SECTION C – Performance Work Statement

Performance Work Statement (PWS)
Information Technology Customer Satisfaction Assessment (ITCSA)
Centers for Disease Control and Prevention (CDC)
Information Technology Services Office (ITSO)
Management Information Systems Office (MISO)

This Performance Work Statement consists of two independent Customer Satisfaction Assessment tasks, which will be funded separately. Proposed solution should be identical and work the same way for both tasks and use the same technology.

1.0 BACKGROUND: As the Centers for Disease Control and Prevention (CDC), changes to meet the challenges of public health in the 21st century, the CDC's Information Technology (IT) systems and services must continuously change to support and advance the agency's business needs. CDC's dependence on information technology, information systems, electronic communications, and digital media continues to grow rapidly and is essential to the mission and program accomplishment. The CDC Information Technology Services Office (ITSO) manages CDC's IT infrastructure capital investments and CDC-wide IT acquisitions of infrastructure technologies, to include the implementation of budgets, policies, and procedures for IT infrastructure services to support CDC's mission. The Centers for Disease Control and Prevention (CDC) Management Information Systems Office (MISO) designs, develops, implements, supports, and evaluates a portfolio of enterprise business information systems for CDC's administrative lines of business. MISO provides data management and integration services to support CDC administrative and non-administrative lines of business as well as integration with programmatic functions. MISO also provides knowledge management services, including information retrieval, information mapping, information sharing, data categorization, and knowledge capture. MISO was established to enable CDC to deliver application development and data management services across a portfolio of applications for the purpose of providing high quality and reliable software. The products and services developed, managed, and maintained by MISO are used across CDC and directly support numerous important CDC programs and initiatives in achieving the Agency's public health objectives. As public health missions and needs evolve, MISO must continually monitor and update its' software and information management capabilities to meet those needs.

As ITSO and MISO move forward into 2016 they seek expert IT consulting services to aid in achieving operating and efficiency goals and provide effective and efficient recommendation of the organizations IT customer service support. The IT analysis and benchmarking services remain a critical need to the organization as it moves forward into the future. The results of the assessments are used to benchmark ITSO and MISO's success against other Government and non-Government IT organizations. ITSO has received a "Best-In-Class" ranking for several years in comparisons with other government and non-government IT organizations. MISO seeks to achieve its 2020 vision.

1.1 OBJECTIVE: The objective of this requirement is to engage in an enterprise-wide CDC measure of its Information Technology Customer Service Assessments (ITCSA), provide expert IT consulting services and recommendations to include benchmarking ITSO's customer satisfaction rating accomplishments results against other Government and non Government IT organizations. All end-users, (excluding ITSO, MISO, and OCISO) shall be invited to participate in the assessment. The Customer Satisfaction Analysis shall assess end-user satisfaction with IT services delivered by ITSO and MISO staff. At the conclusion of the analysis, CDC shall have an enterprise-wide and comprehensive perspective of end-user customer satisfaction levels.

2.0 SCOPE OF WORK: The scope of the task order is to develop web-based, electronic customer satisfaction assessments for each organization (ITSO and MISO), invite participants, collect and analyze the data, report findings and develop recommendations for improvement. In addition to the survey services performed, the IT Customer Service survey results shall be measured against other Government and non-Government IT organizations and a national ranking assigned to the organization, and access (to the COR, Technical Monitor(s), or both) should be granted to an array of available analytical tools and reports to assist ITSO and MISO with any additional analysis of the survey data. The scope of this engagement is an enterprise-wide CDC measure of IT customer satisfaction.

3.0 PERFORMANCE REQUIREMENTS:

3.1 SURVEY SERVICES: The contractor shall develop and deploy a web-based, IT customer service satisfaction survey using a standard set of service criteria to measure satisfaction with specific services. The assessment shall also include demographic data.

3.2 DATA COLLECTION:

3.2.1 The contractor shall initiate the collection of data via email invitation to CDC providing a direct link to the web-based survey and timelines for responding. Participation is voluntary and anonymous. The contractor shall send participation reminders as indicated by the COR or Technical Monitor.

