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

1.0 BACKGROUND: As the Centers for Disease and 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. ITSO provides consolidated IT infrastructure support contracts, consulting services, technical advice and assistance across CDC in the effective and efficient use of IT infrastructure technologies. ITSO also develops CDC's IT infrastructure architecture; maintains state-of-the-art expertise in information science and technology, conducts research and development, performs evaluation and testing of new IT infrastructure technologies to support CDC's mission.

CDC/ITSO requires an IT Customer Satisfaction Assessment, (ITCS) to determine the current satisfaction level of its IT services. The results of the assessments are used to optimize the current service levels for the organization. At the conclusion of the analysis, CDC ITSO will have an enterprise-wide and comprehensive perspective of end user customer satisfaction levels. The results of the survey will aid in achieving operating and efficiency goals**.**

1.2. OBJECTIVE: The objective of this requirement is to engage in an enterprise-wide CDC measure of ITCS and then benchmark the results against other Government Agencies and non Government organizations. All end-users, approximately 16,000 employees, (excluding ITSO and OCISO) will be invited to participate in the assessment. The IT Customer Satisfaction benchmark will assess end-user satisfaction with IT services delivered by ITSO staff. At the conclusion of the analysis, CDC will have an enterprise-wide and comprehensive perspective of end-user customer satisfaction levels.

1.3 TASK ORDER TYPE: Firm Fixed Price

1.4 PERIOD OF PERFORMANCE: The period of performance for the base period shall be twelve months (12) with four (4) subsequent one-year option periods through 31 July 2015. Option periods will address the recurring assessment analysis as required.

The period of performance shall be for a base period and four (4) option periods shall be :

Base Period:	August 01, 2010 – July 31, 2011
Option 1:	August 01, 2011 – July 31, 2012
Option 2	August 01, 2012 – July 31, 2013
Option 3:	August 01, 2013 – July 31, 2014
Option 4:	August 01, 2014 – July 31, 2015

2.0 SCOPE OF WORK: The scope of the task order is to develop a web-based, electronic customer satisfaction assessment, invite participants, collect and analyze the data, report findings and develop recommendations for improvement. In addition the assessment will be measured against

other IT organization in the Federal Government and the private sector. 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, customer service satisfaction survey using a standard set of service criteria to measure satisfaction with specific services. The assessment shall also include demographic data. ITSO will provide both the demographic, service and system criteria.

3.2 **DATA COLLECTION**: The contractor shall initiate the collection of data by sending an email (containing a direct link to the web-based survey and timelines for responding) to all CDC staff requesting participation. Participation is voluntary and anonymous. The contractor shall send reminders to those who have not participated as deemed necessary.

3.2.1 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 Technical Representative (COTR) shall be notified if there are difficulties obtaining access to documents or personnel that will impact the negotiated project completion schedule. An overview of participation shall be provided to the Project Officer or other designated staff on a daily basis.

3.3.1 ANALYSIS/ASSESSMENT INTERIM REPORTS

3.3.1 The contractor shall provide a detailed analysis and assessment of all criteria gathered for the Customer Satisfaction Survey including comparing the data to other governmental and nongovernmental survey results. The analysis shall compare customer satisfaction data against the database average.

3.3.2 The contractor shall provide a detailed analysis and the resulting recommendations for all relevant information. The results shall be compiled into a draft presentation.

3.3.3 The contractor shall present the draft results along with the raw data to COTR. This will be an interim review to discuss important findings in order to receive feedback and will 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.

3.3.4 The contractor shall look at the historical data and provide a trend analysis of the ITSO ITCS.

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 COTR for review and comment, incorporating comments as appropriate. This will include all recommendations for improvement.

