minimums(E5-8000v4,2.2 GHz,Sockets 4,Cores 96, Threads 192, CPU cache 240mb,Max RAM 4,096GB)
Standalone Rackmount server/computer non-blade	Analytics Server w/ SFF Drive support - Minimums(E5-4000v4,2.1 GHz,Sockets 4,Cores 16, Threads 64, CPU cache 160mb,Max RAM 2,048GB)
Standalone Rackmount server/computer non-blade	Web server w/ LFF Drives support - Minimums(E5-2600v4,2.3 GHz,Sockets 2,Cores 28, Threads 56, CPU cache 70mb,Max RAM 128GB)

Compute, Storage and software components for environment configuration and environment maintenance	
Category	**Minimum Requirements**
Standalone Rackmount server/computer non-blade	Application Server w/ LFF Drives support - Minimums(E5-2600v4,2.4 GHz,Sockets 2,Cores 44, Threads 88, CPU cache 110mb,Max RAM 256GB)
Standalone Rackmount server/computer non-blade	Database Server w/ LFF Drives support - Minimums(E5-8000v4,2.2 GHz,Sockets 4,Cores 96, Threads 192, CPU cache 240mb,Max RAM 4,096GB)
Standalone Rackmount server/computer non-blade	Analytics Server w/ LFF Drives support - Minimums(E5-4000v4,2.1 GHz,Sockets 4,Cores 16, Threads 64, CPU cache 160mb,Max RAM 2,048GB)
Memory for Standalone Rackmount systems	64 GB Stick High Speed - Min. Speed: 2400MHz
Memory for Standalone Rackmount systems	32 GB Stick High Speed - Min. Speed: 2400MHz
Memory for Standalone Rackmount systems	16 GB Stick High Speed - Min. Speed: 2400MHz
Memory for Standalone Rackmount systems	8 GB Stick High Speed - Min. Speed: 2400MHz
Memory for Standalone Rackmount systems	64 GB Stick Moderate Speed - Min. Speed: 2133MHz
Memory for Standalone Rackmount systems	32 GB Stick Moderate Speed - Min. Speed: 2133MHz
Memory for Standalone Rackmount systems	16 GB Stick Moderate Speed - Min. Speed: 2133MHz
Memory for Standalone Rackmount systems	8 GB Stick Moderate Speed - Min. Speed: 2133MHz
Internal Storage for Standalone Rackmount systems	(7.2K RPM) RAID 1/0 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(10K RPM) RAID 1/0 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(15K RPM) RAID 1/0 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(SSD) RAID 1/0 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(7.2K RPM) RAID 5 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(10K RPM) RAID 5 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(15K RPM) RAID 5 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(SSD) RAID 5 - Per 100GB Increment of UUS

Compute, Storage and software components for environment configuration and environment maintenance	
Category	**Minimum Requirements**
Internal Storage for Standalone Rackmount systems	(7.2K RPM) RAID 6 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(10K RPM) RAID 6 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(15K RPM) RAID 6 - Per 100GB Increment of UUS
Internal Storage for Standalone Rackmount systems	(SSD) RAID 6 - Per 100GB Increment of UUS
SAN Storage	(7.2K RPM) RAID 1/0 - Per 100GB Increment of UUS
SAN Storage	(10K RPM) RAID 1/0 - Per 100GB Increment of UUS
SAN Storage	(15K RPM) RAID 1/0 - Per 100GB Increment of UUS
SAN Storage	(SSD) RAID 1/0 - Per 100GB Increment of UUS
SAN Storage	(7.2K RPM) RAID 5 - Per 100GB Increment of UUS
SAN Storage	(10K RPM) RAID 5 - Per 100GB Increment of UUS
SAN Storage	(15K RPM) RAID 5 - Per 100GB Increment of UUS
SAN Storage	(SSD) RAID 5 - Per 100GB Increment of UUS
SAN Storage	(7.2K RPM) RAID 6 - Per 100GB Increment of UUS
SAN Storage	(10K RPM) RAID 6 - Per 100GB Increment of UUS
SAN Storage	(15K RPM) RAID 6 - Per 100GB Increment of UUS
SAN Storage	(SSD) RAID 6 - Per 100GB Increment of UUS
Bandwidth Upgrades	3 Mbit Internet
Bandwidth Upgrades	10 Mbit Internet
Bandwidth Upgrades	50 Mbit Internet
Bandwidth Upgrades	100 Mbit Internet
Bandwidth Upgrades	1 Gbit Internet
Bandwidth Upgrades	2 Gbit Internet
Bandwidth Upgrades	10 Gbit Internet
Bandwidth Upgrades	3 Mbit InterCenter
Bandwidth Upgrades	10 Mbit InterCenter
Bandwidth Upgrades	50 Mbit InterCenter
Bandwidth Upgrades	100 Mbit InterCenter
Bandwidth Upgrades	1 Gbit InterCenter
Bandwidth Upgrades	2 Gbit InterCenter
Bandwidth Upgrades	10 Gbit InterCenter
Bandwidth Upgrades	1 Gbit LAN
Bandwidth Upgrades	2 Gbit LAN
Bandwidth Upgrades	10 Gbit LAN
Software and Licensing	Windows Server Operating Systems - Datacenter Edition per Core
Software and Licensing	Windows Server Operating Systems - Standard Edition per Core