3.2.2 The contractor shall utilize the identified criteria, collect the data needed to perform the customer satisfaction assessment. The data should be collected electronically and in a fashion such that the raw data can be given to CDC in a read/write fashion. The contractor shall notify CDC of any information or documents required that were not previously identified. During this phase of the project, the ITSO Contracting Officer's Representative (COR) shall be notified if there are difficulties obtaining access to documents or personnel that will impact the project completion schedule. An overview of participation shall be provided to the COR and ITSO Technical Monitor on a bi-weekly basis.

3.3.1 ANALYSIS/ASSESSMENT INTERIM REPORTS

3.3.1 The contractor shall provide a detailed analysis and assessment of all criteria gathered from the Customer Satisfaction Survey including comparing the survey results to other Governmental and non-Governmental IT organizations. The analysis shall compare and rank the CDC IT customer satisfaction rating results against the contractor's database average and assign a projected national rating of the organizations performance.

3.3.2 The contractor shall present the draft results along with the raw data to COR and Technical Monitor. This shall be an interim review to discuss important findings in order to receive feedback and shall not be the final analysis. The purpose of this review is to validate findings for accuracy and preview working conclusions for relevance. Changes shall be incorporated into the final deliverable as appropriate.

3.3.3 The contractor shall review ITSO's historical ITCSA data results and provide a trend analysis of the ITSO ITCSA results.

3.3.4 The Contractor shall provide access to analysis tools and reports as requested by the COR or Technical Monitor.

3.4 FINAL PROJECT REPORTING AND RECOMMENDATIONS

3.4.1 The contractor shall develop and finalize the Customer Survey Study recommendation report and develop an executive level brief that summarizes the engagement results. This report shall identify and document gaps where customer satisfaction issues need to be addressed.

3.4.2 The contractor shall provide a draft version of the Final Report to the COR and Technical Monitor for review and comment, incorporating comments as appropriate. This shall include all recommendations for

process improvement and the final national ranking assigned to ITSO when compared against other Governmental and non-Governmental IT organizations in the contractor's IT database.

3.5 Optional Task: Management Information Systems Office (MISO) ITCSA

3.5.1 SURVEY SERVICES*: The contractor shall develop and deploy a web-based, IT Customer Service Satisfaction Survey using a standard set of service criteria to measure satisfaction with specific services. The assessment shall also include demographic data.*

3.5.2 DATA COLLECTION*: The contractor shall initiate the collection of data via email invitation by providing a direct link to the web-based survey and timelines for responding. Participation is voluntary and anonymous. The contractor shall send participation reminders as indicated by the MISO Project Officer.*

The contractor shall utilize the identified criteria and collect the data needed to perform the customer satisfaction assessment. The data shall be collected electronically and in the raw data can be given to MISO in a read/write fashion. The contractor shall notify MISO of any information or documents required that were not previously identified. During this phase of the project, the MISO Project Officer shall be notified if there are difficulties obtaining access to documents or personnel that will impact the project completion schedule. MISO will then timely inform the ITSO COR. An overview of participation shall be provided to the MISO Project Officer on a weekly basis via email.

3.5.3 ANALYSIS/ASSESSMENT INTERIM REPORTS (to MISO Project Officer): *The contractor shall provide a detailed analysis and assessment of all criteria gathered from the Customer Service Satisfaction Survey, including comparing the survey results to other Governmental and non-Governmental IT organizations. The analysis shall compare and rank the CDC IT customer satisfaction rating results against the contractor's database average and assign a projected national rating of the organizations performance.*

The contractor shall present the draft results, along with the raw data, to the MISO Project Officer. This shall be an interim review to discuss important findings in order to receive feedback and shall not be the final analysis. The purpose of this review is to validate findings for accuracy and preview working conclusions for relevance. Changes shall be incorporated into the final deliverable as appropriate.

The contractor shall review MISO's historical ITCSA data results (when available) and provide a trend analysis.

3.5.4 FINAL PROJECT REPORTING & RECOMMENDATIONS: *The contractor shall develop and finalize the customer survey study recommendation report and develop an executive level brief that summarizes the engagement results. This report shall identify and document gaps where customer satisfaction issues need to be addressed.*

The contractor shall provide a draft version of the Final Report to the MISO Project Officer for review and comment, incorporating comments as appropriate. This shall include all recommendations for process improvement and the final national ranking assigned to MISO when compared against other Governmental and non-Governmental IT organizations in the contractor's IT database.

