

Procurement Sensitive



Department of Health and Human Services

Centers for Medicare & Medicaid Services

Federal Exchange Program System Data Services Hub Statement of Work

Draft

Version 1.0

July 15, 2011

Table of Contents

1. Introduction	1
1.1 Task Order Scope.....	4
1.2 Contract Outcome	4
1.3 Assumptions and Constraints.....	5
1.4 Standards and Reference Material	6
2. Requirements and Work Activities	8
2.1 General Technical Requirements	8
2.1.1 Infrastructure Requirements.....	8
2.1.2 Data Management Requirements	10
2.1.3 Data Security Requirements	11
2.1.4 Security Requirements and Authority to Operate	12
2.1.5 Authentication and Authorization Requirements.....	14
2.1.6 Web Services	14
2.1.7 System Logs.....	16
2.1.8 Roles and Responsibilities	16
2.1.9 Hours of Operation	17
2.1.10 Travel	18
2.1.11 Connectivity	18
2.1.12 Earned Value.....	18
2.2 Task Order Management.....	20
2.2.1 Management and Reporting.....	20
2.2.2 Exchange Life Cycle Management	21
2.2.3 Change Management	22
2.2.4 Quality Control	23
2.2.5 Risk Management	23
2.2.6 License Management	23
2.2.7 Joint Operating Agreements	24
2.3 Delivery of Data Services Hub	24
2.3.1 Eligibility Verification and Enrollment Services.....	24
2.3.2 Plan Management Services	27
2.3.3 Financial Management Services	27
2.3.4 Remaining Functional DSH Services	28
2.3.5 Comprehensive Testing	29
2.3.6 Nationwide Service Integration Testing	30
2.3.7 Service Governance	30
2.3.8 Training.....	30
2.4 Work Activities.....	31
2.4.1 Work Activity 1 – Program Startup Review.....	32
2.4.2 Work Activity 2 – Platform Architecture	32
2.4.3 Work Activity 3 – E&E Services.....	33
2.4.4 Work Activity 4 – Plan Management Services.....	33

2.4.5	Work Activity 5 – Financial Management Services	34
2.4.6	Work Activity 6 – Oversight Services	34
2.4.7	Work Activity 7 – Customer Service.....	34
2.4.8	Work Activity 8 – Communications Services	34
2.5	Regional Technical Support.....	34
2.6	Operations and Maintenance.....	34
3.	General Requirements.....	35
3.1	Section 508 – Accessibility of Electronic and Information Technology	35
3.2	CMS Information Security.....	37
3.3	Financial Report.....	39
3.4	Transition Out to a New Contractor.....	40
3.5	General Assumptions	41
3.5.1	Other Assumptions.....	42
3.5.2	Contractor Contracting with States.....	Error! Bookmark not defined.
4.	Security	44

Section C. Statement of Work

The Contractor shall furnish all of the necessary personnel, materials, services, facilities, (except as otherwise specified herein), and otherwise do all the things necessary for or incident to the performance of the work as set forth below:

The Contractor, acting independently and not as an agent of the Government, shall furnish all the necessary services, qualified personnel, material, equipment/supplies (except as otherwise specified in the task order), and facilities, not otherwise provided by the Government, as needed to perform the Statement of Work (SOW) below.

Throughout this document, reference is made to notification, delivery, liaison and interaction between the Centers for Medicare and Medicaid Services (CMS) and the Contractor. This task order requires the Contractor to interact with CMS personnel of multiple disciplines (contracting personnel, contract management personnel, technical personnel, etc.) who form a CMS team. Identification of the specific point-of-contact on the CMS team for specific situations has not been addressed in this document; this lack of specificity in no way affects any of the requirements the contractor is required to perform. The Contractor is advised that specific use of the terms “CMS”, “Contracting Officers Technical Representative” (COTR) or “Contracting Officer” (CO) in this document could denote one or several other members of the CMS team (see Appendix A, ACRONYMS).

1. Introduction

On March 23, 2010, the President signed into law the Patient Protection and Affordable Care Act (P.L. 111-148). On March 30, 2010, the Health Care and Education Reconciliation Act of 2010 (P.L. 111-152) was signed into law. The two laws are collectively referred to as the Affordable Care Act. The Affordable Care Act creates new competitive private health insurance markets – called Exchanges – that will give millions of Americans and small businesses access to affordable coverage and the same insurance choices members of Congress will have. Exchanges will help individuals and small employers shop for, select, and enroll in high quality, affordable private health plans that fit their needs at competitive prices. The IT systems will support a simple and seamless identification of people who qualify for coverage through the Exchange, tax credits, cost-sharing reductions, Medicaid, and CHIP programs. By providing a place for one-stop shopping, Exchanges will make purchasing health insurance easier and more understandable and will put greater control and more choice in the hands of individuals and small businesses.

The Centers for Medicare & Medicaid Services (CMS) is working with States (including the District of Columbia and the territories) to establish Exchanges in every State. The law gives States the opportunity to establish State-based Exchanges, subject to certification that the State-based Exchange meets federal standards and will be ready to offer health care coverage on January 1, 2014. The deadline for certification is January 1, 2013. In a State that does not achieve certification by the deadline, the law directs the Secretary of Health and Human Services to facilitate the establishment of an Exchange in that State.

CMS has pursued various forms of collaboration with the States to facilitate, streamline and simplify the establishment of an Exchange in every State. These include an early innovator program, under which seven States were awarded grants to develop IT systems that could serve

as models for other States, as well as a federal data services hub, through which HHS will provide certain data verification services to all Exchanges. These two efforts have made it clear that for a variety of reasons including reducing redundancy, promoting efficiency, and addressing the tight implementation timelines authorized under the Affordable Care Act, many, if not most States, may find it advantageous to draw on a combination of their own work plus business services developed by other States and the Federal government as they move toward certification. Therefore, CMS is planning a menu of Exchange options for States.

“State Partnership Model”

Some States have expressed a preference for a flexible State Partnership Model combining State designed and operated business functions with Federally designed and operated business functions. Examples of such shared business functions could include eligibility and enrollment, financial management, and health plan management systems and services. State partnerships would not preclude States from meeting all certification requirements and choosing to operate an exclusively State-based Exchange. CMS is pursuing an approach that will be flexible to accommodate any of these options available to States.

Exchanges are competitive marketplaces

Section 1311 of the Affordable Care Act sets minimum standards for Exchanges covering key areas of consumer protection, including a certification process for qualified health plans (QHPs). These standards help ensure that all Exchanges will be competitive marketplaces that serve the interests of individuals and small businesses. By pooling people together, reducing transaction costs, and increasing transparency, Exchanges will create more efficient and competitive health insurance markets for individuals and small employers.

CMS has solicited public comment, published guidance, and provided technical support to States as they work to establish Exchanges. Our work to solicit input on the Exchange began with a formal Request for Comment that was published on July 27, 2010. Over 300 responses were received from a wide variety of stakeholders offering perspectives on many aspects of the implementation of Exchanges. Initial guidance was published in November 2010, and the first Notice of Proposed Rule Making, which will address the core standards for establishment and operation of Exchanges, will be published soon. See:

http://cciio.cms.gov/resources/files/guidance_to_states_on_exchanges.html

Exchange will help coordinate interaction with other State health coverage programs

Section 1311 of the Affordable Care Act requires Exchanges to coordinate eligibility determinations across State health coverage programs. On May 31, 2011, CMS issued IT guidance 2.0 to describe coordination among Exchanges, Medicaid and CHIP. See:

<http://www.cms.gov/Medicaid-Information-Technology-MIT/Downloads/exchangemedicaiditguidance.pdf>

States have the first option to establish Exchanges

Section 1311 of the Affordable Care Act provides each State with the option to set up an exclusively State-based Exchange and authorizes grant funding to cover start up costs through

2014 for States meeting benchmarks. Since September 30, 2010, CMS has awarded planning grants to 49 States and the District of Columbia to assist with initial planning activities related to the implementation of the Exchanges (“Planning Grants”). See:

http://cciio.cms.gov/resources/fundingopportunities/exchange_planning_grant_foa.pdf

In an effort to promote re-use and efficiency in the development of IT components for Exchanges, CMS provided funding for IT Innovation on February 15, 2011. These “Innovator Grants” went to seven States, totaling \$241 million in funding to develop Exchange IT systems that will serve as models for other States. These grants require the awardees to make available to other States their work and the IT products and other assets developed under the grants.

Importantly, these grantees participate in an “open collaborative” among States, CMS and other Federal agencies to share interim deliverables and knowledge to facilitate the efficient development and operation of Exchange IT systems. This approach aims to reduce the need for each State and the Federal government to “reinvent the wheel” and aids States in Exchange establishment by accelerating the development of Exchange IT systems. See:

http://cciio.cms.gov/resources/fundingopportunities/early_innovator_grants.pdf

A third funding opportunity was announced on January 20, 2011, which provides States with financial support for activities related to the establishment of exclusively State-based Exchanges (“Establishment Grants”). This funding opportunity provides two levels of funding based on the progress made by each State in planning for and establishing an Exchange. The first level provides one year of funding and can be limited in scope. The second level requires a more advanced state of readiness and provides funding through 2014. Interim deliverables and knowledge gained under these grants will also be supported in an open collaborative among States and CMS.

States can apply for grants to carry out activities in one or more of eleven core areas of Exchange operation: Background Research, Stakeholder Consultation, Legislative and Regulatory Action, Governance, Program Integration, Exchange IT Systems, Financial Management, Oversight and Program Integrity, Health Insurance Market Reforms, Providing Assistance to Individuals and Small Businesses, and Business Operations of the Exchange. State progress will be evaluated under these eleven core areas to support the certification of Exchanges by January 1, 2013. This funding opportunity announcement provided substantial information about standards and benchmarks that Exchanges must meet to achieve certification. See:

http://cciio.cms.gov/resources/fundingopportunities/foa_exchange_establishment.pdf

Certification of State Exchanges will be a flexible process

Section 1321 of the Affordable Care Act requires Exchanges be certified by no later than January 1, 2013. To meet that deadline, CMS anticipates that the certification process will begin no later than July 2012. The process is likely to include initial progress submissions, operational assessments of readiness, final applications, and a substantial amount of collaboration and discussion with CMS. Depending on the State, the process could include the State supplementing its own internally developed systems and services with work products developed by other States or the Federal government. From now through 2012, CMS will be working with States collaboratively, and will be continually evaluating how to develop federal business systems and services, and support similar development by others, in a manner that maximizes

State flexibility. The goal is to give States the full opportunity to compare the menu of options including a flexible State Partnership Model, and an exclusively a State-based Exchange.

1.1 Task Order Scope

The Federal Exchange Program System (FEPS) consists of a FX, which serves the needs of individuals within states where those states do not have their own state-run exchange, and the DSH, which provides common services and interfaces to federal agency information. Since states may elect to establish their own state-run exchanges or portions thereof, this task order will permit future modifications to encompass state's needs that are unknown at this time. Should CMS require additional services over and above those awarded at time of award, CMS will modify this order accordingly to meet the individuals' and states' needs. CMS expects these information technology (IT) systems to support a first-class customer experience, provide seamless coordination between state-administered Medicaid and CHIP programs and the FX, and between the FX and plans, employers, and navigators. These systems will also generate robust data in support of program evaluation efforts.

Through this procurement, CMS seeks qualified contractors to build the technical solution and support the operations of the DSH that serves the needs as described within the Affordable Care Act, enables consumers to obtain affordable health care coverage, and allows employers to offer healthcare coverage to their employees.

The DSH requirements support common services and provide an interface to federal agency information. These requirements drive a data services information hub structure that will act as a single interface point for Exchanges to all federal agency partners, and provide common functional service support. A single interface simplifies the integration required of the Exchanges. Common services allow for adherence to federal and industry standards regarding security, data transport, and information safeguards management.

