Attachment F:

Information Security Plan

Security Requirements for Federal Information Technology Resources
[January 2010; Health and Human Services Acquisition Regulation (HHSAR), Clause 352.239-72]

All data collection systems and practices will adhere to all applicable federal, HHS, CDC, and NIOSH IT security policies and procedures. The security requirements are first described below. Development or implementation of an electronic information system or any electronic data collection effort conducted in the performance of this proposed study will be required to complete Certification and Accreditation (C&A) prior to operation. Contractors would comply with applicable 508 requirements. If an application or system is operated by the Contractor on behalf of the government and/or hosted at a contractor facility, it must comply with HHS, CDC, and NIOSH policies, and is subject to all OMB requirements, including Certification and Accreditation (C&A). All IT and telecommunications equipment, services, and related software acquired under this contract must conform to applicable Federal Information Processing Standards Publications (FIPS PUBS). FIPS Standards can be found at http://www.itl.nist.gov/fipspubs. Since a portion of the system may be developed under contract, requirements described below apply to both potential contractors and NIOSH employees.

Contractor Responsibilities

(a) **Applicability**. This clause applies whether the entire contract or order (hereafter "contract"), or portion thereof, includes information technology resources or services in which the Contractor has physical or logical (electronic) access to, or operates a Department of Health and Human Services (HHS) system containing, information that directly supports HHS' mission. The term "information technology (IT)", as used in this clause, includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources. This clause does not apply to national security systems as defined in Federal Information Security Management Act of 2002 (FISMA).

(b) **Contractor responsibilities**. The Contractor is responsible for the following:

(1) Protecting federal information and federal information systems in order to ensure their —

(i) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

(ii) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and.

(iii) Availability, which means ensuring timely and reliable access to and use of information.

(2) Providing security of any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor, regardless of location, on behalf of HHS.

(3) Adopting, and implementing, at a minimum, the policies, procedures, controls, and standards of the HHS Information Security Program to ensure the integrity, confidentiality, and availability of federal information and federal information systems for which the Contractor is responsible under this contract or to which it may otherwise have access under this contract. The HHS Information Security Program is outlined in the HHS Information Security Program Policy, which is available on the HHS Office of the Chief Information Officer's (OCIO) website.

(c) **Contractor security deliverables**. In accordance with the timeframes specified, the Contractor shall prepare and submit the following security documents to the Contracting Officer for review, comment, and acceptance:

(1) **IT Security Plan (IT-SP)** – due within 30 days after contract award. The IT-SP shall be consistent with, and further detail the approach to, IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The IT-SP shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of IT resources that are developed, processed, or used under this contract. If the

IT-SP only applies to a portion of the contract, the Contractor shall specify those parts of the contract to which the IT-SP applies.

(i) The Contractor's IT-SP shall comply with applicable federal laws that include, but are not limited to, the **Federal Information Security Management Act (FISMA) of 2002** (PDF) (Title III of the E-Government Act of 2002, Public Law 107-347), and the following federal and HHS policies and procedures:

(A) Office of Management and Budget **(OMB) Circular A-130**, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources.

(B) National Institute of Standards and Technology (NIST) **Special Publication (SP) 800-18** (PDF), Guide for Developing Security Plans for Federal Information Systems, in form and content, and with any pertinent contract Statement of Work/Performance Work Statement (SOW/PWS) requirements. The IT-SP shall identify and document appropriate IT security controls consistent with the sensitivity of the information and the requirements of **Federal Information Processing Standard (FIPS) 200**, Recommended Security Controls for Federal Information Systems. The Contractor shall review and update the IT-SP in accordance with **NIST SP 800-26,** Security Self-Assessment Guide for Information Technology Systems and FIPS 200, on an annual basis.

(C) **HHS-OCIO Information Systems Security and Privacy Policy.**

(ii) After resolution of any comments provided by the Government on the draft IT-SP, the Contracting Officer shall accept the IT-SP and incorporate the Contractor's final version into the contract for Contractor implementation and maintenance. On an annual basis, the Contractor shall provide to the Contracting Officer verification that the IT-SP remains valid.