4.0 PERFORMANCE MATRIX:

Deliverable or Required Services (1)	Performance Standard(s) (2)	Acceptable Quality Level (AQL) (3)	Method of Surveillance (4)
PWS 3.1. Survey Development and Deployment	Accurate and complete customer satisfaction survey utilizing established standard set of service criteria to measure satisfaction with a	No deviation	100% Government inspection

	specific service to include demographic data provided 45 days from the start of the survey.		
PWS 3.2 Data collection	Web based IT Customer Satisfaction Survey rollout to the CDC employees in 2nd quarter Fiscal Year 16 3.2.1 Data collection Overview of data collected shall be provided on a weekly basis. 3.2.1Survey Participation reminder sent out to CDC users as indicated by COR or Technical Monitor	95%	Periodic Review
	Reports prepared in a professional format and exhibiting easy to read, easy to understand data. No more than one (1) late document per quarter and no more than one report delivered (5) days late.	95%	100% Government inspection
PWS 3.3.1 Analysis/Assessment	Reports prepared in a professional format and exhibiting easy to read, easy to understand data. Interim Report to include draft presentation, data analysis results along with raw data. Interim report submitted for review per delivery The interim report is due 45 days following the end date of the ITSO survey.	95%	100% Government inspection
PWS 3.4 Final report and Recommendations	Clear concise executive brief prepared in a professional format and exhibiting easy to read, easy to understand data. Executive brief is due 30 days following the Interim report.	95%	100% Government inspection

5.0 TASK ORDER DELIVERABLES: All deliverables shall be delivered to the COR no later than the specified dates stated in the Performance matrix below.

The specific deliverables and schedule for delivery shall be as agreed upon and documented by COR and Contracting Officer. CDC, ITSO reserves the right to prioritize work and negotiate any delivery dates. However, any direction and changes that may impact contractual delivery dates or task order pricing must be coordinated with the COR and Procurement and Grants Office, PGO, Contracting Officer.

All deliverables for this MISO optional task shall be delivered to the MISO Project Officer no later than the specified dates stated in the performance matrix below. The MISO Project Officer will then timely

forward the deliverables to the ITSO COR.

All documents, plan, diagrams, presentations, etc. are to be submitted solely in electronic form and in the native file format of MS Word 2013, MS Excel 2013, MS Visio 2013, MS project 2013, or MS PowerPoint 2013. Also, provide hard copies as needed.

Deliverables shall be submitted to the COR. Name and e-mail information of ITSO COR and MISO Project Officer shall be provided after award of task order and optional task.

5.1 DELIVERABLES

Title	Due Date(
Deliverable or Required Services	
Post Award Meeting	10 days after award of task order
Web based Customer Satisfaction Survey	45 days after award
Data collection Assessment	Weekly
Interim Report	45 days following survey end date
Final Report Executive Briefing	30 days following interim report
Monthly Status Report (MSR)	Within ten (10) business days following the close of the preceding month

Monthly Reports: Each report shall be due on the tenth (10^{th}) workday following the close of the calendar month. Each report shall be submitted to the COR and Project Monitor via electronic mail. The COR and Project Monitor shall be identified at the Post Award meeting.

5.1.1 Monthly Status Report (MSR): The MSR is due on the tenth (10^{th}) workday following the close of the calendar month. Each report shall be submitted to the MISO Project Officer via electronic mail. MISo will then timely forward the MSR to the ITSO COR. The COR and Project Officer shall be identified at award of the optional task.

The MSR shall contain the following information:

- Brief description of requirements;
- Brief summary of accomplishments during the reporting period and significant events;
- Deliverables submitted or progress on deliverable products;
- Any current or anticipated problems; and,
- Brief summary of activity planned for the next reporting period.

5.2 POST AWARD MEETING Within ten (10) business days following the task award date, contractor shall meet with the COR and Technical Monitor, to review goals and objectives of this task order, and to discuss technical requirements.

5.3 Contracting Officer's Represenative (COR) for ITSO IT Customer Satisfaction Survey

June C. Humphrey, IT Business Specialist (Acquisition)
Office of the Chief Information Officer
Information Technology Services Office (ITSO)
Business Services Office (BSO)

University Office Park
Williams Building, Room 5412
Mailstop: K-84
Phone (770) 488-1445; Mobile (404) 293-5881
Email: jchumphrey@cdc.gov

6.0 **SECURITY:** Pursuant to Federal and HHS Information Security Program Policies, the Contractor and any subcontractor performing under this task order shall comply with the following requirements:

Contractor performance and resulting deliverables shall adhere to all Federal, HHS, and/or CDC IT security policies and procedures. The contractor shall adhere to the Federal Information Security Management Act (FISMA) FISMA status and remediation reports shall be proved as required.

