SECTION C: DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

Article C.1 Statement of Work

This contract is designed to permit the Institutes and Centers (ICs) of NIH, the Department of Health and Human Services (DHHS), and all other federal agencies to acquire a wide range of IT services and solutions, both commercial and non-commercial (as referenced in FAR 2.101). These IT services include, but are not limited to, health, health science and biomedical-related IT services to meet scientific, health, administrative, operational, managerial, and information management requirements. The contract also contains general IT services partly because healthcare systems are increasingly integrated within a broader IT architecture, requiring a systems approach to their implementation and a sound infrastructure for their operation. The focus of this contract is to provide to government agencies a mechanism for streamlined ordering of required IT solutions and services at equitable and reasonable prices, to give qualified small businesses a greater opportunity to participate in these requirements, and as a result, give government agencies a mechanism to help meet their socio-economic contracting goals.

The task areas included in the contract, in particular the Task Area 1, "IT Services for Biomedical Research, Health Sciences and Healthcare," support and provide consistency with the accountability goals of the Federal Health Architecture (FHA), whereby federal agencies are to coordinate effective capital planning activities and invest in and implement interoperable health IT. The task areas included in the contract are also designed to support the IT services described in the Federal Enterprise Architecture (FEA). Several examples follow:

a. Task Area 2 (Article C.2.2), Chief Information Officer (CIO) Support can be used to develop and maintain agency enterprise architectures, in support of the FEA.

b. For inherently IT components of the FEA, CIO-SP3 Small Business includes task areas that directly address those components. For example, the FEA includes document management as a digital asset service in the Service Reference Model (SRM) that can be addressed through Task Area 8 (Article C.2.8), Digital Government.

c. For non-IT components of the FEA, the contract includes task areas that support the automation of those components. For example, supply chain management is a business management service in the SRM. Task Area 9 (Article C.2.9), Enterprise Resource Planning includes the services needed to automate supply chain management.

d. Several FEA components provide support for the execution of IT functions, e.g., customer relationship management, a customer service in the SRM. These components can be supported through Task Area 4 (Article C.2.4), Outsourcing and Task Area 5 (Article C.2.5), IT Operations and Maintenance (O&M).

e. The FEA Technical Reference Model (TRM) includes standards and technology that would be selected and integrated into systems under specific task orders. For example, web servers are a delivery server in the TRM that could be selected and installed as part of Digital Government task area. In general, all task areas ultimately to be awarded under the contract must be compatible with the agency architecture defined by the agency's TRM. The standards and technology of the TRM will always be incorporated into the systems that are planned and developed under task orders awarded under the contract.

f. The contract can be used to award task orders that support the Performance Reference Model (PRM) by collecting agency metrics affected by the task. All task areas involve collecting applicable data for the PRM measurement category of Information and Technology Management. Task orders can also support the automation, collection, and evaluation of non-IT measurement areas.

g. The contract can be used to award task orders that require contractors to provide services that plan, implement and manage data defined in an agency's Data Reference Model (DRM).

The Scope of Work set forth under Article C.2 below outlines the general requirements of the contractor under this contract. Specific details of task assignments, deliverables, documentation, training, applicable government/department/industry standards, etc., will be provided within individual task orders issued by OCOs.

The contractor, acting as an independent contractor and not as an agent of the government, shall furnish all materials, personnel, facilities, support and management necessary to provide the services and solutions as set forth in the Scope of Work below. The geographic scope of this requirement includes the Continental United States (CONUS) and Outside the Continental United States (OCONUS).

Article C.2 Scope of Work

Ten task areas constitute the technical scope of this contract:

Task Area 1: IT Services for Biomedical Research, Health Sciences, and Healthcare
Task Area 2: Chief Information Officer (CIO) Support
Task Area 3: Imaging
Task Area 4: Outsourcing
Task Area 5: IT Operations and Maintenance
Task Area 6: Integration Services
Task Area 7: Critical Infrastructure Protection and Information Assurance
Task Area 8: Digital Government
Task Area 9: Enterprise Resource Planning
Task Area 10: Software Development

Each of the task areas described below identifies examples of the types of services that may be included under each task area. The examples are not exhaustive, and other IT services, as required, may be associated with the task areas defined in this Statement of Work.

