A Statement of Work (SOW) is typically used when the task is well-known and can be described in specific terms. Statement of Objective (SOO) and Performance Work Statement (PWS) emphasize performance-based concepts such as desired service outcomes and performance standards. Whereas PWS/SOO's establish high-level outcomes and objectives for performance and PWS's emphasize outcomes, desired results and objectives at a more detailed and measurable level, SOW's provide explicit statements of work direction for the contractor to follow. However, SOW's can also be found to contain references to desired performance outcomes, performance standards, and metrics, which is a preferred approach.

The Table of Content below is informational only and is provided to you for purposes of outlining the PWS/SOO/SOW. This sample is not all inclusive, therefore the reader is cautioned to use professional judgment and include agency specific references to their own PWS/SOO/SOW.

Statement of Objectives

TABLE OF CONTENTS

STATEMENT OF WORK

Enterprise Cloud Computing

Project ID: _____

Date

1.0 BACKGROUND

Currently, a complex collection of heterogeneous networks, devices, and systems provides the communication and computing infrastructure to support IT systems throughout the Agency. The Government is directed to use approved ports and protocols, service network testing & certification processes and other downward-directed regulations that impose additional compliance burdens on the department. Updated equipment, enhancements, and improvements to this infrastructure, services and applications are made regularly without a comprehensive view of the impact it will have on throughput, delay, routing, fault tolerance, and other aspects of the Agency services.

The use of Electronic Health Records (EHR) is becoming more prevalent in a wide variety of military applications and areas. As handheld devices become more advanced and EHR information is stored on them, security and privacy concerns of EHRs must be addressed as the handheld devices cannot be controlled like access to terminals in a fixed location or room. We maintain that data within an EHR should have (and indeed will soon be required to have) the same granularity in the level of data protection as is found in modern computer operating systems. Furthermore, it is reasonable to expect that users will interact with the EHRs with distinct security and privacy policies based on their role in providing care.

The bandwidth available in tactical communications networks is extremely sparse compared with other computer networks (kbps vs. gbps) due to the differing requirements and operating environments of tactical networks. In addition, in the field mobile ad hoc networks are becoming more common necessitating supporting the secure transmission of medical data to such networks. Constrained bandwidth coupled with a mobile environment with sporadic connectivity to a “home” network results in an extremely challenging environment for the delivery of medical services.

For the purposes of this project and the requirements below, the (AGENCY) Health System is defined as ALL medical information systems, clinical, business or of any type that provides capability, interacts with for data with the medical systems and transactions belonging to the (Program Name), Army, Navy, Air Force or Marine Corps.

A Paradigm Shift to “Cloud Computing”:

The “cloud computing” approach promises to provide users on-demand network access to computing resources and services without an on-site IT infrastructure. Applications, data storage, data transport, data processing takes place “within the cloud” much like a utility provides natural

gas, water, or electricity. The user is unaware of what server or servers are providing the resources to accomplish the task.

While attractive due to its' conceptual simplicity and claim of substantial cost savings, the privacy and security of data within the cloud is an open question. The very nature of cloud computing implies that the source and integrity of the data, it's storage and processing is unknown at this time. A long-term objective is to cleave the application or data layer from the network cloud.

This project limits the scope of work on "cloud computing" to the infrastructure (standards, controls and resources) and a distributed network layer (hardware, communications, resources) which establishes the "cloud" and does not include the middle-tier layer up to the user interface that would provide access to utilize data and services presented by the cloud.

The following link relates NIST's role in Cloud Computing for the federal government: NIST's role in cloud computing is to promote the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards.
http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
http://csrc.nist.gov/groups/SNS/cloud-computing/

2.0 SCOPE

A Critical Mission Need: A MHS Network Model (Simulation Framework):

An enterprise-level (node-to-node, gateway-to-gateway) simulation model of the current and alternative MHS network topologies to provide a basis for evaluating the effect of configuration changes (equipment upgrades, application changes, etc.) and network traffic changes (outages, re-routes, Quality of Service (QOS), etc.) . Simulation of the topologies would also benefit capacity planning, link performance, availability and "what-if" analysis.