6.1. **Information Type:** Mission Based Information: It is understood that the Contractor's staff shall be exposed to highly critical systems, however, the nature of the relationship shall be limited, and there shall be an ongoing process which shall include review of security concerns during the work performed under the resultant requirement. Therefore, the positions are judged to be of low risk and the NACI background check shall apply to all Contractor personnel. The requirement for the NACI background check requires no action during the procurement process. Appropriate security screening information/procedures shall be initiated by the Contractor to interview all on-site personnel. Should the Government determine, as a result of any Technology Refreshment, that new equipment and software shall be introduced, such as introduction or expansion of the newer digital communications technologies, the Contractor shall participate in an overall qualitative risk assessment aimed at identifying new or enhanced potential for unauthorized access to systems or services and methods to control or remove the potential risk as well as continually evaluate legacy systems for previously unidentified risks.

6.1.2 **Security Categories and Levels**

Confidentiality	Level:	[X] Low	[ ] Moderate	[] High
Integrity	Level:	[X] Low	[ ] Moderate	[] High
Availability	Level:	[X] Low	[ ] Moderate	[] High
Overall	Level:	[X] Low	[ ] Moderate	[] High

6.1.3 **Position Sensitivity Designations:** The following position sensitivity designations and associated clearance and investigation requirements apply under this task order.

Level 2: Non-Critical Sensitive (Requires Suitability Determination with a Secret) Contractor employees assigned to a Level 2 position shall access sensitive information for which unauthorized disclosure could endanger national security.

Level 5: Public Trust - Moderate Risk (Requires Suitability Determination with NACIC, MBI or LBI). Contractor employees assigned to a Level 5 position with no previous investigation and approval shall undergo a National Agency Check and Inquiry Investigation plus a Credit Check (NACIC), a Minimum Background Investigation (MBI), or a Limited Background Investigation (LBI).

The Contractor shall submit a roster, by name, position and responsibility, of all staff (including subcontractor staff) working under the task order that shall develop, have the ability to access, or host and/or maintain a Federal information system(s). The roster shall be submitted to the Project

Officer/COR, with a copy to the Contracting Officer, within 14 calendar days of the effective date of the task order. Any revisions to the roster as a result of staffing changes shall be submitted within 15 calendar days of the change. The Contracting Officer shall notify the Contractor of the appropriate level of suitability investigations to be performed.

Upon receipt of the Government's notification of applicable Suitability Investigations required, the Contractor shall complete and submit the required forms within 30 days of the notification. The following items shall be completed by the Contractors staff member(s) requiring access to on-site facilities in the performance of the anticipated requirement to include the following forms at a minimum:

Two completed Forms FD-258, "FBI Fingerprint Charts"
One completed Standard Form 85, "Questionnaire for Non-Sensitive Positions"
One completed Optional Form 306, "Declaration for Federal Employment"
One completed resume or curriculum vitae
One copy of the state-wide criminal records check
One copy of the motor vehicle violations check (when applicable)

The Contractor's staff that has been authorized for unescorted access to a facility, either through the temporary clearance process or the formal NACI process, shall display an identification badge as required and furnished by the CDC. The Contractor shall submit to the designated CDC official a completed Identification Badge Request Form (CDC Form 0.1137, Rev. 98) for each employee who has been authorized unescorted access to a facility. If a Contractor staff member needs regular unescorted access to one of the Cardkey access-designated areas, a completed Cardkey Request Form (CDC Form 0.834, Rev. 3/94) shall be submitted to the designated CDC official for approval. Contractor/subcontractor employees who have met investigative requirements within the past five years may only require an updated or upgraded investigation.

6.1.4 Information Security Training: 1HHS policy requires contractors/subcontractors receive security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements. The Contractor shall ensure that each Contractor/subcontractor employee has completed the security awareness and safety training requirements and any other role-based training prior to performing any task order work, and thereafter completing the CDC specific fiscal year refresher course(s) during the period of performance of the task order.

The Contractor shall maintain a listing by name and title of each Contractor/subcontractor employee working under this task order that has completed the 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.