Task Area 1 specifically provides examples of solutions and services pertaining to biomedical research, health sciences, and healthcare. However, all other nine task areas may also be used to support a health-related mission.

C.2.1 Task Area 1 - IT Services for Biomedical Research, Health Sciences, and Healthcare

The objective of this task area is to support Biomedical Research, Health Sciences and Healthcare by performing studies and analyses, and providing operational, technical, and maintenance services for the systems, subsystems, and equipment, some of which interface with, and are extensions to, information systems throughout the federal government. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. Health Sciences Informatic and Computational Services
b. Health Communication Support Services and Enhancements to Facilitate Integration and Data Exchange at the Federal, State, and Local Level
c. Integration of Health Systems Across Federal Agencies and Public and Private Healthcare Systems
d. Modernization and Enhancement of Existing Health IT Legacy Systems
e. Automation of Administrative and Clinical Processes
f. Biomedical Information Services
g. Biomedical Modeling, Visualization, and Simulation
h. Biosurveillance and Disease Management Support
i. Scientific Computing Services
j. IT Clinical Support Services
k. Telemedicine (e.g., mobile health/mHealth)
l. Healthcare Payment Processes and Fraud and Abuse in Medical Claims
m. Health Emergency Preparedness and Response to Include IT Support for Epidemic and Bio-Terrorism Simulations, Emergency Response Training, Exercise Support, etc.
n. Security of Healthcare and Biomedical Research Systems
o. IT Service Management
p. Healthcare Systems Studies
q. Natural Language Processing Software and Services (Biology/Medicine Focus)
r. Medical Computer-based Training
s. Standards Development for Health IT Services

C.2.2 Task Area 2 - Chief Information Officer (CIO) Support

The objective of this task area is to support Chief Information Officers (CIOs) in implementing laws, regulations, and polices and to facilitate evolving CIO practices. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. IT Governance Process Development and Management
b. Workforce Management
c. Capital Planning and Investment Control Support
d. Independent Verification and Validation
e. Agency Information Technology Architecture Support
f. IT Portfolio Analysis
g. Risk Management
h. Program Analyses and Implementation (including Business Cases Analysis, Cost/Benefit Analysis and Cost Effectiveness Analyses)
i. IT Organizational Development
j. Program Management Office Support
k. Advisory and Assistance Services
l. FEA Alignment Support Services
m. Market Research

C.2.3 Task Area 3 – Imaging

The objective of this task area addresses systems and services that support the collection, storage, and retrieval of digital images. Digital images can include scanned documents, medical images, geographical information systems, video, and photographs. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. Document Management Systems
b. Image Conversion
c. Image Content Management
d. Medical Imaging, including Picture Archiving and Communication Systems
e. Document Imaging
f. Workflow Management for Digital Imaging Functions
g. Geospatial and Scientific Imaging
h. Environmental Imaging
i. Image Analysis
j. 3D Immersive Visualization
k. Imaging Related to Laboratory and Test Equipment
l. Security Imaging
m. Identity and Access Management

C.2.4 Task Area 4 – Outsourcing

The objective of this task area is to provide the Information Technology (IT) infrastructure and IT services required to assume management and operations of government IT resources and IT business functions. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. Program Management
b. Management of Call Centers
c. Network Operations and Web Management Support
d. Leasing of Hardware and Software
e. Tools and Applications (including Application Service Provider)
f. Hardware/Software Maintenance
g. Transition Planning
h. A-76 Studies Specific to IT Operations or Support
i. Data Base Administration and Data Storage Management
j. Backup and Recovery Services System Console Operations
k. Production Control and Management

l. Asset Management (including Radio Frequency Identification [RFID] Tracking)
m. IT Acquisition Management
n. Desktop Computing as a Unified Service
o. Managed IT Services Support
p. IT Impact Analyses
q. Workflow Management
r. Implementation of Standards (e.g., International Organization for Standardization (ISO) 9000, Capability Maturity Model Integration (CMMI), IT Services Management)
s. Solution Leasing
t. Software-as-a-service (SaaS)
u. Cloud Computing