Communications:

These proof-of-concept studies and analysis will evaluate alternatives, model and simulate the communications network requirements and framework to support the secure delivery of military medical mission data as well as medical imagery to units and personnel all medical mission needs to include operational tactical environments. Additionally, alternatives for mobile medical data and communication devices should be configurable model for simulation (device dependent but standards driven) in the proposed network environments. The model will be used to evaluate latency, impact of error and corruption, etc. Furthermore, at the device level the MHS requires an analysis of dynamic across the network and packet prioritization, including rules-based or directed routing/re-routing through the network.

The objectives of this PWS are to define the action items required to support the Office with technical and IT engineering services and subject matter expertise to provide proof-of-concept studies including modeling, simulation, and analysis supporting the Pacific and European Regional Data Processing centers. This involves creating a nimble, strategic approach to new

MHS network and hardware provisioning architectures. Additionally, this strategy would define an open standards-based approach for meeting current and future interoperability requirements. These studies will need to address the need to meet the Department's complex security and use-case requirements supporting the Government overarching health requirements.

Define the best distributed network architecture, topology and strategy for the Theater medical mission (integrated and interoperable with garrison-based network architecture) that will improve scalability, reduce hardware costs (commodity hardware and software), simplify maintenance and improve speed of processing.

3.0 PERIOD OF PERFORMANCE

The base period of performance is for one year from contract award with four, one-year options.

4.0 OBJECTIVES

At a minimum, this SOO supports the following goals:

TASK 1 – MHS Simulation Framework Model

1. An enterprise-level (node-to-node, gateway-to-gateway) simulation framework model of the current and alternative MHS network topologies to provide a basis for evaluating the effect of configuration changes (equipment upgrades, application changes, etc.) and network traffic changes (outages, re-routes, Quality of Service (QOS), etc.) . Simulation of the topologies would also benefit capacity planning, link performance, availability and "what-if" analysis.

Dynamic Enterprise Simulation Framework to allow the MHS users to model, simulate, document, visualize and update changes to the "As-Is" MHS Network:

- Determine current network configuration via combination of documentation and automated discovery of network devices using OPNET Virtual Network Environment (VNE) software
- Develop OPNET ™ model of MHS enterprise; outputs from any other software application used must be able to integrate/import-export to OPNET.
- Measure MHS message traffic and build model for use in simulation.
- Validate enterprise model using performance statistics collected on MHS by MCiS
- Provide the capability for the MHS users to run simulations on the simulation framework that could be "to-be" alternatives of the MHS Network to include regional distributed networks / shared databases.
- Web-based front-end interface.
- User guide and training.

The government will provide the contractor with the following information (POC – MCiS):

- Router configuration and routing table information

- Usage profiles for services and applications
- Characterization of non-MHS traffic running on the same network
- Access to configuration strategy and management
- Network architecture documentation and access to Simple Network Management Protocol (SNMP) data stored on network devices

TASK 2 - Model MHS alternative future network architectures and evaluate "cloud computing" impacts

2. This project limits the scope of work on "cloud computing" to the infrastructure (standards, controls and resources) and a distributed network layer (hardware, communications, resources) which establishes the "cloud" and does not include the middle-tier layer up to the user interface that would provide access to utilize data and services presented by the cloud.

The MHS needs to study the potential of alternative future network architectures. The vendor will provide:

Model an MHS architecture approach that supports cloud computing principles
Evaluate, analyze and document whether a cloud computing architecture will meet requirements for availability, reliability, and performance; utilizing business case analysis of cloud use in enterprise applications (garrison, humanitarian and warfighter deployed capability)
Configuration strategy and management
Integration of NIPR / SIPR approach/strategy into the cloud future model

TASK 3 – NIPR/SIPR integration into the MHS Network Architecture

3. Evaluate current NIPR / SIPR structures and communication needs and propose to-be future integration strategies that co-locate the classified and unclassified networks into the physical MHS infrastructure enclave (a new endeavor – current ops has the SIPR capability in Skyline 4 vs. incorporated into the current DP centers and future regional distribution centers);
Define systems' migration, integration, detailed management processes, procedures and SOPs for integrated centers.

On direction of the government, acquire, test and integrate a department approved high-assurance, low-to-high guard (NIPR > SIPR) and/or DoD department approved high-to-low (SIPR>NIPR).