In order to ensure exceptional performance and accountability for these projects, CMS is following the Exchange Life Cycle (ELC), a life-cycle model derived from the CMS Integrated IT Investment & System Life Cycle Framework (ILC) used for development and implementation of all CMS IT systems. The ELC was created with an Exchange-specific Project Process Agreement (PPA). All planning will also comply with Office of Management and Budget (OMB) Circular A-130 and the Clinger-Cohen Act, which mandates that each federal agency develop a depiction of the functional and technical processes utilized to accomplish its mission. All work performed should be compliant with HHS Enterprise Architecture.

1.2 Contract Outcome

For this task order, CMS desires a Managed Services approach that will include the following:

1. Architecting and developing of solutions for DSH that includes building of functional common services that can be used by multiple Exchanges and federal partners
2. Designing a solution that is flexible, adaptable, and modular to accommodate the implementation of additional functional requirements and services; and

3. Participating in a collaborative environment and relationship to support the coordination between CMS and the primary partners, e.g., the Internal Revenue Service (IRS)

The foregoing activities must be completed to ensure the DSH will be ready. The following reviews represent the key milestones (stage gate reviews in the ELC, dates represented as calendar year) for the DSH:

- Architecture Review: October 2011
- Project Startup Review: Q4 2011
- Project Baseline Review: Q4 2011
- Preliminary Design Review: Q1 2012
- Detailed Design Review: Q1 2012
- Final Detailed Design Review: Q2 2012
- Pre-Operational Readiness Review: Q2 2012
- Operational Readiness Review: Q3 2012

A detailed description of the foregoing activities and milestones can be found in the *Collaborative Environment and Life Cycle Governance Supplement to the Exchange Reference Architecture: Foundation Guidance* document and the CMS ILC site at <http://www.cms.hhs.gov/SystemLifecycleFramework/>

The planned artifacts and templates for the FEPS development will also be stored in the Application Life Cycle Management (ALM) environment that CMS is standing up for the use of multiple stakeholders across the Affordability Care Act projects.

1.3 Assumptions and Constraints

The Contractor shall take the following assumptions and constraints into consideration:

- The Affordable Care Act requires individuals to be enrolled in appropriate health insurance programs by January 2014. CMS expects open enrollment to begin in October 2013. CMS requires that Exchange and DSH capability be ready for nationwide testing by January 2013.
- The DSH will need to be developed and available to support state information exchange testing with various federal entities. In addition, CMS requires full functionality of the DSH to be designed, developed, and implemented by September 1st, 2013.
- The DSH will be utilized by other HHS agencies for shared services. For example, Community Living Assistance Services and Supports (CLASS) will utilize the DSH to conduct Eligibility verifications with other federal agencies.
- Varying schedules among participants within overall Exchange Program. Other federal agency partners and the states will determine their own development and delivery schedules for their components of the program.

- Level of cooperation and support for consistent milestones. CMS will track the progress of the states and federal partners with a focus on nationwide integration testing starting in January 2013.
- The applicability of the system models developed by Early Innovator States must be evaluated to assess the degree of leverage that can be recognized from innovation grant state deliverables in support of the remaining states, the federal exchanges, and the DSH
- The contractor shall acquire the required infrastructure services from the CMS Managed Service provider, Terremark. CMS will provide the contractor with a FEDSTRIP authorization to permit the contractor to order the required services from the cloud service provider's GSA contract, at pricing equal or better than the negotiated pricing on the CMS Cloud Services task order with Terremark.
- The Government intends on establishing a ceiling for indirect rates of not more than +/- 5% from the proposed rates.
- CMS defines local travel as travel that is less than twelve (12) hours in duration within the Washington Metropolitan Area, including Baltimore, MD, and Virginia, and does not require overnight lodging.
- Travel performed for personal convenience or daily travel to and from work at the contractor's facility or local Government facility (i.e., designated work site) shall not be reimbursed under this contract.
- If travel is proposed it shall be segregated from other pricing/elements and broken out as follows: Names of travelers, destination (to and from), mode of transportation, mileage, rental cars, hotel, purpose of trip, etc.
- All travel will be performed on an as needed basis and submitted to the CMS Contracting Officer Technical Representative (COTR) for approval prior to execution. Per diem will be reimbursed at Government-approved rates in effect at the time of travel. All travel as well as per diem (lodging, meals and incidentals) shall be reimbursed in accordance with the Federal Travel Regulation (FTR) – For reference purposes refer to the below link: <http://www.gsa.gov/portal/content/104790>

1.4 Standards and Reference Material

The following documents are provided as background material to this procurement:

- Guidance for Exchange and Medicaid IT Systems, versions 1.0 and 2.0
- Medicaid and Exchange IT Architecture Guidance: Framework for Collaboration with State Grantees. This overview document describes the relationships between the Exchange Reference Architecture documents.
- Exchange Reference Architecture Foundation Guidance
- Collaborative Environment and Life Cycle Governance – Exchange Reference Architecture Supplement
- Harmonized Security and Privacy Framework – Exchange TRA Supplement

- Eligibility and Enrollment – Exchange Business Architecture Supplement
- Plan Management – Exchange Business Architecture Supplement
- Conceptual Data Model and Data Sources – Exchange Information Architecture Supplement
- Business Blueprint Master Glossary. Glossary of key terms and concepts referenced in the Exchange Business Architecture supplements.
- Business Blueprint Services Workbook. Contains the inventory of Exchange business services and supporting business services identified from the process models and their mapping to business processes.
- Eligibility & Enrollment Blueprint Data Capture Workbook. Contains the meta-data describing the Eligibility & Enrollment process flows, and associated activities, information flows, and capabilities.
- Plan Management Blueprint Data Capture Workbook. Contains the meta-data describing the Plan Management process flows, and associated activities, information flows, and capabilities
- Financial Management Blueprint Data Capture Workbook. Contains the meta-data describing the Plan Management process flows, and associated activities, information flows, and capabilities
- CMS Technical Reference Architecture (TRA), v.2.1 and supplements. Several relevant TRA supplements are listed on the CMS web site (<http://www.cms.gov/SystemLifecycleFramework/TRAS/list.asp#TopOfPage>) and other supplements are under development. Supplements are available upon request.
- CMS Testing Framework document, which can be found at <http://www.cms.gov/SystemLifecycleFramework/Downloads/CMSTestingFrameworkOverview.pdf>
- MITA Framework 2.0 and supporting material. MITA material is available on the CMS web site (http://www.cms.gov/MedicaidInfoTechArch/04_MITAFramework.asp#TopOfPage).
- Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies. OMB No. 1545-0962. See www.irs.gov/pub/irs-pdf/p1075.pdf.
- Internal Revenue Manual (IRM); Part 10; Security, Privacy and Assurance. See www.irs.gov/irm/part10/

2. Requirements and Work Activities

These requirements are for systems development and delivery of a federally operated DSH. The Contractor's proposed solution shall be designed and developed to interoperate with the Federal and State Exchanges. As such, the majority of the tasks below relate to life cycle activities that support delivery. The CMS ELC is the baseline system development life cycle model used to structure and track progress. Each specific development task includes full life cycle coverage from technical requirements definition to testing and Authority to Operate (ATO). CMS has tailored the ELC through a PPA to create the ILC used in this SOW. CMS believes that an iterative development approach or agile development approach may provide the best opportunity to incrementally build and test DSH functionality.

The Contractor's proposed solution shall be based on a modular, agile, flexible services based approach to systems development, including use of open interfaces, open source software, Government Off-The-Shelf (GOTS) software, and exposed application programming interfaces supported as web services; the separation of business rules from core programming; and the availability of business rules in both human and machine readable formats.

2.1 General Technical Requirements

Each of the following technical areas describes one aspect of an integrated service capability to support DSH operations. Although the areas are described individually, the Contractor shall architect an integrated, flexible, and adaptable end-to-end solution.

2.1.1 Infrastructure Requirements

The key objectives of this infrastructure approach are to provide elasticity (flexibility with respect to capacity-on-demand), an operating expense model instead of a capital expense model, and usage-based pricing for processing, storage, bandwidth, and license management. To that end, the Contractor's proposed solution shall be incorporated into CMS' Terremark hosted environment and the Contractor shall work with Terremark, to ensure that these objectives are met as part of the infrastructure design and implementation, and the platform design and implementation.

The FEPS infrastructure is supported by managed services contract(s) for development, test, and production awarded to Terremark. Depending on the definition of the term "managed service," these managed services may be considered a federal cloud implementation. As such, it is imperative that the DSH services are designed and implemented in a platform independent manner, namely, the Contractor shall make no assumptions about the specifics of the managed service platform, but shall design and implement the services to take advantage of platform capabilities to allow for vendor independence, location independence, and elasticity (e.g., capacity-on-demand). This means that DSH services shall be built using open standards, open source software products, and platform-independent application programming interface (API) products, such as those available from Dasein or Deltacloud. If the Contractor believes another approach, for example using a COTS product suite or incorporating GOTS tools, will perform equally or better than an open source software suite, the Contractor may recommend such a solution. The Contractor shall then demonstrate that from performance, support, response, ease

of development, connectivity, and cost considerations the alternative solution meets or exceeds all requirements in this SOW.

The Contractor shall utilize the CMS secure managed services environment. The CMS secure managed services environment includes Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) support. The Contractor shall provide a comprehensive listing of all system infrastructure and platform components needed to support this SOW and work with Terremark to acquire, configure, and deliver them as part of the contractor's proposed solution to CMS. . The Contractor shall present the benefits, risks, and implementation technologies recommended, and work with CMS to finalize the approach. The Contractor shall develop, implement, test, and deliver the DSH services using the approved managed services approach.

The Contractor shall define an infrastructure that is consistent with the CMS TRA, the Medicaid Information Technology Architecture (MITA), and the Exchange Reference Architecture, for development, test, and production. The infrastructure shall be comprised of managed services, including, but not limited to, managed server services, managed network services, managed storage services, managed monitoring and reporting services, and managed security services. The Contractor shall support and operate the DSH systems running on the infrastructure, for the period of performance of this SOW. The infrastructure must be capable of scaling to meet the anticipated peak demands during open enrollment. The infrastructure must meet all data management safeguard requirements required for Personally Identifiable Information (PII), Personal Health Information (PHI), and FTI data.

The Contactor shall:

- Be responsible for developing and maintaining all interfaces specific to supporting the work required under this SOW and ensure all interfaces are compatible with the CMS secure managed services environment
- Ensure services provided as part of this SOW will not degrade the existing Service Level Agreements (SLA) for the CMS secure managed services environment
- Ensure services provided as part of this SOW will not degrade the security levels of the CMS secure managed services environment
- Ensure their delivered Software as-a Service (SaaS) products are capable of seamlessly integrating and supporting the IaaS and PaaS services
- Ensure the infrastructure is comprised of managed services, including, but not limited to, managed server services, managed network services, managed storage services, managed monitoring and reporting services, and managed security services.
- Ensure that peak volume does not overload the WWW and the data hub infrastructure
- Ensure the proposed infrastructure is consistent with the CMS Technical Reference Architecture (TRA), the Medicaid Information Technology Architecture (MITA), and the Exchange Reference Architecture.

The Contractor's proposed IT structure shall adhere strictly to CMS standards for connectivity, interfaces, security, and data transmission.

2.1.2 Data Management Requirements

The Contractor shall work in coordination and collaboration with the CMS Data Strategy and Governance Team to support the strategic data vision for the FEPS. As of the issuance of this SOW, issues include, but are not limited to, the following:

- Data format standards for internal processing (e.g., XML, X12, or other formats)
- Data transport formats, including formats based on NIEM
- Data translation approaches for Exchange interfaces
- Data translation approaches for federal interfaces
- Data model(s) for maintaining individual data, transaction audit data, federal agency partner data, etc.
- Data retention policy
- Recommendations for Data Use agreements and Data Exchange agreements with stakeholders.