References:
http://intranet.hhs.gov/infosec/docs/policies_guides/1SS/001SStdSecConfig_01302009.html

6.1.5 Rules of Behavior and Responsibilities: The Contractor shall wear the badge at all times when entering and in the CDC building. The badge shall be shown or presented to the security personnel when entering CDC buildings.

When a Contractor/subcontractor employee terminates work under this contract, all documentation shall be made available to the Project Officer/COR and/or Contracting Officer upon request.

Return of Identification Badges/Cardkeys
The Contractor shall arrange for the return of all employee identification badges and/or cardkeys to the Cardkey/ID Badge Office, located on the Roybal campus, immediately upon separation of duties at the on-site facility. Contact the Project Officer for location of the depositories for the return of badges. Cardkeys shall be returned to the appropriate Office.

6.1.6 Commitment to Protect Non-Public Departmental Information Systems and Contractor Agreement

Contractor Agreement
The Contractor and its subcontractors performing under this PWS shall not release, publish, or disclose non-public Departmental information to unauthorized personnel, and shall protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of such information:

18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
Public Law 96-511 (Paperwork Reduction Act)
30 U.S.C.

Contractor-Employee Non-Disclosure Agreements
Each Contractor/subcontractor employee who may have access to non-public Department information under this task order shall complete the Commitment to Protect Non-Public Information - Contractor Agreement (http://nitaac.nih.gov/downloads/ciosp2/Contractor_Employee_Non-Disclosure.doc). A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the Project Officer prior to performing any work under the contract.

6.1.7 Security Processes: Contractor/subcontractor employees shall comply with the HHS criteria for the assigned position sensitivity designations prior to performing any work under this task order. The following exceptions apply:
Levels 5 and 2: Contractor/subcontractor employees may begin work under the task order after the Contractor has submitted the name, position and responsibility of the employee to the Project Officer.

The Personnel Security Section (PSS) shall immediately notify the Contracting Officer if the fingerprint results come back inconclusive. The Contracting Officer shall communicate the results to the Project Officer and the Contractor. The Contractor may require the employee to be re-fingerprinted or may substitute another employee to be fingerprinted (if not already fingerprinted). The process shall continue until favorable results are received.

The PSS shall provide the names of Contractor personnel who do not favorably pass the NACI to the Contracting Officer and Project Officer. Upon receipt of such a list, the Contracting Officer shall notify the Contractor and require the Contractor to immediately remove any contract employee on the list from the on-site facility who failed to receive a favorable suitability determination. Such a demand shall be made because that employee's continued employment is deemed contrary to the public interest, inconsistent with the best interests of security, or may be identified as a potential threat to the health, safety, security, general well being, or operational mission of the on-site facility and its population. The Contracting Officer may also require the Contractor to immediately remove any contract employee from the on-site facility should it be determined that the individual who is being assigned to duty has been disqualified for suitability reasons, or who is found to be unfit for performing duties during their tour(s) of duty. Contract employees who require removal from the on-site facility shall leave the work site immediately.

After normal business hours, or in situations where a delay would not be in the best interest of the Government, or a potential threat to the health, safety, security, general well being, or operational mission of the facility and its population, the Contracting Officer shall have the authority to direct immediate removal of the Contractor employee from the on-site facility.

The Contracting Officer shall subsequently provide the official, written notification to the Contractor documenting the reason for removal of the Contractor employee from the CDC facility. When removal is directed due to an unfavorable NACI report constituting a non-suitability determination, no further information shall be provided. If removal is directed for other reasons relating to specific conduct of the employee during performance of the work, the Contracting Officer's official, written notification shall provide information as to these reasons.

6.1.8 Secure One HHS:

HHS-OCIO Standard for Security Configurations Language in HHS Contracts

HHS Standard 2009-0001.001S

January 30, 2009

To implement Federal Acquisition Regulation (FAR) 39.101(d) regarding Common Security Configurations, and Department of Health and Human Services (HHS) information security requirements, the following standard language shall be incorporated in solicitations and new contracts for the operation or acquisition of information technology systems. This document supersedes HHS Standard 2008-0004.001S, *HHS-OCIO Standard for Security Configurations Language in HHS Contracts* (dated September 11, 2008), and is effective immediately.[1] An approved *HHS Department Information Security Policy/Standard Waiver*[2] *is required to deviate from the technical standard set forth below.*

Contractor computers containing HHS data shall be configured with the applicable Federal Desktop Core Configuration (FDCC) (http://nvd.nist.gov/fdcc/index.cfm),[3] and shall have and maintain the latest operating system patch level and anti-virus software level.