TASK 4 – MHS Network Load Capacity Testing

4. Provide network load capacity testing and determine correct scalability, interoperability requirements to meet the Government missions; Scale and load test pilot/prototype network configurations to optimize the system's ability to handle maximum number of concurrent users and records replication, update and storage

- Load capacity testing to accommodate X# of concurrent users; utilize most demanding DP queries and incorporate Government users – extend to a consolidated that has over 41M records. Would need to determine both departments estimate of maximum usage and number of concurrent users worldwide.
- Determine maximum number of concurrent users and records replication, update and storage

5.0 CONSTRAINTS

This section lists laws, rules, regulations, standards, technology limitations and other constraints that the service and/or service provider must adhere to or work under.

5.1 HSPD-12 Personnel Security Clearances

Acquired services shall comply with the following regulations and requirements:

Homeland Security Presidential Directive-12 requires that all federal entities ensure that all contractors have current and approved security background investigations that are equivalent to investigations performed on federal employees.

The Contractor shall comply with GSA order 2100.1 – IT Security Policy, GSA Order ADM 9732.1C – Suitability and Personnel Security, and GSA Order CIO P 2181 – HSPD-12 Personal Identity Verification and Credentialing Handbook. GSA separates the risk levels for personnel working on federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk. Criteria for determining which risk level a particular contract employee falls into are shown in Figure A-1 of GSA ADM 9732.1C. The Contractor shall ensure that only appropriately cleared personnel are assigned to positions that meet these criteria.

Those contract personnel determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) or equivalent investigation.

Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.

Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

The Contracting Officer, through the Contracting Officer's Technical Representative or Program Manager will ensure that a completed Contractor Information Worksheet (CIW) for each Applicant is forwarded to the Federal Protective Service (FPS) in accordance with the GSA/FPS Contractor Suitability and Adjudication Program Implementation Plan dated 20 February 2007. FPS will then contact each Applicant with instructions for completing required forms and releases for the particular type of personnel investigation requested.

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been no break in service, and the position is identified at the same or lower risk level.

After the required background investigations have been initiated, the Contractor may request

authorization for employees whose investigations are pending to access systems supporting GSA e-mail and collaboration applications. The GSA Chief Information Officer may grant this authorization based on determination of risk to the government and operational need for the support of these applications.

5.2 Non-Disclosure Agreements

Standard non-disclosure statements shall be provided as required for system administration personnel who may have access to government data in the course of their duties.

5.3 Accessibility

Requirements for accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) are determined to be relevant. Information about the Section 508 Electronic and Information Technology (EIT) Accessibility Standards may be obtained via the Web at the following URL: www.Section508.gov . The Government Product/Service Accessibility Template (GPAT) is found in Attachment 7 of this solicitation. Generally accepted inspection and test methods corresponding to the identified Section 508 standards are reflected in the EIT Acceptance Guide found at Attachment 8.

5.4 Data

Records and data shall be documented in deliverable reports (electronically). Any databases/code shall be delivered electronically and become the sole property of the United States Government. All deliverables become the sole property of the United States Government. The Government, for itself and such others as it deems appropriate, will have unlimited rights under this contract to all information and materials developed under this contract and furnished to the Government and documentation thereof, reports and listings, and all other items pertaining to the work and services pursuant to this agreement including any copyright.

Unlimited rights under this contract are rights to use, duplicate, or disclose data, and information, in whole or in part in any manner and for any purpose whatsoever without compensation to or approval from the provider. The Government will at all reasonable times have the right to inspect the work and will have access to and the right to make copies of the above-mentioned items. All digital files and data, and other products generated under this contract, shall become the property of the Government.

All Contract participants shall sign a non-disclose and non-compete agreement to restrict use and protect confidential and proprietary information.

5.5 Confidentiality, Security, and Privacy

In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, the Contractor shall be responsible for the following privacy and security safeguards:

(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards used by the Contractor under the resulting contract or otherwise provided by or for the government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public government data collected and stored by the Contractor, the Contractor shall afford the government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(d) The Offeror's solution must comply with the GSA CIO IT Security Procedural Guide CIO-IT Security-09-48, Security Language for IT Acquisition Efforts as required for a Moderate Impact system.

(e) Work on this project may require or allow contractor personnel access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

(f) All data at rest will reside within the contiguous United States, the District of Columbia, and Alaska (CONUS) with a minimum of two data center facilities at two different and distant geographic locations