Any information exchanges developed in this task which cross organizational boundaries must be consistent with existing health information exchange standards, including, specifically the latest National Information Exchange Model (NIEM) specifications and guidelines through the harmonization process. If there are not current NIEM specifications, the task must be consistent with the NIEM guidelines. Further information and training about development of NIEM conformant schemas and the use of NIEM specifications and guidelines is available at <http://www.niem.gov> via online and in-class courses. Also, various information, expertise, and reviews will be accessible through the appropriate Domain governance and NIEM-PMO committees.

The objective of Master Data Management (MDM) is to provide processes for collecting, aggregating, matching, consolidating, persisting and distributing data to ensure consistency and control for the use of information. The Contractor shall provide processes to ensure authoritative sources of master data are used by all services. The Contractor shall utilize data management standards and procedures for the definition, collection, and exchange of data elements, as outlined by the CMS Data Strategy and Governance Program. The Contractor shall provide a data dictionary that includes each data element attribute defined by the CMS Data Strategy and Governance Program.

The Contractor shall provide data validation and verification support to assist in ensuring the cleanliness and accuracy of the data being exchanged, and as input to sources within CMS. CMS anticipates implementing a metadata registry and repository based on the ISO/IEC 11179 standard.

To encourage seamless sharing, exchange and integration of tools and repositories, the Contractor shall support and adhere to the CMS metadata and data governance strategy and policies.

The Contractor shall ensure the data management approach is consistent with, interfaces with, and supports the CMS data analytic solution, known as Multidimensional Insurance Data Analytics System (MIDAS), which provides the following functions

- Centralizes and consolidates business logic into a metadata repository required to report and manage performance of the Affordable Care Act activities under CCIIO
- Integrates data from multiple operational source systems into a single, web-based information data store
- Provides access to standardized reporting, ad hoc queries, and data visualization
- Provides reporting on the data collected and maintained
- Provides robust analytic capabilities supporting trending and prediction from the data collected and maintained.

The Contractor shall present the benefit, risks, and implementation technologies recommended, and work with CMS to finalize the design. The Contractor shall develop, implement, test, and deliver the data models.

2.1.3 Data Security Requirements

As the Exchange and DSH may contain a variety of sensitive data, including PHI, PII, and IRS FTI described in Section 6103 of the Internal Revenue Code of 1986, the Contractor's solution design and implementation shall incorporate appropriate data security.

Federal agencies and their contractors must adhere to the Federal Information Security Management Act (FISMA) in developing, documenting, and implementing programs to provide security for federal government information and information systems. Both federal and state agencies may be "covered entities" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and thus, subject to these laws when handling PHI. These federal agencies and, in some instances, their contractors, are also subject to the Privacy Act of 1974, which places limitations on the collection, disclosure, and use of certain personal information, including PHI. The privacy provisions of the e-Government Act of 2002 require federal agencies to conduct privacy impact assessments (PIA) to assess risks and protections when collecting, maintaining, and disseminating PII. Finally, IRS data safeguard requirements, as outlined in IRS Publication 1075, dictate how to handle Section 6103 data.

The Contractor shall comply with any security requirements established by CMS to ensure proper and confidential handling of data and information. The Contractor shall refer to the HHS-OCIO Policy for Information Systems Security and Privacy, dated September 22, 2010. The Contractor shall also comply with the HHS Departmental Information Security Policies, which may be found at: <http://www.hhs.gov/ocio/policy/2007-0002.html> These documents implement relevant Federal laws, regulations, standards, and guidelines that provide a basis for the information security program at the Department.

The Contractor shall comply with any security and privacy requirements established by the IRS (e.g., Publication 1075 Tax Information Security Guidelines for Federal, State, and Local

Agencies) to ensure proper and confidential handling and storage of Section 6103 FTI data. In addition, any system handling tax information shall have audit trails that meet IRS standards.

The Contractor shall architect, design, implement, and test each component of the DSH to assure sufficient data security for all categories of sensitive data. The Contractor shall support CMS in conducting PIAs to assess risks and PII data protection.

2.1.4 Security Requirements and Authority to Operate

The Contractor shall provide security services in support of CMS, which shall include coordination among the CMS Chief Information Security Officer (CISO), business owners, and other stakeholders. The collection of CMS policies, procedures, standards, and guidelines are located on the CMS Information Security “Virtual Handbook” Web site at:

<http://www.cms.gov/InformationSecurity>.

The Contractor shall

- Provide certification documentation required by the CISO for compliance with CMS systems security requirements for the DSH infrastructure and delivered application system(s).

The Contractor shall build and deliver system(s) that are compliant with the CMS Acceptable Risk Safeguards and creating all artifacts necessary to receive an ATO in CFACTS; and the Contractor shall comply with the guidance in the Business Partner System Security Manual (BPSSM).

The Contractor shall provide the CMS ISSO all required documentation in the security certification of existing controls and compliance with CMS systems security requirements as described in the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36).

- Administer a security program

The Contractor shall comply with all CMS security program requirements as specified within the CMS Information Security (IS) “Virtual Handbook” (a collection of CMS policies, procedures, standards and guidelines that implements the CMS Information Security Program). The Virtual Handbook can be found at

www.cms.hhs.gov/informationsecurity.

The Contractor shall comply with all security controls outlined in the CMS Information Security (IS) Acceptable Risks and Safeguards (ARS) for “Moderate” systems. Appropriate references are the CMS IS ARS, Appendix B and the CMS System Security Levels by Information Type (located at www.cms.hhs.gov/informationSecurity in the Info Security Library).

The Contractor shall provide CMS with a security plan of action within 30 days of request and implement the plan within thirty (30) days of approval by CMS. The Contractor shall maintain any Corrective Action Plan (CAP) associated with deficiencies in the IS Program (e.g., those items identified during a FISMA audit). Moreover, the

Contractor shall comply with the guidance and requirements of the CMS Information Security Plan of Action & Milestones (POA&M) Procedure, which is located at www.cms.hhs.gov/InformationSecurity in the Info Security Library.

The Contractor shall comply with the CMS Policy for the Information Security Program (PISP) and all CMS methodologies, policies, standards, and procedures contained within the CMS PISP unless otherwise directed by CMS in writing.

The Contractor shall document its compliance with CMS security requirements and maintain such documentation in the System Security Plan as directed by CMS.

- Correct deficiencies in a timely manner

The Contractor shall perform work to correct any security deficiencies, conditions, weaknesses, findings, or gaps identified by all audits, reviews, evaluations, tests, and assessments, including but not limited to, Office of the Inspector General (OIG) audits, self-assessments, Contractor management review, security audits, and vulnerability assessments in a timely manner. Deviations or waivers regarding the inability to correct security deficiencies shall be coordinated and approved by CMS.

The Contractor shall develop, in conjunction with CMS, Corrective Action Plans (CAP) for all identified weaknesses, findings, gaps, or other deficiencies in accordance with IOM Pub. 100-17, Business Partner System Security Manual (BPSSM) or as otherwise directed by CMS.

The Contractor shall validate through post-hoc analysis and document that corrective actions have been implemented and demonstrated to be effective.

The Contractor shall provide CAPs and quarterly progress reports to CMS as directed by CMS.

- Attest to corrective actions

The Contractor shall provide, from all involved parties, attestation of initiated and completed corrective actions to CMS upon request.

- Support security review and verification

The Contractor shall comply with the CMS Security Assessment methodology, policies, standards, procedures, and guidelines for contractor facilities and systems (http://www.cms.hhs.gov/InformationSecurity/14_standards.asp#TopOfPage).

The Contractor shall conduct or undergo, as specifically selected and directed by CMS, an independent evaluation and test of its systems security program in accordance with CMS Reporting Standard for Information Security (IS) testing and adhere to the prescribed template

(http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage). The Contractor shall support CMS validation and accreditation of contractor systems and facilities in accordance with CMS Security Assessment methodology.

The Contractor shall provide annual certification in accordance with Security Assessment methodology that certifies it has examined the management, operational, and technical

controls for Contractor's systems supporting CMS and that it considers these controls adequate to meet CMS security standards and requirements.

2.1.5 Authentication and Authorization Requirements

All trading partners and stakeholders who interact with the DSH will authenticate themselves and be able to exercise certain actions based on their assigned authority.

The Contractor shall architect security models that meet the requirements for authenticating users and authorizing access for DSH services. The Contractor shall identify the benefits, risks, and implementation technologies recommended, and work with CMS to finalize the design(s). The Contractor shall develop, implement, test, and deliver the security model(s) for the DSH. The anticipated connections for the DSH are: up to 50 states, District of Columbia, US territories, up to 12 federal agencies, and up to 5,000 system administrators or other authorized individuals. The Contractor shall ensure that the A&A solution does not impact the overall throughput or performance of the DSH.

The HHS Certificate Authority will be the source of all security certificates.

2.1.6 Web Services

The Contractor shall employ Web Services as the implementation model to be used for implementing the systems in this SOW. For CMS, "Web Services" means interoperable, network-based application interactions between different systems, typically as components within a service-oriented architecture (SOA). The goal in using SOA-based Web Services is to maximize interoperability, through open standards, and reusability of service components. The components necessary to support a Web Services implementation include, but are not limited to, service visibility (often through a UDDI registry), an enterprise service bus (ESB), a rules engine, and a metadata catalog.

The Contractor shall architect a Web Services model that meets the requirements for use of services, routing of service requests and other messages, aggregating responses, tracking messages, and management of business rules.

The Contractor shall describe services using Web Services Description Language (WSDL). WSDL is a machine-readable description of a Web services interface. The Contractor and other service providers shall describe services using WSDL. The Contractor shall publish the WSDL to a UDDI directory of services to facilitate a consumer's ability to locate and determine how to communicate with that service. WSDL is used by the service consumer in identifying the requests and responses available from that service provider. Service consumers use the WSDL when to identify the requests and responses available from that service provider. WSDL is often used in combination with SOAP and an XML Schema to provide Web services over the Internet. A client program connecting to a Web service can read the WSDL file to determine what operations are available on the server. Any special data types used are embedded in the WSDL file in the form of XML Schema. The client can then use SOAP to actually call one of the operations listed in the WSDL file. It is envisioned that a UDDI will be the central service directory for federal exchange operations. The UDDI will register state level services and

federal agency services to allow coordinated use of these services between stakeholders in the FEPS environment.

ESB is an architectural concept that unifies, mediates, orchestrates, and connects shared services across systems. ESB is the platform by which the exposed services of business systems are made available for reuse by other business systems. An application will communicate via the bus, which acts as a message broker between applications. Such an approach has the primary advantage of reducing the number of point-to-point connections required to allow applications to communicate. This, in turn, makes impact analysis for major software changes simpler and more straightforward. By reducing the number of points-of-contact to a particular application, the process of adapting a system to changes in one of its components becomes easier.

For CMS, an ESB is an integration infrastructure component used to implement independent sharing of data and business processes. The collection of Business Service Pattern documents describe the use cases for the supporting services to be implemented in the DSH; additional service pattern documentation will be provided for the Exchange as it is developed.

Business rules can describe both the logic governing CMS front office mission and system execution-related automation processes and the logic governing back office support systems, applications, and other information technology. Business rules are also the most frequently changed SOA components because of new legislation, regulation, or changed front office processes. For ease of maintenance, it is thus necessary to separate these rules from technical services. For CMS, a business rules engine is an infrastructure component used to capture, define, maintain, and expose business rules for use by the systems under this requirement.