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 Deployment	Accurate and complete customer satisfaction survey utilizing established standard set of service criteria to measure satisfaction with a specific service to include demographic data provided 90 days from the start of the contract.	No deviation	100% Government inspection
PWS 3.2 Data collection	Data collection assessment provided 30 days from the start of the contract and every quarter thereafter.	95%	Periodic Review
PWS 3.2.1 Analysis/Assessment	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 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 schedule and no more than one (1) day late	95%	100% Government inspection
PWS 3.4 Final report and Recommendations	Clear concise report prepared in a professional format and exhibiting easy to read, easy to understand data. submitted for review per the delivery schedule and no more than one (1) day late	95%	100% Government inspection

5.0 TASK ORDER DELIVERABLES: All deliverables shall be delivered to the COTR 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 COTR 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 COTR and Procurement and Grants Office, PGO, Contracting Officer.

All documents, plan, diagrams, presentations, etc. are to be submitted solely in electronic form and in the native file format of MS Word 2003 - 2007, MS Excel 2003 - 2007, MS Visio 2003 - 2007, MS project 2003 - 2007, or MS PowerPoint2003 - 2007 – or later versions of those packages. Also, provide hard copies as needed.

Deliverables will be submitted to the COTR. Name and e-mail information will be provided after award of task order.

5.1 DELIVERABLES

Title	Due Date (
Deliverable or Required Services	
Startup Meeting Agenda	10 days after award of task order
Web based Customer Satisfaction Survey	60 days after award
Data collection Assessment	90 days after award
Interim Report	6 months after award
Final Report	15 days prior to end of POP
Monthly Status Report (MSR)	Within ten (10) business days following the close of the preceding month

5.2 Initial Business and Technical Meeting: Within ten (10) business days following the task award date, contractor will meet with the COTR and Technical Monitor, to review goals and objectives of this task order, and to discuss technical requirements.

6.0 RECORDS/DATA: All data rights associated with this effort will be property of the CDC, ITSO Atlanta, GA

7.0 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.

7.1. 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.

7.1.2 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

7.1.3 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 1 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/COTR, 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.

7.1.4 Information Security Training: HHS 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.

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

7.1.6 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/COTR 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 or the Project Administrative Office (ASPO) for location of the depositories for the return of badges. Cardkeys shall be returned to the appropriate Office.

Final payment shall be withheld in the amount of $500.00 for each badge or cardkey issued until all badges and cardkeys are returned to appropriate CDC Office. The Project Officer shall be responsible for monitoring this activity.

7.1.7 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.

7.1.8 **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 1: 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.

7.1.9 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

7.1.10 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.

8.0 TASK ORDER TERMS AND CONDITIONS:

8.1 Place of Performance: The majority of work shall be accomplished in the Contractor provided facilities.

8.1.2 Hours of Operation: Work is to be performed at the contractor's site.

8.2 Inspection and Acceptance: Inspection and acceptance will occur in accordance with 52.212-4(a). In the absence of other agreements negotiated with respect to time provided for government review, deliverables will be inspected and the contractor notified of the ITSO, Project Manager's findings within five (5) work days of normally scheduled review. If the deliverables are not acceptable, the COTR will 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.

8.3 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 COTR for acceptance not later than ten (10) calendar days after award. The ITSO COTR will 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.

8.3.1 Quality Assurance: The Government will evaluate the contractor's performance of this task order. For those tasks listed in the Performance Matrix, the COTR or other designated evaluator will follow the method of surveillance specified in this task order. Government personnel will record all surveillance observations. When an observation indicates defective performance, the COTR or other designated evaluator will 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 will be done according to standard inspection procedures or other task order provisions. Any action taken by the CO as a result of surveillance will be according to the terms of the task order.

8.4 Expertise and Certifications - The contractor shall have certifications or skills in the following areas: CDC desires to obtain comparative analysis to compare CDC Customer Satisfaction to "best in class" organizations. Therefore, it is absolutely vital that the measurement service provider has a large and growing base of participants in order to ensure that accurate comparisons utilizing current data are performed. At a minimum the contractor shall have:

- At least 300 clients to help 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 and accurate information assures each participant that their distributed environment will be compared with 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, not a small practice area. 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 the CDC, IT environments from both a quantitative and qualitative perspective.
- Possess a proven process and methodology in benchmarking analysis.

8.4.1 Key Personnel: The contractor shall identify key personnel in their quote. Any substitution of key personnel must be of equally or better qualified individuals as those identified in the contractor's original quote.