2. The Contractor shall apply approved security configurations to information technology that is used to process information on behalf of the Department, its Operating Divisions (OPDIVs) and Staff Divisions (STAFFDIVs).

Such approved security configurations shall be identified jointly by the OPDIV/STAFFDIV Contracting Officer's Technical Representative (COTR) and Chief Information Security Officer (CISO). Approved security configurations include, but are not limited to, those published by the Department,[4] by the OPDIV/STAFFDIV, and by the National Institute of Standards and Technology (NIST) at http://checklist.nist.gov. OPDIVs/STAFFDIVs may have security configurations that are more stringent than the minimum baseline set by the Department or NIST. When incorporating such security configuration requirements in solicitations and contracts, the OPDIV CISO shall be consulted to determine the appropriate configuration reference for a particular system or services acquisition.

3. The Contractor shall ensure applications operated on behalf of the Department or OPDIV/STAFFDIV are fully functional and operate correctly on systems configured in accordance with the above configuration requirements. The Contractor shall use Security Content Automation Protocol (SCAP)-validated tools with FDCC Scanner capability to ensure its products operate correctly with FDCC configurations and do not alter FDCC settings.[5] The Contractor shall test applicable product versions with all relevant and current updates and patches installed. The contractor shall ensure currently supported versions of information technology (IT) products meet the latest FDCC major version and subsequent major versions.[6]

4. The Contractor shall ensure applications designed for end users run in the standard user context without requiring elevated administrative privileges.

5. The Contractor shall ensure hardware and software installation, operation, maintenance, update, and patching shall not alter the configuration settings or requirements specified above

6. Federal Information Processing Standard 201 (FIPS-201)[7] compliant, Homeland Security Presidential Directive 12 (HSPD-12) card readers shall: (a) be included with the purchase of servers, desktops, and laptops; and (b) comply with FAR Subpart 4.13, *Personal Identity Verification*.

7. The Contractor shall ensure all its subcontractors which perform work under this contract (at all tiers) comply with the above requirements.

APPROVED BY & EFFECTIVE ON:January 30, 2009
Michael W. Carleton,HHS Chief Information Officer and Deputy Assistant Secretary for Information Technology

APPROVED BY & EFFECTIVE ON:

January 30, 2009
Martin J. Brown, HHS Senior Procurement Executive and
Deputy Assistant Secretary for Acquisition Management and Policy

[1] This requirement shall be incorporated into the HHS Acquisition Regulation and the HHS Acquisition Plan.
[2] The *HHS Departmental Information Security Policy/Standard Waiver* form and process is available at http://intranet.hhs.gov/infosec/policies_memos.html.
[3] FDCC is applicable to all computing systems using Windows XP™ and Windows Vista™, including desktops and laptops—regardless of function—but not including servers. The Department has developed an HHS version of FDCC (henceforth HHS FDCC) for Windows XP™ and Vista™ to accommodate business and operational needs in the HHS environment. These settings are available at http://intranet.hhs.gov/infosec/guidance.html. When there is a compelling business or operational need to deviate from the FDCC, Operating Divisions (OPDIVs) and Staff Divisions (STAFFDIVs) may use the HHS FDCC settings instead of the government-wide FDCC settings.
[4] See *HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications* (as amended) at http://intranet.hhs.gov/infosec/guidance.html.
[5] See http://nvd.nist.gov/validation.cfm, as required by the Office of Management and Budget (OMB) Memorandum (M) 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC),* released August 11, 2008.
[6] This meets the self-assertion requirement under OMB M-08-22. Future FDCC changes having minimal security impact may be released as minor versions to FDCC. Self-assertion is not required for minor releases.
[7] http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

6.1.9 HHS-OCIO Standard for Encryption Language in HHS Contracts

HHS Standard 2009-0002.001S

January 30, 2009

The Department of Health and Human Services (HHS) requires incorporation of the following standard language in solicitations and new contracts that either purchase or require the use of desktop or laptop computers, mobile devices, or portable media to store or process HHS sensitive information that is categorized as Moderate or High under Federal Information Processing Standard 199 (FIPS 199).[1] An approved *HHS Department Information Security Policy/Standard Waiver*[2] *is required to deviate from these technical standards.* This standard is effective immediately.[3]