C.2.5 Task Area 5 – IT Operations and Maintenance

The objective of this task area is to support the operation and maintenance of IT systems, keeping IT systems viable with supported vendor releases or off-the-shelf applications software upgrades. Operations and maintenance on IT systems shall include all software and hardware associated with mainframes, client/server, web-based applications, and networking. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. Operational Support
b. Software Maintenance and Upgrades
c. Telecommunications Maintenance (Data, Voice, Images, including Wireless)
d. Infrastructure Management Services (IMS)
e. Configuration Management
f. Network/Hardware Support
g. Help Desk/IT Support
h. Resource Management
i. Backup and Recovery Management
j. Installation, Configuration, and Tuning
k. Electronic Software Licensing Services including license: deployment, management, tracking, upgrading, etc.
l. System Management
m. IT Training
n. IT Operation and Maintenance Planning
o. Data Quality Management
p. Transformation Services
q. Continual Service Improvement
r. Balanced Scorecard for Operations
s. IT Infrastructure Optimization

C.2.6 Task Area 6 – Integration Services

The objective of this task area is to support the development and deployment of integrated information systems, which includes the integration of technical components, information technology components, organizational components and documentation. Integration projects can support a wide range of agency functions. In the healthcare and research domain, medical imaging systems, patient management systems, clinical management systems, and laboratory management systems are often provided via integration of commercial components with existing infrastructure. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. Infrastructure Engineering, Development, Implementation, Integration
b. Enterprise Application Integration
c. Gap Analysis and Benchmarking
d. Data Migration and Integration
e. Open Source Integration
f. Enterprise Data Management
g. Collaboration Tools

h. Business Process Reengineering
i. Test and Evaluation Services
j. Financial Analysis
k. Feasibility Studies
l. Requirements Analysis
m. System Design Alternative (SDA) Studies
n. Systems Engineering
o. Architecture Validation and Verification
p. Risk Assessment
q. Acquisition Support

C.2.7 Task Area 7 – Critical Infrastructure Protection and Information Assurance

The objective of this task area is to support the protection of critical infrastructure, assurance of agency information, and operations that protect and defend information and information systems by ensuring confidentiality, integrity, availability, accountability, restoration, authentication, non-repudiation, protection, detection, monitoring, and event react capabilities. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. Cyber Security
b. Critical Infrastructure Asset Identification and Configuration Management Databases
c. Information Assurance of Critical Infrastructure
d. Risk Management (Vulnerability Assessment and Threat Identification)
e. Facility Protection Planning
f. Information Systems Security
g. Security Operations Center Development and Operations Management
h. Application Security
i. Disaster Recovery
j. Critical Infrastructure Continuity and Contingency Planning
k. Incident Response Planning and Execution
l. Security Certification and Accreditation
m. Training and Awareness Programs
n. Exercises and Simulation
o. Federal Information Security Management Act (FISMA) Implementation Support
p. Health Insurance Portability and Accountability Act Implementation Support
q. Cryptographic Support and Services
r. Record Management
s. Public Key Infrastructure
t. Trusted Internet Connections implementation
u. Security Review and Analysis of Automated Information Systems
v. Identity Management and Assurance
w. Intelligent, Automated Data Collection and Analysis
x. IT Forensics and eDiscovery

C.2.8 Task Area 8 – Digital Government

The objective of this task area is to support government services that are provided through digital, electronic means, creating a transparent interaction between government and citizens (G2C – government-to-citizens), government and business enterprises (G2B – government-to-business enterprises) and government interagency relationships (G2G - government-to-government). A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. Data Warehousing and Data Mining
b. Business Intelligence
c. Web Development and Support
d. Electronic Commerce and Electronic Data Interchange
e. Customer Relationship Management
f. Knowledge Management (IT-based sharing/storing of agency individuals' knowledge)

g. IT –Enhanced Public Relations
h. IT Strategic Planning
i. Records/Document Management
j. Business-to-Government (B2G) Solutions
k. Communications Management
l. Accessibility Services (508 and 504 compliance)
m. Automated Abstraction, Taxonomies, and Ontologies
n. Deep web and federated searching
o. Computational linguistics and machine-based translation
p. Telecommuting Support Services
q. Interactive Marketing