8.5 Government Furnished Items and Information: Work will be performed at the contractor's choice of location. If any additional government furnished items are needed by the contractor, they should be identified in the contractor's proposal

8.5.1 Contractor Furnished Items: Except for those items or services stated in section 8.5 as Government furnished, the contractor must furnish everything needed to perform this contract according to all its terms.

8.5.2 Support Items: Support Items are categories of charges utilized by the contractor in the performance of the contract service. Support Items are ancillary in nature and integrally related to the contractor's ability to perform the service being acquired, i.e., they must be necessary for the completion of the task. Acquisition of Support Items cannot be the primary purpose of a task order. The Contract Support Items (CSI) must satisfy the criteria expressed within the scope of

the contract/task order. Support Items must not duplicate cost covered in other areas of the contract. - No CSI are anticipated.

8.5.3 Open Market (Non-Schedule) Items: Open Market Items are any item or labor category offered by the Contractor that is not awarded and priced under their Contract or a Teaming Partner's Contract. These items must be competed in accordance with FAR requirements if their cumulative total over the life of the contract exceeds or is expected to exceed $3,000.00. The contractor shall provide a breakdown of any Open Market Items and their cost(s) in their Price Quote. Requests for Open Market Items must first be reviewed and approved by the Contracting Officer.

Open Market Items must be necessary and integral with the overall service being performed in the task order. All Open Market Items must be itemized in the offeror's quote. No Open Market Items are anticipated under this task and the offeror should not quote any.

The Contractor is strongly encouraged to have necessary Open Market Items added under their Schedule Contract as a CSI or to seek a Contractor Teaming Arrangement with another Schedule Contract instead of offering Open Market Items or labor categories not on the contractor's schedule.

8.6 TRAVEL: Travel is to be reimbursed only in accordance with the Federal Travel Regulations. All travel must be authorized by the COTR and be in compliance with the task order and all other applicable requirements. The contractor shall ensure that the requested travel costs will not exceed the amount authorized in this task order. No G&A or other percentage markup will be allowed on travel (unless specifically negotiated or approved in your FSS Schedule award) since applicable G&A expenses should already be included in the contract labor rates

8.6.1 Travel for Contractor Personnel: The budget for the Contractor travel under this task order is:

Base Period	$4,000
Option One	$4,000
Option Two	$4,000
Option Three	$4,000
Option Four	$4,000

8.6.2 Travel for Contractor Personnel: The budget for the Contractor travel under this task order is $20,000.00 for 60 months.

8.7 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.

8.8 Personal Service: This solicitation and resulting contract is for the procurement of IT consulting services and shall not being used to procure personal services which are prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled "Personal Services Contract".

8.9 Problem Resolution: The contractor shall bring problems, or potential issues, affecting performance to the attention of the CR and GSA PM as soon as possible. Verbal reports will 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 will work cooperatively with the Government to resolve issues as they arise.

8.10 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 in the *ITSO, COTR via* electronic mail. The COTR will be identified at the startup meeting.

8.10.1 Monthly Status Report (MSR): The MSR shall contain the following information:

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

9.0 INVOICES

9.1 Invoices - Payment by Electronic Funds Transfer (May 1999)

a. The Government shall use electronic funds transfer to the maximum extent possible when making payments under this contract. FAR 52.232-34, Payment by Electronic Funds Transfer–Other than Central Contractor Registration, incorporated by reference the Contractor shall designate in writing a financial institution for receipt of electronic funds transfer payments.

b. The Contractor shall make the designation by submitting the form titled "ACH Contractor/Miscellaneous Payment Enrollment Form" to the address indicated below. Note: The form may be obtained by contacting the CDC Financial Management Office at (404) 687-6666.

c. In cases where the Contractor has previously provided such designation, i.e., pursuant to a prior contract/order, and been enrolled in the program, the form is not required.

d. The completed form shall be mailed after award, but no later than 14 calendar days before an invoice is submitted, to the following address:

Centers for Disease Control and Prevention
Attention: Financial Management Office
Post Office Box 15580
Atlanta, Georgia 30333

9.2 Voucher/Invoice Submission: The Contractor is required to submit a copy of each invoice directly to the Project Officer, Financial Management Office and the Contracting Officer. The date of receipt of an invoice by the Financial Management Office shall determine whether interest is required under the Prompt Payment Act.