A Metadata Catalog (MC) provides the interface to a central site for publication and distributed management of metadata. The MC is a virtual "place" where participants at large can access and understand collections of metadata components, in which internal and external organizations and other stakeholders have invested. CMS expects the MC to evolve transparently and collaboratively as the interface to the service registry, since it is "managed" by representatives of a large, diverse, geographically distributed group of people and organizations. XML is the primary type of metadata for building the CMS. Any system that makes use of any XML should be visible, accessible, and understandable via the MC. The MC should facilitate the way communities of interest collaborate on, evolve, and transparently manage information-sharing "vocabularies" encoded in XML-based forms for both machine (WSDLs, schema, etc.) and human interfaces (e.g. web pages).

The Contractor shall present the benefits, risks, and implementation technologies recommended, and work with CMS to finalize the design of the Web Services infrastructure.

If the Contractor believes another approach will perform equally or better than an open source Web Services software suite or the components defined above, the Contractor may recommend such a solution. The Contractor shall then demonstrate that from performance, support, response, ease of development, connectivity, and cost considerations the alternative solution meets or exceeds all requirements in this SOW.

The Contractor shall develop, implement, test, and deliver the Web Services implementation for the systems in this SOW.

2.1.7 System Logs

Tracking of DSH transaction processing is critical to assure that CMS meets performance requirements and serves individuals in accordance with the mandates of the Affordable Care Act. Toward this end the Contractor shall:

- Design an appropriate level of transaction logging through all relevant components as necessary, e.g., the ESB and the DSH
- Design a data model sufficient to capture and store the logged information
- Implement the logging approach, that includes security auditing, monitoring, and review – subject to approval of the design(s) by CMS
- Assure a minimum impact on performance to allow efficient processing of anticipated peak loads

2.1.8 Roles and Responsibilities

The Contractor shall:

- Comply with CMS policies and standards and regulations applicable to CMS for information, information systems, personnel, physical and technical security, and change control
- Comply with Federal policies and standards with regard to data management and security, including those related to PII, PHI, and FTI
- Work collegially and share information with CMS staff and designated contractors. The Contractor shall work closely, collaboratively, and cooperatively with CMS staff from across the organization, contractor(s) supporting Healthcare.gov and Healthcare.Gov Plan Finder, contractors and staff from other government agencies, and contractors and staff from state organizations. The Contractor shall develop Joint Operation Agreements, as needed.
- Work collegially and share information with the states. The contractor shall work closely, collaboratively, and cooperatively with all states, as directed by CMS, to document activities and artifacts, and develop capabilities in such a way that they are easily shareable with the states.
- Conform to changes in laws, regulations and policies, as appropriate
- Work within the definition of the CMS Technical Reference Architecture (TRA), the Medicaid Information Technology Architecture (MITA), and the Exchange Reference Architecture.
- Provide timely creation, updates, maintenance and delivery of all appropriate project plans, project time and cost estimates, technical specifications, product documentation, and management reporting in a form/format that is acceptable to CMS for all projects and project activities

- Use existing CMS Change Management Systems and procedures. For example, requests for change (RFC) and standard requests forms (SRF) shall be used and submitted by the required deadlines to the appropriate review groups; and the Contractor shall await approval from the Government before implementation of the change requests. Examples of Government review groups and personnel include, but are not limited to: Technical Advisory Group (TAG), Change Control Boards (CCBs), CO, COTR, GTL, and the Office of Information Services (OIS).
- Recommend standards, industry best practices, and key performance indicators to the Government for configuration and operations; and implement the practices, once approved
- Acquire and manage all consumables necessary for the operations of the system, such as, but not limited to: backup media, labels, office supplies, and spare parts
- Use incident management and work ticketing/tracking systems
- Generate all documentation to ensure it is compliant with the requirements of Section 508 of the Rehabilitation Act
- Follow and implement eGov Accessibility and Usability guidelines, as appropriate
- Provide multi-lingual support for public, consumer-facing Internet portals, as appropriate
- Provide all scripts and software, including source code developed to support the task order to the Government; these artifacts become the property of the Government
- Ensure all software licenses are transferrable to the Government
- Make full use of the CMS Application Life Cycle Management (ALM) environment, including CollabNet, for storing, distributing, and communicating SOW products to the entire FEPS community

2.1.9 Hours of Operation

Primary Business hours for availability of Contractor resources to CMS and coverage during Operations and Maintenance are 9:00 AM Eastern to 6:00 PM Eastern time, Monday to Friday. On-call coverage is acceptable all other hours including weekends and holidays. When on-site services are necessary to resolve an outage or problem, arrival on-site is required within one (1) hour of the request. The Contractor shall provide CMS with a roster that includes contact information such as cell and home phone numbers.

Below represents the coverage requirements:

Coverage Type	Hours of Operation (HOO)
Onsite, at contractor location, during development	9AM-6PM EST, M-F
Onsite, at contractor location, during production, up to first 210 calendar days	8AM-8PM, EST, M-F, on call 24X7 as directed by CMS to address any outages of

following “go live” date	Exchange or Hub
Onsite, contractor location, following first 210 calendar days after “go live”	9AM-6PM EST, M-F
Onsite, CMS location(s) Bethesda or Woodlawn	As directed by CMS

2.1.10 Travel

All travel shall be as approved by the COTR prior to execution. The Contractor shall submit their request for travel at least twenty-five (25) days prior or at the direction of CMS to the onset of travel so there can be adequate time to obtain the best available airfare rates, etc. The Contractor shall make staff available to meet with CMS representatives and provide staff support for meetings and conferences, as requested. (For travel assumptions see Appendix C).

2.1.11 Connectivity

The Contractor shall be required to establish network connectivity to CMS. Contractors who have existing connectivity to CMS through circuits provided on CMSNet (formerly MDCN) may use those circuits to establish connectivity for their employees engaged in work on CMS tasks. All employee workstations communicating with the CMS network shall conform to the CMS standard desktop configuration and abide by the CMS Desktop Features and Specifications. All users shall comply with the HHS Rules of Behavior. Contractors who do not have connectivity to the CMS network or those who need to provide their employees with remote access to the CMS Baltimore Data Center (BDC) shall provide employees with CMS VPN based remote access over Internet broadband connections. The employee workstation configurations shall comply with the requirements defined in the current version of “VPN Process Instructions For CMS Contractors”. These requirements include a CMS standard desktop configuration, an RSA token supported by CMS, a currently patched operating system, current anti-virus software, and a current version of the VPN client used by CMS.

If the above connectivity solution does not meet the contractor’s requirements or needs, the contractor shall contact their assigned COTR and schedule a kick-off meeting with all parties to discuss the project and networking requirements. This kick-off meeting will also necessitate the COTR and/or GTLs to validate the contractor’s authority to gain access to the CMS Network prior to starting the process for acquiring direct circuit connectivity.

2.1.12 Earned Value

The Contractor shall have an Earned Value Management System (EVMS) that is flexible enough to support a range of EV requirements depending on the scope, budget, duration, and complexity of the project. The purpose of the EVMS is to

- a. Plan and control schedule and cost and to evaluate technical performance,

- b. Measure the value of completed tasks,
- c. Generate timely and reliable information reports on a monthly basis.

The Contractor shall provide documentation for the proposed EVMS that complies with the EVMS guidelines in the American National Standards Institute/Electronic Industry Alliance's (ANSI/EIA) Standard-748 and ESD SOW section J.3.2: Earned Value Management System.

If the Contractor proposes to use a system that does not meet the requirements of the ANSI/EIA Standard-748, the Contractor shall submit a comprehensive plan for compliance with the EVMS guidelines.

- a. The plan shall:
 - (1) Describe the EVMS that the Contractor intends to use in performance of the contract,
 - (2) Distinguish between the Contractor's existing management system and modifications proposed to meet the guidelines,
 - (3) Describe the management system and its application in terms of the EVMS guidelines,
 - (4) Describe the proposed procedure for administration of the guidelines, as applied to sub-contractors,
 - (5) Provide documentation describing the process and results of any third-party or self-evaluation of the system's compliance with the EVMS guidelines.
- b. The Contractor shall provide information and assistance as required by the Contracting Officer to support review of the plan.

The Contractor shall identify the major sub-contractors, or major sub-contracted effort if major sub-contractors have not been selected, planned for application of the guidelines. The Contractor and CMS shall agree to sub-contractors selected for application of the EVMS guidelines.

2.1.12.1 Integrated Baseline Review (IBR)

The Contractor shall plan and take part in an IBR. The objective of the IBR is for CMS and the Contractor to jointly assess the Contractor's Performance Measurement Baseline to ensure complete coverage of the SOW, logical scheduling of the work activities, adequacy of resources, and identification of risks. In the IBR, the Contractor shall:

- a. Verify that the cost, schedule, and technical plans are integrated,
- b. Demonstrate that there is a logical sequence of effort consistent with the contract schedule,
- c. Demonstrate the validity of the allocated cost accounts and budgets, both in terms of total resources and scheduling,
- d. Support CMS's technical assessment of the earned value methods that the Contractor is using to measure progress to assure that objective and meaningful performance shall be provided,
- e. Support CMS's technical assessment of the SDMP, project standards, and procedures for software development,
- f. Keep management informed about project status, directions being taken, technical agreements reached, and overall status of evolving software products,

- g. Identify and resolve management-level issues and risks,
- h. Obtain commitments and CMS approvals needed for timely accomplishment of the project.

2.2 Task Order Management

2.2.1 Management and Reporting

Management activities include, but are not limited to: project planning, resource management, quality assurance, risk management, status and problem reporting, project management of activities involving user impact, such as pilots and migrations, and administrative support.

The Contractor shall create, maintain and provide all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to CMS, and made readily available to appropriate CMS staff. The project work plan shall be revised as needed throughout the period of performance. The Contractor shall provide all architectural, design and performance documentation.

The Contractor's Project Manager, or a designated representative, shall attend (in person) regularly scheduled contract review meetings for the purpose of status updates, progress reports, and problem resolutions. Meetings shall be held at a location of the Government's choosing in the Washington DC Metropolitan area. With the Government's prior approval, attendance at these meetings can be via phone or teleconference.

The Contractor shall provide a Dashboard Status and Budget Tracking Reporting template; the Contractor shall make amendments to the template to reflect additional information regarding project status and/or budget at the request of the COTR.

The Contractor shall provide the COTR and Government Task Leads (GTL) with a written response within two (2) business days to any proposed changes initiated by CMS. Responses from the Contractor shall contain the following:

- Project Timeline Assessment
- Risk Assessment
- Cost estimate representing any additional funding required from the Project Team

The Contractor shall provide monthly status reports to ensure that the expenditure of resources is consistent with and will lead toward successful completion of all tasks within projected cost and schedule limitations. Monthly status reports shall detail progress made during the prior month, progress expected during the next month, resources expended, any significant problems or issues encountered, recommended actions to resolve identified problems, and any variances from the proposed schedule and discussed during a monthly briefing. In coordination with CMS and pending the content approval of the COTR, the monthly status reports may take the form of a "PowerPoint briefing deck" to expedite the identification and resolution of issues.

Earned Value Management (EVM), as described in the ESD Contract, is required for all design, development, implementation, testing, and delivery activities. The Contractor shall report on EVM on a schedule to be determined by the Contractor and CMS that meets the flexibility and response of an agile development process.

The Contractor shall assist CMS in building customer relationships, identifying business needs, and controlling demand through CMS business liaison activities.

2.2.2 Exchange Life Cycle Management

The Contractor shall follow the CMS ELC, including the ordering of phases, stage gates, and other reviews. The Contractor shall supply all appropriate documentation to support the stage gate reviews shall be supplied by the Contractor at least one (1) week prior to the review.

To support an agile development process, the Contractor shall plan for multiple reviews of each type, as appropriate, to support the life-cycle activities for each agile sprint increment of work. No effort on the next increment of work will be performed until stage gate review approval is obtained.

Listed below are the requisite life-cycle reviews and products that will accompany each increment, as appropriate. CMS reserves the right to define and request additional or replacement products for each review. CMS reserves the right to hold fewer reviews for any agile sprint increment of work.