Compute, Storage and software components for environment configuration and environment maintenance	
Category	**Minimum Requirements**
Software and Licensing	Windows Server Operating Systems User CAL
Software and Licensing	Windows Server Operating Systems Device CAL
Software and Licensing	Windows Server Operating Systems External Connecters License
Software and Licensing	Microsoft SQL Server - Enterprise Edition - Per Core
Software and Licensing	Microsoft SQL Server - Standard Edition - Per Core
Software and Licensing	Microsoft SQL Server - Standard Edition - Server instance * requires SQL CAL's
Software and Licensing	Microsoft SQL Server - Standard Edition User CAL
Software and Licensing	Microsoft SQL Server - Standard Edition Device CAL
Software and Licensing	Microsoft SQL Server - Standard Edition External Connecters License
Software and Licensing	RavenDB - Enterprise - Per Core w/ Production Support
Software and Licensing	RavenDB - Enterprise - Per Core

ATTACHMENT 21 WORK-FROM-HOM HELP DESK REPRESENTATIVE SECURITY POLICY

The Department prefers centralized Help Desk operations to support this TORFP. However, Master Contractors may propose a Help Desk operation that includes the use of Work-from-Home (WFH) Help Desk Representatives under the following conditions.

1. TO Contractor shall have a robust Telework Security Policy that defines telecommuting and remote access requirements. TO Contractor shall ensure their Policy is consistent with the recommended best practices contained in NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, and as updated from time to time (http://csrc.nist.gov/publications/PubsSPs.html)

2. The policy shall establish minimum information security standards and requirements that include but are not limited to the following:

    a. Establish required measures to protect the integrity and security of the LTSS System and its data including but not limited to: required equipment, operating system, and application software for the WFH Help Desk Representative' remote devices; personal firewall programs; physical security requirements; and specified secure, remote access channel, such as a VPN.
    b. Provide a robust authentication procedure to minimize unauthorized access through the WFH Help Desk Representative' remote device (e.g., two-factor authentication).
    c. Employ an "acceptable use policy" in regards to the WFH Help Desk Representatives' remote device that prohibits the downloading of the LTSS System's Sensitive Data the Representatives' use of any personal files and applications resident on their personal computer or device. These files and applications should not be trusted and need to be seen as potential attack vectors.
    d. Restrict WFH Help Desk Representatives' access through the use of limited user authority and network connections so that they may only access those TO Contractor applications needed to support the Help Desk operation.
    e. Systemically prohibit the WFH Help Desk Representatives' from using their remote device without having all required information security mechanisms installed, including but not limited to all operating system updates and patches, anti-malware and anti-virus software.
    f. Perform regular remote vulnerability assessments against the WFH Help Desk Representatives' device to confirm compliance with the Telework Security Policy. Identify non-compliant systems and disable their access until the deficiencies are corrected.
    g. Log all WFH Help Desk Representative activity.
    h. Require the use of an acceptable telephone solution.   For example, if WFH Help Desk Representatives are not utilizing an enterprise VoIP-based telephone solution, then require the WFH Help Desk Representatives to use analog telephone lines when talking with customers. Consumer VoIP telephone systems (e.g., Vonage) should not be used because they may not be encrypted.

3. WFH Help Desk Representative should be required to acknowledge the security requirements as part of their daily sign-in process. In addition, all security policies and procedures within the policy should be reviewed annually with WFH Help Desk Representatives.

4. The policy shall establish clear guidance over the management of paper records handled by remote Help Desk Representatives which includes minimum requirements for securely storing and disposing of paper records with sensitive information.

5. The policy should establish a monitoring plan for WFH Help Desk Representatives that includes review of recorded WFH Help Desk Representative's screen activity as well as voice conversations.

6. Provide WFH Help Desk Representatives with regular, obligatory training sessions to raise their awareness of security risks, preventive measures, and information security best practices.

7. A criminal background check shall be completed for all WFH Help Desk Representatives in conformity to Section 3.14 Security Requirements, 3.14.5 Criminal Background Check.

8. All WFH Help Desk Representatives must reside and operate from within the United States.

ATTACHMENT 22 TEFT IVR PROPOSED CALL FLOW

See attached document.