C.2.9 Task Area 9 – Enterprise Resource Planning

The objective of this task area is to support the implementation of enterprise management applications and systems in the federal environment, which are integrated software applications used to control, monitor, and coordinate key business activities across an enterprise. These applications generally fall into the following categories: Financials, Human Resources, Logistics, Manufacturing, and Projects. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. ERP Package Implementation
b. Integration of Business Systems
c. Business Consulting Services
d. Business Transformation and Business Process Reengineering
e. Business Systems Modernization
f. IT Software Package Selection
g. ERP IT Infrastructure
h. ERP Infrastructure Planning, Installation, and Tuning
i. Performance Load Testing
j. ERP End User Training

C.2.10 Task Area 10 – Software Development

The objective of this task area is to develop customized software applications, database applications, and other solutions not available in off-the-shelf modular software applications. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a. Requirements Analysis, Design, Coding, and Testing
b. Production Deployment
c. Application Prototyping
d. Multimedia Software for Patient/Staff Education
e. Program Evaluation Software
f. Administrative and General Decision Support Software
g. Business Intelligence and Analytics
h. GIS-Enhanced Planning and Program Evaluation Software
i. Web 2.0 Development and Management
j. Database Development and Management
k. Clinical Protocol and Quality Assurance Decision Support Software

Article C.3 Reporting Requirements

The contractor is responsible for the following reporting on task order activity under the GWAC. Reporting required under paragraphs a. through e. below shall be made through the Electronic Government Ordering System (e-GOS). (See G.7.1 Electronic Government Ordering System for further information.)

All reports required herein shall be submitted in electronic format. All reports submitted in electronic format shall be compliant with Section 508 of the Rehabilitation Act of 1973. Additional information about testing documents for Section 508 compliance, including specific checklists, by application, can be found at: http://www.hhs.gov/web/508/index.html under "Helpful Resources."

a. Award and Modification Report

All task order awards and modifications issued shall be reported in e-GOS within 3 business days of receipt by the contractor. The reporting of modifications pertains to both funded modifications and administrative modifications.

b. Quarterly Activity Report

The Quarterly Activity Report is a summary of the award and modification activity reported by the contractor in the e-GOS during the previous quarter. The contractor is responsible for correcting any errors in the information prior to quarterly certification of the information through e-GOS.

c. NIH Contract Access Fee Payment Report

The NIH Contract Access Fee (NCAF) Payment Report is a summary of payment activity by the contractor. The contractor shall certify NCAF payments through e-GOS on a quarterly basis. During the process of certification, the contractor shall provide the status on any balances that are due and identify and explain any discrepancies found.

d. Contractor Profile Report

The contractor shall be responsible for maintaining the contractor company profile in e-GOS. On a quarterly basis, the contractor shall certify the accuracy of the information in e-GOS.

e. Reporting Schedule

The certifications required by paragraphs b through d shall be submitted in accordance with the following schedule:

Quarter	Period	Due Date
Quarter 1	October 1 – December 31	by January 15
Quarter 2	January 1 – March 31	by April 15
Quarter 3	April 1 – June 30	by July 15
Quarter 4	July 1 – September 30	by October 15

f. Limitations on Subcontracting Certification

The contractor shall submit an annual certification by October 15 of each year stating whether or not the contractor complied with FAR 52.219-14(c)(1) (Limitations on Subcontracting) for the previous fiscal year.

g. Information Security and Physical Access Security Reporting Requirements

*(The following reporting requirements **do not apply to this contract**; however, these requirements apply to applicable HHS task Orders. For non-HHS task orders, the Information and Physical Access Security clause may be appropriately tailored by the customer agency as applicable.)*

The Contractor shall submit the following reports as required by the Information and Physical Access Security clause in Article H.6 of Section H of this contract.

1. Roster of Employees Requiring Suitability Investigations

   The contractor shall submit a roster, by name, position, e-mail address, phone number and responsibility, of all staff (including subcontractor staff) working under the contract who will develop, have the ability to access, or host and/or maintain a Federal information system(s). The roster shall be submitted to the Contracting Officer's Representative (COR), with a copy to the Contracting Officer, within 14 calendar days of the effective date of the contract. (Reference subparagraph A.e of the Information and Physical Access Security clause in Article H.6 of Section H of this contract.)