Project Startup Reviews (PSR)

Products: Concept of Operations, Risk Analysis, Project Management Plan, Alternatives Analysis, Scope Definition, Performance Measures, briefings/presentations to OIS, level of effort (LOE) estimate to achieve the Architecture Review

Architecture Reviews (AR)

Products: Business Process Models, Architectural diagrams, briefings/presentations to CMS, LOE estimate to achieve the Project Baseline Review

Project Baseline Reviews (PBR)

Products: Project Management Plan, Project Schedule, Project Process Agreement, Release Plan, Privacy Impact Assessment, briefings/presentations to OIS, LOE estimate to achieve the Preliminary Design Review

Preliminary Design Review (PDR)

Products: Requirements Document, Information Security Risk Assessment, System Security Plan, Test Plan(s) and Traceability Matrix, Logical Data Model, Technical Architecture Diagrams (software architecture, network, infrastructure, security, etc.), briefings/presentations to OIS, LOE estimate to achieve the Detailed Design Review

Detailed Design Review (DDR)

Products: System Requirements Document, System Design Document, Interface Control Document(s), Database Design Document(s), Physical Data Model, Data Management Plan,

Data Conversion Plan, briefings/presentations to OIS, LOE estimate to achieve the Final Detailed Design Review

Final Detailed Design Review (FDDR)

Products: See DDR products, LOE estimate to achieve the Pre-Operational Readiness Review
Pre-Operational Readiness Review (PORR)

Products: Test Plan and Test Case Specifications, Contingency/Recovery Plan, Implementation Plan, User Manuals, Operations & Maintenance Manual, Training Plan and Materials, System Security Plan, Information Security Risk Assessment, Integration Testing results, End-to-End Testing results, Test Summary Report, Defect Reports, Security Testing results, briefings/presentations to OIS, LOE estimate to achieve the Operational Readiness Review

Operational Readiness Review (ORR)

Products: See PORR products, Project Completion Report, SLAs, Privacy Impact Assessment, Plan of Action & Milestones (POA&M), Authority to Operate, LOE estimate to support Operations and Maintenance

For an explanation of each product, please reference the following CMS ILC framework:
https://www.cms.gov/ILCReviews/01_Overview.asp

For examples of product templates, please refer to the following:

<http://www3.cms.gov/SystemLifecycleFramework/Tmpl/list.asp#TopOfPage>

2.2.3 Change Management

The Contractor shall be proactive in notifying CMS of any developing situation that may impact operations, system interoperability, scheduled deadlines, the states and federal agencies, or any other contractual issue. In the case of a known impending problem, the Contractor shall be forthcoming with CMS to address the risks and to identify mitigation strategies. The Contractor shall identify, document, track, and correct issues that impart risk on service delivery. In addition, the Contractor shall recognize recurring problems and inefficiencies, address procedural issues, and contain, mitigate, or reduce the impact of problems that occur. The Contractor shall provide assistance to the Government in explanation of reports on problem resolution and root causes of problems.

The Contractor shall hold regular weekly meetings to review pending and past changes, problems and actions taken within the prior week, or actions that will occur within the next four (4) weeks. One (1) day prior to the weekly meeting, the Contractor shall, unless otherwise notified by the COTR, provide the COTR and GTL with status reports.

The Contractor's Project Manager and the Contractor's appropriate technical experts shall identify and present any improvements, enhancements and/or changes being made to the appropriate change management and advisory boards, and shall receive approval from the authorized and appropriate board before implementation.

2.2.4 Quality Control

The Contractor shall provide and maintain a Quality Control Plan that defines the Contractor's approach, processes, and procedures for ensuring the quality and reliability of its products and services.

The Contractor shall develop and deliver a Quality Assurance Surveillance Plan (QASP) within 45 days after contract award. The QASP shall provide a systematic and structured process for the Government to evaluate the services the Contractor will provide, including, but not limited to, processes, methods, metrics, customer satisfaction surveys, service level agreements, and operational level agreements. The results of the applying the QASP will document the Contractor's performance on this effort.

The Contractor shall present interim in-process reviews and shall support technical quality audits by CMS.

The Contractor shall provide all testing and quality control processes necessary to ensure its products and services meet the requirements of the Enterprise System Development (ESD) Indefinite Delivery Indefinite Quantity (IDIQ) and this task order.

2.2.5 Risk Management

The Contractor shall develop and maintain a Risk Management Plan (RMP). The plan should, at a minimum, identify all risks, categories, impact, priority, mitigation response/strategy, and status and include a risk assessment matrix. The Contractor shall provide the draft Risk Management Plan to the COTR thirty (30) days after award for the Government to review. The Contractor shall incorporate any Government comments and provide the final Risk Management Plan to the COTR within five (5) working days. The document is a living document, and therefore, the Contractor shall update the plan, as necessary.

2.2.6 License Management

In conjunction with acquiring the required infrastructure services from the CMS Cloud Service provider, Terremark, the Contractor shall develop, document, and maintain software license management procedures that meet CMS requirements and adhere to CMS-defined policies.

The Contractor shall leverage existing CMS resources and assets where possible, utilizing a previous software agreements, licenses, or enterprise services/tools.

The Contractor shall develop and maintain inventory of all software licenses. The Contractor shall manage and maintain (e.g., monitor, track status, verify, audit, perform contract compliance, renew, reassign) all software licenses and media through the software license life cycle.

The Contractor shall coordinate software license and maintenance agreement reviews and warranties, allowing at least 180 days for renewal activities before expiration.

The Contractor shall provide CMS with reports and recommendations to use in making software acquisition and discontinuance decisions.

The Contractor shall provide recommendations to purchase additional license capacity, and shall recommend alternatives, or curtail usage where necessary and appropriate, to restore or continue to maintain license compliance.

2.2.7 Joint Operating Agreements

The Infrastructure Services Contractor (see Section 2.1.1) is tasked with providing Infrastructure-as-a-Service that includes all components necessary to stand up, execute, and maintain development, test, and production sites.

The Contractor shall develop a Joint Operating Agreement (JOA) with the Infrastructure Contractor. The purpose of the agreement is to facilitate a close working relationship between the two contractors and establish an understanding of the responsibilities of each to the overall DSH project. Success on this project requires a much closer working relationship than is common between separate contracts. The agreement does not replace or change the requirements of the Statements of Work each contractor is operating under. CMS approval is required for the agreement. The COTR must approve budget changes that result from a transition or change in scope before any work is performed.

Additional JOAs may be necessary with additional CMS contactors in the future. The Contractor shall develop any additional JOAs to the same level of rigor.

2.3 Delivery of Data Services Hub

The Contractor shall perform all tasks required to deliver the DSH information broker services and the associated common services. As the scope of the services will evolve over the life of this contract, the effort will be performed as a series of work activities starting with eligibility verification services. Six (6) functional areas have been identified as sufficient to encompass all DSH requirements: Eligibility & Enrollment, Plan Management, Financial Management, Oversight, Communications, and Customer Service.

The DSH is a single interface to the states and federal partners to provide information exchange and business functionality in support of Exchange operations. The DSH will streamline and simplify the information flows between states and federal agencies.

The Contractor shall build the DSH to perform the following tasks in subsections 2.3.1 through 2.3.8, and as described in the eight (8) work activities described in subsection 2.4.

2.3.1 Eligibility Verification and Enrollment Services

Eligibility verification services include DSH services necessary to verify individual's eligibility for health insurance through the Exchange. These services include, but are not limited to, income verification, citizenship verification, lawful presence verification, incarceration status verification, and eligibility for other public minimum essential coverage or employee sponsored minimum essential coverage. The eligibility verification services:

- Present DSH interfaces for use by the Exchanges
- Present federal interfaces for connecting to federal partners

- Add data to the DSH data model
- Perform business service processing.

Enrollment services include services necessary to allow an eligible individual to view, compare, select and enroll in a health plan or service delivery options available through the Exchange, Medicaid, CHIP, a Basic Health Plan, or a QHP.

The referenced E&E Blueprint documents (including the E&E Supplement, E&E Process Models, and E&E Data Capture workbook) provide a detailed set of business requirements defining the necessary DSH supporting services. The products from the CMS Requirements Contractor will provide additional business level requirements, business rules, and business process definition.

The Contractor shall use the E&E blueprinting information and the products from the Requirements Contractor to finalize the verification services technical and system requirements to develop and deliver the E&E services. The Contractor shall present the requirements, design, and implementation approach to CMS for approval. The Contractor shall develop, implement, test, and deliver the verification services using the Web Services model for the DSH.

E&E Hub Services

The following table lists the known E&E Hub services. After contract award, CMS will provide an updated list of services. High, medium, and low refer to the relative complexity of the supporting business service.

Business Process Name	Supporting Services			
	Total	High	Med	Low
BP-EE:10 Prepare / Update Individual Eligibility Application	0			
BP-EE:11 Verify Individual Eligibility Application Information	3		1	2
BP-EE:12 Determine Individual Eligibility	2	1	1	
BP-EE:13 Enroll Individual in Qualified Health Plan	3		3	
BP-EE:14 Disenroll Individual from Qualified Health Plan	1		1	
BP-EE:15 Renew Individual Eligibility and Enrollment	9	1	6	2
BP-EE:16 Appeal Exchange Eligibility Decision	1		1	
BP-EE:20 Prepare / Update Individual Exemption Application	0			
BP-EE:21 Verify Individual Exemption Application Information	0			
BP-EE:22 Determine Individual Exemption Eligibility	2		2	
BP-EE:25 Renew Individual Exemption Eligibility	2		2	
BP-EE:30 Prepare / Update Employer Eligibility Application	0			
BP-EE:31 Verify Employer Eligibility Application Information	0			
BP-EE:32 Determine Employer Eligibility for Participation	1		1	
BP-EE:33 Determine Employer Contribution	1		1	
BP-EE:34 Terminate Employer Participation	1		1	

Business Process Name	Supporting Services			
	Total	High	Med	Low
BP-EE:35 Renew Employer Participation	3		3	
BP-EE:36 Appeal SHOP Eligibility Decision	1		1	
BP-EE:40 Prepare / Update Employee Eligibility Application	0			
BP-EE:41 Verify Employee Eligibility Application Information	0			
BP-EE:42 Determine Employee Eligibility	0			
BP-EE:43 Enroll Employee in Qualified Health Plan	3		3	
BP-EE:44 Disenroll Employee from Qualified Health Plan	1		1	
BP-EE:45 Renew Employee Eligibility and Enrollment	4		4	

Finding the Descriptions of Business Processes and Supporting Services

Each business process and business supporting service listed above is described in the *Eligibility and Enrollment – Exchange Business Architecture Supplement* listed in the reference documents in subsection 1.4. The Business Process descriptions are found in Table 4, section 3.2 of the supplement and the Supporting Business Services descriptions are found in subsection 5.1.2 of the supplement.

For example, business process *BP-EE:11 Verify Individual Eligibility Application Information* is described in Table 4 in section 3.2 on page 15 as follows:

Verifies the information provided on the application with data needed to determine eligibility. This process includes verifying the applicant’s citizenship, immigration status, incarceration status, and other relevant checks.

Subsection 5.2.2 shows the list of supporting business services for BP-EE:11. Table 17 in section 5.2.2 shows the list of supporting business services for the BP-EE:11 business process. The three services with the “CMS” tag: (1) Verify Lawful Presence, (2) Review Documentation to Verify Lawful Presence, and (3) Verify Household Income are the supporting business services assigned to the DSH.

The descriptions of all supporting business services are found in Table 15 in subsection 5.1.2. For example, the description for *SBS-CMS:08 – Verify Household Income* is:

In response to a request from an Exchange, CMS obtains information from an individual’s tax return regarding household MAGI from the IRS. This utilizes the supporting services from IRS that will calculate the individual’s MAGI based on his/her tax return.