All original invoices or vouchers must be submitted to the Financial Management Office at the address show below:

The Centers for Disease Control and Prevention Financial Management Office (FMO)
P.O. Box 15580
Atlanta, GA 30333

Or

The Contractor may submit the original invoice/voucher or progress payment via facsimile or email:

Fax: 404-638-5324 Email: FMOAPINV@CDC.GOV

NOTE: Submit to only one (1) of the above locations.

In addition, the contractor shall submit 2 copies of the invoice/voucher or progress payment to the cognizant contracting office identified in this contract. These invoices/voucher copies shall be addressed to the attention of the Contracting Officer.

9.2.1 For an invoice to be accepted by the FMO the following information shall be on each invoice.

(1) Contractor's Name & Address
(2) Contractor's Tax Identification Number (TIN)
(3) Contract Number
(4) Invoice Number
(5) Invoice Date
(6) Task Number
(7) Contract Line Item Number /labor category
(8) Quantity
(9) Unit Price & Extended Amount for each line item
(10) Total Amount of Invoice
(11) Name, title and telephone number of person to be notified in the event of a defective invoice
(12) Payment Address,
(13) Contractor's DUNS number

9.1.2.1 The contractor shall be entitled to bill the monthly amount(s) for the services performed. The Government reserves the right to withhold payments if the contractor is not meeting all requirements or if performance is unsatisfactory.

REMINDER: **The original and each copy should be easily identifiable. Vouchers should be *collated*. Failure to submit vouchers in the proper format shall delay your payment.**

10.0 EARNED VALUE MANAGEMENT: Earned Value Management of this task shall consist of organizing and breaking down the complete scope of work into performance and deliverables based on the tasks and the performance matrix.

In accordance with Earned Value Management (EVM) principles, success shall be measured by the completion of the deliverables, performance and acceptance by the Government. As stated in the aforementioned guidelines, "The intent is to provide management information using existing company resources and a scaled EVMS application that achieves the project requirements and is compliant the EVMS principles. EVMS scalability is viewed as a spectrum employing the principles of EVMS guidelines to large complex and/or high risk projects allowing any project regardless of size and complexity to realize the benefits of earned value management." "The essence of Earned Value Management is that at some level of detail within the Work Breakdown Structure, appropriate for the degree of technical, schedule and cost risk, or uncertainty associated with the project, a target planned value is established for each scheduled element of work. As these elements of work are completed, their target planned values are "earned." As such, work

progress is quantified and the earned value becomes a metric against which to measure both what has been spent to perform the work and what was scheduled to have been accomplished."

As part of the requirement of this project, the Government is requiring the Contractor to use EVM guidelines to effectively integrate the scope of work with the performance matrix established for this project to achieve optimum project planning and control. The principles to be utilized by the Contractor shall be as outlined below:

- Plan all activities for this project from award through completion.
- Breakdown the project work scope into finite pieces that can be assigned a responsible person or group for the purpose of the control of deliverables and work objectives.
- Integrate project work scope and schedule objectives into a performance measurement plan against which milestones can be measured and changes can be controlled.

11.0 GENERAL AND SPECIAL CONTRACT CLAUSES.

11.1 GENERAL CLAUSES:

52.217-8 Option to Extend Services. (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six (6) months. The Contracting Officer may exercise the option by written notice to the Contractor within thirty (30) calendar days of the end of the task order.

11.2 52.217-9 Option to Extend the Term of the Contract. (Mar 2000)
(a) The Government may extend the term of this contract by written notice to the Contractor within thirty (30) calendar days before the contract expires; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires. The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed three (3) years.

12.0 Historical Data. The Government estimates that base year requirements will 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

13.0 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.