2. Reporting of New and Departing Employees

   The Contractor shall notify the Contracting Officer's Representative (COR) and contracting Officer within five working days of staffing changes for positions that require suitability determinations as follows:

a. New Employees who have or will have access to HHS Information systems or data: Provide the name, position title, e-mail address, and phone number of the new employee. Provide the name, position title and suitability level held by the former incumbent. If the employee is filling a new position, provide a description of the position and the Government will determine the appropriate security level.

b. Departing Employees: 1) Provide the name, position title, and security clearance level held by or pending for the individual; and 2) Perform and document the actions identified in the "Employee Separation Checklist", attached in Section J, List of Attachments of this contract, when a Contractor/Subcontractor employee terminates work under this contract. All documentation shall be made available to the COR and/or Contracting Officer upon request. (Reference subparagraph E.2.a through E.2.c of the Information and Physical Access Security clause in Article H.6 of Section H of this contract.)

c. Contractor - Employee Non-Disclosure Agreement(s): The contractor shall complete and submit a signed and witnessed "Commitment to Protect Non-Public Information - Contractor Agreement" form for each contractor and subcontractor employee who may have access to non-public Department information under this contract. This form is located at: http://ocio.nih.gov/docs/public/Nondisclosure.pdf . (Reference subparagraph E.3.d. of the Information and Physical Access Security clause in Article H.6 of Section H of this contract.)

(The following reporting requirement does not apply to this contract, but will apply to any HHS task order that involves contractor access to federal information or federal information systems.)

3. IT Security Plan (IT-SP)

In accordance with HHSAR Clause 352.239-72, Security Requirements For Federal Information Technology Resources, the contractor shall submit the IT-SP within thirty (30) days after contract award. The IT-SP shall be consistent with, and further detail the approach to, IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The IT-SP shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of IT resources that are developed, processed, or used under this contract. If the IT-SP only applies to a portion of the contract, the Contractor shall specify those parts of the contract to which the IT-SP applies.

The Contractor shall review and update the IT-SP in accordance with NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, on an annual basis.

(Reference subparagraph D.c.1 of the Information and Physical Access Security clause in Article H.6 of Section H of this contract.)

(The following reporting requirement does not apply to this contract, but will apply to any HHS task order that involves contractor access to federal information or federal information systems.)

4. IT Risk Assessment (IT-RA)

In accordance with HHSAR Clause 352.239-72, Security Requirements For Federal Information Technology Resources, the contractor shall submit the IT-RA within thirty (30) days after contract award. The IT-RA shall be consistent, in form and content, with NIST SP 800-30, Risk Management Guide for Information Technology Systems, and any additions or augmentations described in the HHS-OCIO Information Systems Security and Privacy Policy.

The Contractor shall update the IT-RA on an annual basis.

(Reference subparagraph D.c.2 of the Information and Physical Access Security clause in Article H.6 of Section H of this contract.)

(The following reporting requirement does not apply to this contract, but will apply to any HHS task order that involves contractor access to federal information or federal information systems.)

5. FIPS 199 Assessment

In accordance with HHSAR Clause 352.239-72, Security Requirements For Federal Information Technology Resources, the Contractor shall submit a FIPS 199 Assessment within thirty (30) days after

contract award. The FIPS 199 Assessment shall be consistent with the cited NIST standard.

(Reference subparagraph D.c.3 of the Information and Physical Access Security clause in Article H.6 of Section H of this contract.)

(The following reporting requirement does not apply to this contract, but will apply to any task order that involves contractor development, maintenance, and access to federal information systems.)

6. IT Security Certification and Accreditation (IT-SC&A)

   In accordance with HHSAR Clause 352.239-72, Security Requirements for Federal Information Technology Resources, the Contractor shall submit written proof to the Contracting Officer that an IT-SC&A was performed within three (3) months after contract award.

   The Contractor shall perform an annual security control assessment and provide to the Contracting Officer verification that the IT-SC&A remains valid.

   (Reference subparagraph D.c.4 of the Information and Physical Access Security clause in Article H.6 of Section H of this contract.)