This function may be called as an individual DSH service and/or may be part of a composite verification service call from the Exchange to the DSH. In addition, it is possible that some of the business logic defined in the business process flow as being Exchange-specific processing may be moved to the DSH to simplify the implementation necessary within each Exchange. These are some of the technical decisions that will be made as part of the system requirements capture during discussions between CMS, the states, and the Contractor.

2.3.2 Plan Management Services

Plan management services include the services necessary to acquire, certify and manage issuers offering Qualified Health Plans (QHPs) through an exchange. The services include, but are not limited to: certifying/recertifying/decertifying plans offered by issuers as QHPs; establishing agreements with issuers to offer QHPs; monitoring agreements with issuers to ensure compliance and take corrective action when necessary; terminating agreements with issuers, processing changes in plan enrollment availability, and maintaining the operational data associated with issuers and plans.

The Contractor shall use the PM blueprinting information and the products from the requirements contractor to finalize the services technical and system requirements to develop and deliver the PM services. The Contractor shall present the requirements, design, and implementation approach to CMS. The Contractor shall develop, implement, test, and deliver the PM services using the web services model for the DSH.

Plan Management Services

The following table lists the Plan Management Hub services. After contract award, CMS will provide an updated list of services. High, medium, and low refer to the relative complexity of the supporting business service.

Business Process Name	Supporting Services			
	Total	High	Med	Low
BP-PM:01 Establish Issuer and Plan Initial Certification and Agreement	3	2	1	
BP-PM:02 Monitor Issuer and Plan Certification Compliance	3	2	1	
BP-PM:03 Establish Issuer and Plan Renewal and Recertification	2	2		
BP-PM:04 Maintain Operational Data	1	1		
BP-PM:05 Process Change in Plan Enrollment Availability	1		1	
BP-PM:06 Review Rate Increase Justifications	1	1		

The descriptions of the Plan Management business processes and supporting business services can be found in the *Plan Management – Exchange Business Architecture Supplement* listed in the reference documents in subsection 1.4.

2.3.3 Financial Management Services

Financial management services include the services necessary to spread risk among issuers and to accomplish financial interactions with issuers. The risk spreading services include, but are not limited to: payment calculation for reinsurance, risk adjustment and risk corridors, along with required data collection to support these services. The issuer financial transactions include: SHOP and Individual Premium (optional) processing, Advanced Premium Tax Credit (APTC) and Cost Sharing Reduction (CSR), Reinsurance, Risk Adjustment and Risk Corridors payments

The Contractor shall use the FM blueprinting information and the products from the requirements contractor to finalize the services technical and system requirements to develop and deliver the FM services. The Contractor shall present the requirements, design, and

implementation approach to CMS. The Contractor shall develop, implement, test, and deliver the FM services using the web services model for the DSH.

Financial Management Services

The following table lists the Financial Management Hub services. After contract award, CMS will provide an updated list of services. High, medium, and low refer to the relative complexity of the supporting business service.

Business Process Name	Supporting Services			
	Total	High	Med	Low
BP-FM:01 Plan Assessment for State Exchanges	0		0	
BP-FM:02 Reinsurance Contributions	2		2	
BP-FM:03 Reinsurance Contribution Verification	0		0	
BP-FM:04 Reinsurance Payment	2		2	
BP-FM:05 Non-Exchange Enrollee/Rate Data Collection	2		2	
BP-FM:06 Claims/Encounter Data Collection	0		0	
BP-FM:07 Risk Adjustment Calculation	0		0	
BP-FM:08 Risk Adjustment Payment	0		0	
BP-FM:09 Risk Corridors	0		0	
BP-FM:10 Determine Issuer APTC and CSRs (No Offset)	6		6	
BP-FM:11 CSR Reconciliation	9		9	
BP-FM:12 SHOP Premium Aggregation	0		0	
BP-FM:13 SHOP Reconciliation	0		0	
BP-FM:14 State Options to Collect Premiums in the Exchange	0		0	

2.3.4 Remaining Functional DSH Services

The details of the business processes and flows for the following Exchange functional areas will be provided post award: Oversight, Communication, and Customer service.

Exchange Functional Area - Oversight: Services for Oversight include the services necessary to define, implement, manage, and measure the performance of both Federal oversight of Exchange operations, and Exchange management and operations.

Exchange Functional Area - Communication: Services for Communication include the services necessary to define, implement, manage, and measure the effectiveness of communications, education and outreach strategies, both within an Exchange, and also when these strategies occur in concert with HHS and/or other Exchanges.

Exchange Functional Area - Customer Service: Services for Customer Service include the services necessary to manage Exchange responses to information requests and requests for service from consumers, employers, 3rd parties (navigators, agents, brokers) and issuers. Customer Service includes the creation and management of multi-channel response mechanisms

(e.g., phone, web, paper, and face-to-face) and the efficient distribution/management of requests across channels. Finally, Customer Service includes the creation and management of web-based consumer tools.

2.3.5 Comprehensive Testing

The Contractor shall perform testing and validation of all major and minor releases prior to completing implementation. Testing shall include unit and integration testing of all functional deliverables – both integration testing internal to the DSH and externally with DSH stakeholders (e.g. IRS). The Contractor shall follow the CMS Testing Framework documented in <http://www.cms.gov/SystemLifecycleFramework/Downloads/CMSTestingFrameworkOverview.pdf>

The Contractor shall define, create, manage, update/reload, and administer test data sufficient to ensure successful results for all test activities.

The Contractor shall conduct the following verification and tests:

- Unit tests: verification of individual hardware or software units or groups of related items prior to integration of those items; and
- Integration tests: verification that the assembled individual components functions properly as a system

The Contractor shall conduct system testing at the hosting environment. System testing includes the following activities to ensure that the application meets all requirements and expectations:

- Functional tests: verification that the system meets documented requirements
- Interface tests: verification that the system interacts with external applications according to specifications
- Regression tests: verification that changes do not adversely affect existing functionality
- Parallel tests: comparison of the results of a new application baseline against the results of a production version to ensure that the new version functions as intended
- Performance and load tests: activities to determine how the system performs under a particular workload to demonstrate that the system meets performance criteria. This includes developing load scripts for stress testing.

The Contractor shall collaborate with CMS and designated CMS contractors for functional validation. Functional validation includes the following:

- Activities to ensure that the application meets the customer needs and accomplishes the intended purpose
- User Acceptance Testing (UAT) that will allow end users to validate that the system delivers the requested functionality and will accomplish its business objectives.

The Contractor shall document test cases based on test data provided by CMS. The Contractor shall collaborate with CMS to ensure development of adequate test cases. The Contractor shall establish test cases (in terms of inputs, expected results, and evaluation criteria), test procedures,

and test data for testing the software. The Contractor shall deliver a draft and a final Test Case Specification.

2.3.6 Nationwide Service Integration Testing

The Contractor shall perform unit, system, and integration testing during the development and validation of each DSH service. In addition, beginning on or about January 1, 2013, nationwide testing will begin for integration of existing state systems, Exchanges, the DSH, and federal agencies. The Contractor shall be responsible for end-to-end integration testing, including issuing test reports, to validate the effectiveness of the nationwide FEPS.

2.3.7 Service Governance

The Contractor shall provide governance services throughout the period of performance of this effort. Governance services include, but are not limited to configuration management, release management, document/deliverable management, risk management, and quality control.

Transaction Capability Governance oversees the management of transaction formatting. The Contractor shall work with CMS to ensure that all transaction formats, mechanisms, and integration points are standardized to maximize data interoperability.

The Contractor shall document the change management and other governance processes and procedures used.

2.3.8 Training

As part of the DSH development and implementation, the Contractor shall develop and deliver a Training Plan. The plan shall include conducting training for CMS personnel, other CMS contractors, and any other participants as identified by CMS. The plan shall include all aspects of the system to ensure collective and consistent knowledge of process execution, including access and usage of the proposed solution.

The Training Plan shall include at a minimum, the following information:

- Steps in using the proposed solution
- How training will be provided
- Maximum number of people that can be trained at one time
- Type of training environment required, including equipment required
- Skill set of trainers
- Type of training materials to be provided
- Identification of trainer(s), if available.

The Contractor shall conduct training for CMS, and any other contractor designated by CMS. Moreover, the Contractor shall create any supporting artifacts/documentation required to support the delivery of the training. At a minimum, the following information shall be provided as appropriate: handouts, slides, guides, and manuals.

The Contractor shall develop, update, and maintain the User and Operator Training Materials. The Contractor shall create and maintain User Manuals. User Manuals shall contain the information and references necessary for the user to learn, navigate, and use the solution. The User Manuals shall be updated with changes as a result of system releases that occur during the period of performance of this effort. User Manuals shall include, but are not limited to, the following:

- Table of Contents
- Step-by-step instructions and help references
- Descriptions of user roles, sample user screens and reports, a menu hierarchy, diagrams, and definitions of all fields
- All error messages and corrective action instructions
- Separately bound quick-reference guide (or page). If appropriate to the software, this guide shall provide or reference a quick-reference card or page for using the software. This quick-reference guide shall summarize, as applicable, frequently used function keys, control sequences, formats, commands, or other aspects of software use.
- Answers to Frequently Asked Questions (FAQs)
- Glossary.

The Contractor shall develop a Development Guide for the states (and other stakeholders, as necessary) that contains the technical information necessary to guide the states in their development of interfaces to DSH services. This guide will define the protocols and payloads of the designed transmission mechanism, and recommended approaches for defining, creating, and testing the DSH service interfaces to all stakeholders.

2.4 Work Activities

The work activities described below constitute the actual tasking to be completed under this Task Order to implement the requirements for the DSH.

Upon award of the task order, the Contractor shall proceed with the first two work activities, the Program Startup Review and the design of the platform infrastructure. The Contractor shall obtain approval of the PSR, of the platform design and architecture, and approval of the level of effort (LOE) definitions to proceed with the next work segment.

Each subsequent work activity will follow the same approach. That is, there will be a defined activity, such as Eligibility & Enrollment service/function design, development, and implementation that follows the CMS ELC and the stage gate reviews. Continuation of contract activities requires CMS approval of the products of each work activity and the LOE plan for the next work activity at each stage gate review. No subsequent work shall begin until successful completion of each gate review.

2.4.1 Work Activity 1 – Program Startup Review

The first work activity to be performed under this Task Order is the Program Startup Review that represents the kickoff of the Task Order.

Within five (5) business days of the award of the task order, the Contractor shall conduct an orientation meeting and briefing for CMS. The completion of this briefing shall result in (but is not limited to) the following:

- Management Approach – To include project assumptions and constraints and the overall approach to project management.
- Project Work Plan – To include the comprehensive methodology for implementing the DSH in a phased approach and detailed project schedule. The project plan shall include work activity descriptions, work activity dependencies, work activity durations, milestones, resources and deliverables for each near- and long-term phase, and identification of the critical path.
- Staffing Approach – To include the roles, responsibilities, and allocations of each resource assigned to the effort; the approach to transitioning staff between each life cycle phase; and the approach to estimating levels of resources required.
- Communication Approach – To include the methodology for communicating status, issues, and risks to CMS stakeholders.
- Risk Management Approach – To include the process, methods, tools, and resources that will be applied to the project for risk management. Describe how risks will be identified and analyzed, the basis for prioritizing risks, how risk responses will be developed and implemented, and how the success of those responses will be measured.
- Configuration Management Approach – To include the responsibilities and authorities for accomplishing identified configuration management activities performed during the project's life cycle and coordination with other project activities.

This Program Startup Review will constitute the PSR for the Task Order. Approval of the PSR is required prior to beginning work on subsequent work activities.

2.4.2 Work Activity 2 – Platform Architecture

The second work activity to be performed under the task order is the design of the infrastructure platform and software component platform necessary to support the development, testing, and production of the DSH at Terremark.