1. The Contractor shall use FIPS 140-2 (as amended) compliant encryption[4] to protect all instances of HHS sensitive information[5] during storage and transmission.
2. The Contractor shall verify that the selected encryption product has been validated under the Cryptographic Module Validation Program (http://csrc.nist.gov/cryptval/) to confirm compliance with FIPS 140-2 (as amended). The Contractor shall provide a written copy of the validation documentation to both the Contracting Officer and the Contracting Officer's Technical Representative (COTR).
3. The Contractor shall use the Key Management Key on the HHS personal identification verification (PIV) card; or alternatively, the Contractor shall establish and use a key recovery mechanism to ensure the ability for authorized personnel to decrypt and recover all encrypted information.[6]
4. The Contractor shall securely generate and manage encryption keys to prevent unauthorized decryption of information, in accordance with FIPS 140-2 (as amended).
5. The Contractor shall: ensure that this standard is incorporated into the Contractor's property management/control system; or establish a procedure to account for all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive HHS information.
6. The Contractor shall ensure that all of its employees, subcontractors (at all tiers), and employees of each subcontractor, who perform work under this contract/subcontract, comply with the above requirements.

APPROVED BY & EFFECTIVE ON:
January 30, 2009
Michael W. Carleton HHS Chief Information Officer and Deputy Assistant Secretary for Information Technology
APPROVED BY & EFFECTIVE ON:
January 30, 2009
Martin J. Brown, HHS Senior Procurement Executive and Deputy Assistant Secretary for Acquisition Management and Policy

[1] FIPS-199, Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.
[2] The HHS Departmental Information Security Policy/Standard Waiver form and process is available at http://intranet.hhs.gov/infosec/policies_memos.html.
[3]This requirement shall be incorporated into the HHS Acquisition Regulation and the HHS Acquisition Plan.

[4] The Office of Management and Budget (OMB) Memorandum (M) 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (released May 22, 2007) requires the use of FIPS 140-2, Security Requirements for Cryptographic Module, compliant encryption technologies on laptop computers and all other mobile computers and devices containing sensitive information. The HHS memorandum Mandatory Protection of Sensitive Information on Computers, Mobile Devices, and Portable Media (henceforth called the Protection of Sensitive Information Memo), signed by the HHS Chief of Staff on May 19, 2008, directs expansion of the current HHS Encryption Standard for Mobile Devices and Portable Media to "all government and non-government-furnished desktops used on behalf of the government that store sensitive information."

[5] For the purposes of this contract, information is considered sensitive if the FIPS 199 Confidentiality or Integrity security objective is rated Moderate or High by the OPDIV Chief Information Security Officer (CISO) or HHS Chief Information Security Officer (CISO), as appropriate.

[6] Key recovery is required by OMB Guidance to Federal Agencies on Data Availability and Encryption, November 26, 2001, http://csrc.nist.gov/policies/ombencryption-guidance.pdf. Authorized personnel to decrypt and recover all encrypted information shall be identified by contract.

7.0 TASK ORDER TERMS AND CONDITIONS:

7.1 Place of Performance Contractor facilities.

7.2 Inspection and Acceptance: Inspection and acceptance shall occur in accordance with 52.212-4(a). In the absence of other agreements negotiated with respect to time provided for government review, deliverables shall be inspected and the contractor notified of the COR'S findings within five (5) work days of normally scheduled review. If the deliverables are not acceptable, the COR shall notify the Contracting Officer, CO immediately.

Unsatisfactory work - Performance by the contractor to correct defects found by the Government as a result of quality assurance surveillance and by the contractor as a result of quality control, shall be at its' own expense and without additional reimbursement by the government. Unless otherwise negotiated, the contractor shall correct or replace all non-conforming services or deliverables not later than five (5) workdays after notification of non-conformance.

7.3 Quality Control: The contractor shall provide and maintain a Quality Control Plan (QCP) that contains, as a minimum, the items listed below to the ITSO COR and MISO Project Officer for acceptance not later than ten (10) calendar days after award. The COR shall notify the contractor of acceptance or required modifications to the plan. The contractor shall make appropriate modifications and obtain acceptance of the plan within thirty (30) calendar day from the date of award.