The Contractor shall produce a hardware architecture, including but not limited to managed servers, managed storage, and managed bandwidth, and a software component architecture consisting of the recommended open source tools necessary to provide a web services platform for developing, testing, and hosting the DSH.

At contract award, CMS will provide any existing hardened baseline operating system images for instantiating servers at Terremark. The Contractor shall develop and provide to CMS any operating system images, system installation scripts, and configuration guides for products recommended for the DSH. The Contractor shall ensure that these images, scripts, and guides

create installed components and environments that meet all CMS and IRS security controls as described in subsections 2.1.3 and 2.1.4. The Contractor shall work with Terremark, at CMS direction, to validate the recommended approach.

The Contractor shall provide diagrams, descriptions, tool product recommendations, an integration plan and schedule, the benefits and risks of the approach, and an LOE estimate of the Contractor hours by labor category for the implementation of the approach. The Contractor shall schedule and plan an Architecture Review stage gate review to gain approval of the recommended approach.

2.4.3 Work Activity 3 – Plan Management Services

The third work activity to be performed under the task order is the design, development, implementation, and delivery of the Plan Management Hub Services as described in subsection 2.3.2.

The Contractor shall refine the business process models, requirements documents, and create architectural diagrams sufficient to fully describe the Plan Management business area. The Contractor shall provide diagrams, descriptions, the benefits and risks encountered, assumptions made, and an LOE estimate of the Contractor hours by labor category for the Program Baseline Review for this activity. The Contractor shall schedule and plan an Architecture Review stage gate review to gain approval of the recommended approach.

2.4.4 Work Activity 4 – E&E Services

The fourth work activity to be performed under the task order is the design, development, implementation, and delivery of the Eligibility and Enrollment Hub Services as described in subsection 2.3.1.

The Contractor shall refine the business process models, requirements documents, and create architectural diagrams sufficient to fully describe the E&E business area. The Contractor shall provide diagrams, descriptions, the benefits and risks encountered, assumptions made, and an LOE estimate of the Contractor hours by labor category for the PBR for this activity. The Contractor shall schedule and plan an Architecture Review stage gate review to gain approval of the recommended approach.

2.4.5 Work Activity 4 – Plan Management Services

The fourth work activity to be performed under the task order is the design, development, implementation, and delivery of the Plan Management Hub Services as described in subsection 2.3.2.

The Contractor shall refine the business process models, requirements documents, and create architectural diagrams sufficient to fully describe the Plan Management business area. The Contractor shall provide diagrams, descriptions, the benefits and risks encountered, assumptions made, and an LOE estimate of the Contractor hours by labor category for the Program Baseline Review for this activity. The Contractor shall schedule and plan an Architecture Review stage gate review to gain approval of the recommended approach.

2.4.6 Work Activity 5 – Financial Management Services

The fifth work activity to be performed under the task order is the design, development, implementation, and delivery of the Financial Management Hub Services as described in subsection 2.3.3.

2.4.7 Work Activity 6 – Oversight Services

The sixth work activity to be performed under the task order is the design, development, implementation, and delivery of the Oversight Hub Services. Details on these services will be provided post award.

2.4.8 Work Activity 7 – Customer Service

The seventh work activity to be performed under the task order is the design, development, implementation, and delivery of the Customer Service Hub Services. Details on these services will be provided post award.

2.4.9 Work Activity 8 – Communications Services

The eighth work activity to be performed under the task order is the design, development, implementation, and delivery of the Communications Hub Services. Details on these services will be provided post award.

2.5 Regional Technical Support

As described in subsection 1.1, states will likely require some level of technical support during the course of the development of Exchanges and the interactions required with the DSH. The Contractor shall propose a plan to provide qualified, senior-level technical architects regionally throughout the United States so as to minimize travel expenses. These technical architects shall have experience with state Medicaid systems, commercial insurance systems, or related federal health systems. The required technical support includes, but will not be limited to: stage gate reviews, particularly architecture reviews; design reviews; implementation and test plan reviews; and other related application life-cycle activities.

2.6 Operations and Maintenance

Once CMS has accepted and deemed DSH to be fully operational, the Contractor shall provide operations and maintenance (O&M) support of the DSH systems for the period of performance of this effort. O&M includes, but is not limited to daily operations, systems change management, systems maintenance, second and third-level help desk support, and monitoring and oversight support of the DSH systems. During key operational phases that occur during the performance of this effort, such as open enrollment, the Contractor shall provide 24x7 support for each of these services.

3. General Requirements

3.1 Section 508 – Accessibility of Electronic and Information Technology

- (a) This task order is subject to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by the workforce Investment Act of 1998 (P.L. 105-220). Specifically, subsection 508(a)(1) requires that when the Federal Government procures Electronic and Information Technology (EIT), the EIT must allow Federal employees and individuals of the public with disabilities comparable access to and use of information and data that is provided to Federal employees and individuals of the public without disabilities.
- (b) The EIT accessibility standards at 36 CFR Part 1194 were developed by the Architectural and Transportation Barriers Compliance Board ("Access Board") and apply to contracts and task/delivery orders, awarded under indefinite quantity contracts on or after June 25, 2001.
- (c) Each Electronic and Information Technology (EIT) product or service furnished under this contract shall comply with the Electronic and Information Technology Accessibility Standards (36 CFR 1194), as specified in the contract, as a minimum. If the Contracting Officer determines any furnished product or service is not in compliance with the contract, the Contracting Officer will promptly inform the Contractor in writing. The Contractor shall, without charge to the Government, repair or replace the non-compliant products or services within the period of time to be specified by the Government in writing. If such repair or replacement is not completed within the time specified, the Government shall have the following recourses:
1. Cancellation of the contract, delivery or task order, purchase or line item without termination liabilities; or
 2. In the case of custom Electronic and Information Technology (EIT) being developed by a contractor for the Government, the Government shall have the right to have any necessary changes made or repairs performed by itself or by another firm for the noncompliant EIT, with the contractor liable for reimbursement to the Government for any expenses incurred thereby.
- (d) The contractor must ensure that all EIT products that are less than fully compliant with the accessibility standards are provided pursuant to extensive market research and are the most current compliant products or services available to satisfy the contract requirements.
- (e) For every EIT product or service accepted under this contact by the Government that does not comply with 36 CFR 1194, the contractor shall, at the discretion of the Government, make every effort to replace or upgrade it with a compliant equivalent product or service, if commercially available and cost neutral, on either a contract specified refresh cycle for the product or service, or on a contract effective option/renewal date; whichever shall occur first.

Section 508 Compliance for Communications

The Contractor shall comply with the standards, policies, and procedures below. In the event of conflicts between the referenced documents and this **SOW, PWS, or TO**, the **SOW, PWS, or TO** shall take precedence.

Rehabilitation Act, Section 508 Accessibility Standards

1. 29 U.S.C. 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (508 Standards)
3. www.access-board.gov/sec508/508standards.htm (508 standards)
4. FAR 39.2 (Section 508)
5. CMS/HHS Standards, policies and procedures (Section 508)

In addition, all contract deliverables are subject to these 508 standards as applicable.

Regardless of format, all Web content or communications materials produced, including text, audio or video - must conform to applicable Section 508 standards to allow federal employees and members of the public with disabilities to access information that is comparable to information provided to persons without disabilities. All contractors (including subcontractors) or consultants responsible for preparing or posting content must comply with applicable Section 508 accessibility standards, and where applicable, those set forth in the referenced policy or standards documents above. Remediation of any materials that do not comply with the applicable provisions of 36 CFR Part 1194 as set forth in the **SOW, PWS, or TO**, shall be the responsibility of the contractor or consultant.

The following Section 508 provisions apply to the content or communications material identified in this **SOW, PWS, or TO**:

- 36 CFR Part 1194.21 a - l
- 36 CFR Part 1194.22 a - p
- 36 CFR Part 1194.31 a - f
- 36 CFR Part 1194.41 a - c

The contractor shall provide a completed Section 508 Product Assessment Template and the contractor shall state exactly how proposed EIT deliverable(s) meet or does not meet the applicable standards.

The following Section 508 provisions apply for software development material identified in this **SOW, PWS, or TO**:

For software development, the Contractor/Developer/Vendor shall comply with the standards, policies, and procedures below:

Rehabilitation Act, Section 508, Accessibility Standards

- (1) 29 U.S.C. 794d (Rehabilitation Act as amended)
- (2) 36 CFR 1194 (508 Standards)

36 CFR Part 1194.21 (a – l)

36 CFR Part 1194.31 (a – f)

36 CFR Part 1194.41 (a – c)

(3) www.access-board.gov/sec508/508standards.htm (508 Standards)

(4) FAR 39.2 (Section 508)

(5) CMS/HHS Standards, policies and procedures (Section 508)

a. Information Technology – General Information

(<http://www.cms.hhs.gov/InfoTechGenInfo/>)

For web-based applications, the Contractor shall comply with the standards, policies, and procedures below:

Rehabilitation Act, Section 508, Accessibility Standards

(1) 29 U.S.C. 794d (Rehabilitation Act as amended)

(2) 36 CFR 1194 (508 Standards)

36 CFR Part 1194.22 (a – p)

36 CFR Part 1194.41 (a – c)

(3) www.access-board.gov/sec508/508standards.htm (508 Standards)

(4) FAR 39.2 (Section 508)

(5) CMS/HHS Standards, policies and procedures (Section 508)

a. Information Technology – General Information

(<http://www.cms.hhs.gov/InfoTechGenInfo/>)

3.2 CMS Information Security

This requirement applies to all organizations which possess or use Federal information, or which operate, use or have access to Federal information systems (whether automated or manual), on behalf of CMS.

The central tenet of the CMS Information Security (IS) Program is that all CMS information and information systems shall be protected from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft—whether accidental or intentional. The security safeguards to provide this protection shall be risk-based and business-driven with implementation achieved through a multi-layered security structure. All information access shall be limited based on a least-privilege approach and a need-to-know basis, i.e., authorized user access is only to information necessary in the performance of required tasks. Most of CMS' information relates to the health care provided to the nation's Medicare and Medicaid beneficiaries, and as such, has access restrictions as required under legislative and regulatory mandates.

The CMS IS Program has a two-fold purpose:

- (1) To enable CMS' business processes to function in an environment with commensurate security protections, and
- (2) To meet the security requirements of federal laws, regulations, and directives.

The principal legislation for the CMS IS Program is Public Law (P.L.) 107-347, Title III, Federal Information Security Management Act of 2002 (FISMA), <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>. FISMA places responsibility and accountability for IS at all levels within federal agencies as well as those entities acting on their behalf. FISMA directs Office of Management and Budget (OMB) through the Department of Commerce, National Institute of Standards and Technology (NIST), to establish the standards and guidelines for federal agencies in implementing FISMA and managing cost-effective programs to protect their information and information systems. As a contractor acting on behalf of CMS, this legislation requires that **the Contractor shall**:

- Establish senior management level responsibility for IS,
- Define key IS roles and responsibilities within their organization,
- Comply with a minimum set of controls established for protecting all Federal information, and
- Act in accordance with CMS reporting rules and procedures for IS.

Additionally, the following laws, regulations and directives and any revisions or replacements of same have IS implications and are applicable to all CMS contractors.