The QCP shall include the following minimum requirements:

- A description of the inspection system to cover all major services and deliverables. The description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title of inspectors.
- A description of the methods to be used for identifying and preventing defects in the quality of service performed.
- A description of the records to be kept to document inspections and corrective or preventative actions taken.
- All records of inspections performed shall be retained and made available to the Government upon request throughout the task order performance period, and for the period after task order completion, until final settlement of any claims under this task order.

7.3.1 Quality Assurance: The Government shall evaluate the contractor's performance of this task order. For those tasks listed in the Performance Matrix, the COR or other designated evaluator shall follow the method of surveillance specified in this task order. Government personnel shall record all surveillance observations. When an observation indicates defective performance, the COR or other designated evaluator shall require the contractor manager or representative at the site to initial the observation. The initialing of the observation does not necessarily constitute concurrence with the observation. It acknowledges that the contractor has been made aware of the non-compliance. Government surveillance of tasks not listed in the Performance Matrix or by methods other than those listed in the Performance Matrix (such as provided in the Inspection clause) may occur during the performance period of this task order. Such surveillance shall be done according to standard inspection procedures or other task order provisions. Any action taken by the CO as a result of surveillance shall be according to the terms of the task order.

7.4 Expertise and Certifications - CDC desires to obtain expert IT consulting services to provide process improvement recommendations to also include a comparative analysis of ITSO's IT Customer Satisfaction services to other Government and nongovernment IT organizations'. It is vital the contractor have a large and growing base of both Government and nongovernment IT organizations in order to

ensure that accurate comparisons utilizing current IT data are performed. The contractor shall have certifications or skills in the following areas:

- At minimum substantial proven client base and IT Metric data which has been collected over the last 10 years and includes Government and nongovernment IT organizations. This shall ensure proper comparisons are made along geographic, workload / complexity, size (economies of scale), industry or public sector points of view, as well as, outsourcing alternatives and best in class participant subsets.
- Large repository of up-to-date IT Metrics data to ensure a comparison of a true peer group of participants, managing handling similar levels of workload and complexity.
- Information Technology Customer Satisfaction (ITCS) analysis should be a core competency. The measurement service provider must be independent and objective. The simple concept of objectivity guides all benchmark assessments. The measurement service provider must not favor any single IT product, supplier, group of IT suppliers or computing architecture, but accurately provides enterprises with a credible means of evaluating options to intelligently reduce IT costs. That means that a measurement service provider must have no alliances with hardware, software or service providers that might cause them to have a vested interest in the results of the analysis.
- Contractor must be experienced in validating and analyzing data, and possess a comprehensive understanding of IT environments from both a quantitative and qualitative perspective.
- Possess a proven process and methodology in benchmarking analysis.

7.5 **TRAVEL:** Travel is to be reimbursed only in accordance with the Federal Travel Regulations. All travel must be authorized by the COR and be in compliance with the task order and all other applicable requirements. The contractor shall ensure that the requested travel costs shall not exceed the amount authorized in this task order.

7.6 **Privacy Act:** Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy act, Title 5 of the U.S. Code,
Section 552a and applicable agency rules and regulations.

7.7 **Problem Resolution:** The contractor shall bring problems, or potential issues, affecting performance to the attention of the COR and Contracting Officer as soon as possible. Verbal reports shall be followed up with written reports when directed. This notification shall not relieve the Contractor of its responsibility to correct problems for which they are responsible. The Contractor shall work cooperatively with the Government to resolve issues as they arise.

7.8 **Section 508:** The Contractor shall support the Government in its compliance with Section 508 throughout the development and implementation of the work to be performed. Items need to meet Section 508 standards for web based development 36CFR1194.22, 36CFR1194.31, and 36CFR1194.41. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is

comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

The Contractor should review the following Web sites for additional Section 508 information:

http://www.section508.gov/index.cfm?FuseAction=Content&ID=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

8.0 Historical Data. The Government estimates that base year requirements shall involve a level-of-effort delineated below: (Current firm workload and support requirements). **However, offeror's are advised to conduct their own analysis of these requirements, and propose amounts based its own independent assessments.**

Base Year		**Years 2 - 5**
1750– 2,000 surveys		1750– 2,000 surveys

9.0 TASK ORDER CLOSEOUT: The contractor shall submit a final invoice within forty-five (45) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.