- P.L. 93-579, The Privacy Act of 1974, <http://www.usdoj.gov/oip/privstat.htm> , (as amended);
- P.L. 99-474, Computer Fraud & Abuse Act of 1986, www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.pdf P.L. 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35, www.archives.gov/federal-register/laws/paperwork-reduction;
- P.L. 104-208, Clinger-Cohen Act of 1996 (formerly known as the Information Technology Management Reform Act), http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html;
- P.L. 104-191, Health Insurance Portability and Accountability Act of 1996 (formerly known as the Kennedy-Kassenbaum Act) <http://aspe.hhs.gov/admsimp/pl104191.htm>;
- OMB Circular No. A-123, Management's Responsibility for Internal Control, December 21, 2004, http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html;
- OMB Circular A-130, Management of Federal Information Resources, Transmittal 4, November 30, 2000, <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>;
- NIST standards and guidance, <http://csrc.nist.gov/>; and,
- Department of Health and Human Services (DHHS) regulations, policies, standards and guidance <http://www.hhs.gov/policies/index.html>

These laws and regulations provide the structure for CMS to implement and manage a cost-effective IS program to protect its information and information systems. Therefore, the

Contractor shall monitor and adhere to all IT policies, standards, procedures, directives, templates, and guidelines that govern the CMS IS Program, <http://www.cms.hhs.gov/informationsecurity> and the CMS System Lifecycle Framework, <http://www.cms.hhs.gov/SystemLifecycleFramework>.

The Contractor shall comply with the CMS IS Program requirements by performing, but not limited to, the following:

- Implement their own IS program that adheres to CMS IS policies, standards, procedures, and guidelines, as well as industry best practices;
- Participate and fully cooperate with CMS IS audits, reviews, evaluations, tests, and assessments of contractor systems, processes, and facilities;
- Provide upon request results from any other audits, reviews, evaluations, tests and/or assessments that involve CMS information or information systems;
- Report and process corrective actions for all findings, regardless of the source, in accordance with CMS procedures;
- Document its compliance with CMS security requirements and maintain such documentation in the systems security profile;
- Prepare and submit in accordance with CMS procedures, an incident report to CMS of any suspected or confirmed incidents that may impact CMS information or information systems; and
- Participate in CMS IT information conferences as directed by CMS.

If the contractor believes that an updated IS-related requirement posted to the CMS website may result in a significant cost impact, the contractor may submit a request for equitable cost adjustment before implementing change.

3.3 Financial Report

The Contractor shall provide financial reports to reflect the work performed by both the prime Contractor and Subcontractors. The Contractor shall provide financial reports to reflect the cost in both hours and dollars of work performed by both the prime Contractor and Subcontractors. Included with the financial reports shall be CMS' Financial Status Report spread sheet (See Appendix D).

The Financial Report shall contain the following sections for both the Contractor and each Subcontractor:

- a. Contract Name
- b. Contract Number
- c. Authorized Contractor Representative
- d. Period of Performance
- e. Contract or Task Order Value
- f. Total Amount Billed
- g. Total Payment Received

- h. Current Month Hours Expended by Labor Category
- i. Cumulative Month Hours Expended by Labor Category
- j. Estimated Hours To Completion by Labor Category
- k. Current Month Cost Expended by Labor Category
- l. Cumulative Cost Expended by Labor Category
- m. Balance of Remaining Funds
- n. Estimated Cost To Completion by Labor Category
- o. Burn rate

3.4 Transition Out to a New Contractor

Transition to a new contractor is subsequent to the award of contract, should a follow-on contractor be awarded the HIX contract. (The transition to a new contractor may be required as a result of a future competitive RFP for this effort.)

The Contractor SHALL work proactively with CMS and any other organization, as designated by CMS, to ensure a smooth, orderly, cooperative transition of services to a new contractor, if necessary. The Contractor SHALL submit a phase-in plan that describes the Contractor's methodology, processes, and phase-in transition activities. Work phase-in plans and delivery dates shall be negotiated as soon as possible after notification of the new contractor's transition completion date.

Activities related to transition (should the transition be required) shall be conducted over a period not expected to exceed ninety (180) calendar days (6 months). During this transition period, the incumbent contractor shall work with CMS and the new contractor to set up a training schedule and a schedule of events to smoothly changeover to the new contractor.

Not more than two weeks after notification by CMS that the transition to a new contractor will take place, the incumbent contractor shall submit to the Project Officer a draft written Joint Operating Agreement (JOA). Both the incumbent contractor and the new contractor shall sign the JOA.

The purpose of the JOA is to establish a process for managing the workload while both contracts are in place and to also establish a process to fully transition the workload from the incumbent contract to the new contract. The incumbent Contractor's JOA shall illustrate the manner in which the two entities will maintain support during the transition of the work from the incumbent's contract to the new contract including methods that will be used to communicate and coordinate activities among themselves and to communicate to CMS.

The JOA shall define the responsibilities for the incumbent contractor and the new contractor and shall be submitted to CMS for approval before final signatures are obtained. In addition, as part of the JOA, the incumbent contractor and the new contractor shall form a joint coordinated management team that will ensure that communication, coordination, cooperation, and consultation between the two entities is maintained in support of the transition and ongoing work. Such a team shall have regular meetings and shall monitor the work of any subgroups during transition and ongoing work, and shall submit status reports as determined by CMS.

The new contractor shall participate in the formation of a joint team with the incumbent contractor that will be managed by CMS to ensure that communication, coordination, cooperation, and consultation between all the entities is maintained in support of the transition and ongoing work. This joint contractor team shall meet regularly (as defined by CMS) and shall monitor and manage the work of any subgroups during transition.

Incumbent Contractor Responsibilities

Not later than four weeks after notification by CMS that the transition to a new contractor will take place, the incumbent contractor shall submit to the Project Officer a Transition Plan. The Plan shall address the specific steps and dates the incumbent contractor will take to change the program to a new contractor. The Plan shall include but not be limited to the following:

- Transition plans and procedures
- Transition milestones and timeframes, including a detailed timeline for work-in-progress, test-site and production cutovers,
- A CMS approved comprehensive listing of the responsibilities of all personnel participating in the transition to include the policies, practices and procedures to be employed by the incumbent contractor to ensure there is no conflict between routine system maintenance and the activities of the transition,
- A CMS approved in-depth schedule and thorough description of the methodology to be employed by the incumbent contractor to ensure no degradation of service during the transition period,
- A CMS approved risk management plan that includes a list of the potential risks during the transition period and the plan to mitigate each, and
- A CMS approved complete and detailed resource-planning/resource-turnover analysis that includes network, Single Testing Contract (STC) and contractor infrastructure requirements.
- Any CMS approved travel necessary to support the transition (if applicable).

3.5 General Assumptions

To the extent that tasks in this scope of work pertain to the number of States that may be certified to operate an exclusively State-based Exchange, or to the operation of a State Partnership Exchange with the Federal government performing a range of business services from significantly all to a few, the Contractor shall use at least the following assumptions for pricing its proposal to assure the use of the same or similar basic assumptions. Some of the assumptions provided below pertain to tasks that may not be included in this scope of work, (e.g., onsite visits and analytic work to develop a payment notice), in which case the Contractor shall not include such tasks in the proposal or related pricing. Leading up to State certification, the Federal government will track State progress and provide technical assistance with the intention of maximizing the number of States that meet the necessary requirements for certification.

CMS will not know for certain how many States will apply for certification and be certified until January 1, 2013. Given this uncertainty, the Contractor shall assume that 50 states, the District of Columbia, and U.S. territories will participate in a three-phase review process in 2012 that will include at least:

- An early assessment and a draft certification application review;
- A final certification application review approval process; and
- Three onsite visits per State.

For the purpose of costing out a proposal, the Contractor shall also assume that all Exchanges will access a Federal data services hub that will facilitate transactions between States and federal agencies where federal information is required, for example, to support the determination and verification of consumer eligibility for tax credits. For all business functions that an exchange must provide, the Contractor shall assume that States will fall into one of three categories. i.e., States that:

- Build or use vendor or other State services under direct arrangement and will be certified to run a State-based Exchange;
- Opt for an Exchange facilitated by Federal agencies that will operate in States; and
- Operate under a State Partnership Model allowing a State's business services that are ready in time for certification to operate in combination with Federal services. For such States the Contractor shall assume, on average, two business systems or services (e.g., eligibility and enrollment, financial management, plan management) developed by the Federal government (not including access to the Federal data services hub) to be operating.

As of July 7, 2011, eleven states have Exchange laws, and one more has legislation awaiting the Governor's signature. An additional nine states have laws or executive orders to study establishment of a State-based Exchange.

For each of these three categories, the Contractor shall assume that the size of the States in each category range from high to low in terms of the number of people estimated to be eligible for enrollment in Medicaid, CHIP and an exchange. Using local and regional Part C contracts and health plans as a simple approximation of the impact of Issuer and qualified health plans on Exchange functions, the Contractor shall assume 500 Issuer contracts and 3000 qualified health plans across all exchanges.

3.5.1 Other Assumptions

The Affordable Care Act requires the Federal government to provide technical support to States with Exchange grants. To the extent that tasks included in this scope of work could support State grantees in the development of Exchanges under these grants, the Contractor shall assume that data provided by the Federal government or developed in response to this scope of work and their deliverables and other assets associated with this scope of work will be shared in the open collaborative that is under way between States, CMS and other Federal agencies. This open

collaborative is described in IT guidance 1.0. See <http://www.cms.gov/Medicaid-Information-Technology-MIT/Downloads/exchangemedicaiditguidance.pdf>.

This collaboration occurs between State agencies, CMS and other Federal agencies to ensure effective and efficient data and information sharing between state health coverage programs and sources of authoritative data for such elements as income, citizenship, and immigration status, and to support the effective and efficient operation of Exchanges. Under this collaboration, CMS communicates and provides access to certain IT and business service capabilities or components developed and maintained at the Federal level as they become available, recognizing that they may be modified as new information and policy are developed. CMS expects that in this collaborative atmosphere, the solutions will emerge from the efforts of Contractors, business partners and government projects funded at both the State and federal levels. Because of demanding timelines for development, testing, deployment, and operation of IT systems and business services for the Exchanges and Medicaid agencies, CMS uses this collaboration to support and identify promising solutions early in their life cycle. Through this approach CMS is also trying to ensure that State development approaches are sufficiently flexible to integrate new IT and business services components as they become available.

- The Contractor's IT code, data and other information developed under this scope of work shall be open source, and made publicly available as directed and approved by the COTR.
- The development of products and the provision of services provided under this scope of work as directed by the COTR are funded by the Federal government. State Exchanges must be self-funded following 2014. Products and services provided to a State by the Contractor under contract with a State will not be funded by the Federal government.

4. Security

Contractor personnel visiting any Government facility in conjunction with the task order shall be subject to the Standards of Conduct applicable to Government employees. Site-specific regulations regarding access to classified or sensitive materials, computer facility/IT network access, issue of security badges, etc., shall be provided as required by the Government. All products, source code and scripts produced and their associated work papers are to be considered the property of the Government, specifically, the Department of Health and Human Services.

The provisions outlined in this section apply to the prime contractor, all subcontractors and all prime or subcontractor employee(s) that may be employed during the course of the task order.

Requirements

To perform the work specified herein, contractor personnel will require access to sensitive data, regular access to HHS-controlled facilities and/or access to HHS information systems. All Contractor personnel shall meet the minimum requirements of Homeland Security Presidential Directive 12 prior to beginning work. All contractor personnel fulfilling the requirements of the task order, are required to read and sign a Nondisclosure Statement, prior to beginning work.

HHS Information Security Program Contract Oversight Guide

The Contractor shall comply with the HHS Information Security Program Contractor Oversight Guide dated November 7, 2006. The contractor shall ensure that each contractor/subcontractor employee has completed the HHS Computer Security Awareness Training course prior to performing any contract work, and thereafter shall complete the HHS-specified fiscal year refresher course during the period of performance of the contract.

The contractor shall maintain a listing by name and title of each contractor/subcontractor employee working under the task order that has completed the HHS required training. Any additional security training completed by contractor/subcontractor staff shall be included on this listing. [The listing of completed training shall be included in the first technical progress report. Any revisions to this listing as a result of staffing changes shall be submitted with next required technical progress report.]

Physical Security

The contractor is to be responsible for safeguarding all government property provided for contractor use. At the close of each work period, government facilities, equipment, and materials are to be secured.