(2) **IT Risk Assessment (IT-RA)** – due within 30 days after contract award. The IT-RA shall be consistent, in form and content, with **NIST SP 800-30**, Risk Management Guide for Information Technology Systems, and any additions or augmentations described in the HHS-OCIO Information Systems Security and Privacy Policy. After resolution of any comments provided by the Government on the draft IT-RA, the Contracting Officer shall accept the IT-RA and incorporate the Contractor's final version into the contract for Contractor implementation and maintenance. The Contractor shall update the IT-RA on an annual basis.

(3) **FIPS 199 Standards for Security Categorization of Federal Information and Information Systems Assessmen**t (FIPS 199 Assessment) – due within 30 days after contract award. The FIPS 199 Assessment shall be consistent with the cited NIST standard. After resolution of any comments by the Government on the draft FIPS 199 Assessment, the Contracting Officer shall accept the FIPS 199 Assessment and incorporate the Contractor's final version into the contract.

(4) **IT Security Certification and Accreditation (IT-SC&A)** – due within 3 months after contract award. The Contractor shall submit written proof to the Contracting Officer that an IT-SC&A was performed for applicable information systems – see paragraph (a) of this clause. The Contractor shall perform the IT-SC&A in accordance with the HHS Chief Information Security Officer's Certification and Accreditation Checklist; **NIST SP 800-37**, Guide for the Security Certification and Accreditation of Federal Information Systems; and **NIST SP 800-53,** Recommended Security Controls for Federal Information Systems. An authorized senior management official shall sign the draft IT-SC&A and provide it to the Contracting Officer for review, comment, and acceptance.

(i) After resolution of any comments provided by the Government on the draft IT-SC&A, the Contracting Officer shall accept the IT-SC&A and incorporate the Contractor's final version into the contract as a compliance requirement.

(ii) The Contractor shall also perform an annual security control assessment and provide to the Contracting Officer verification that the IT-SC&A remains valid. Evidence of a valid system accreditation includes written results of (A) annual testing of the system contingency plan and (B) the performance of security control testing and evaluation.

(d) **Personal identity verification**. The Contractor shall identify its employees with access to systems operated by the Contractor for HHS or connected to HHS systems and networks. The Contracting Officer's Technical Representative (COTR) shall identify, for those identified employees, position sensitivity levels that are commensurate with the responsibilities and risks associated with their assigned positions. The Contractor shall comply with the HSPD-12 requirements contained in "HHS-Controlled Facilities and Information Systems Security" requirements specified in the SOW/PWS of this contract.

(e) **Contractor and subcontractor employee training**. The Contractor shall ensure that its employees, and those of its subcontractors, performing under this contract complete HHS-furnished initial and refresher security and privacy education and awareness training before being granted access to systems operated by the Contractor on behalf of HHS or access to HHS systems and networks. The Contractor shall provide documentation to the COTR evidencing that Contractor employees have completed the required training.

(f) **Government access for IT inspection**. The Contractor shall afford the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of this contract to the extent required to carry out a program of IT inspection (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the integrity, confidentiality, and availability, of HHS data or to the protection of information systems operated on behalf of HHS.

(g) **Subcontracts.** The Contractor shall incorporate the substance of this clause in all subcontracts that require protection of federal information and federal information systems as described in paragraph (a) of this clause, including those subcontracts that—

(1) Have physical or electronic access to HHS' computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, process, or exchange data with HHS or on behalf of HHS, regardless of whether the data resides on a HHS or the Contractor's information system.

(h) **Contractor employment notice**. The Contractor shall immediately notify the Contracting Officer when an employee either begins or terminates employment (or is no longer assigned to the HHS project under this contract), if that employee has, or had, access to HHS information systems or data.

(i) **Document information**. The Contractor shall contact the Contracting Officer for any documents, information, or forms necessary to comply with the requirements of this clause.

(j) **Contractor responsibilities upon physical completion of the contract**. The Contractor shall return all HHS information and IT resources provided to the Contractor during contract performance and certify that all HHS information has been purged from Contractor-owned systems used in contract performance.

(k) **Failure to comply**. Failure on the part of the Contractor or its subcontractors to comply with the terms of this clause shall be grounds for the Contracting Officer to terminate this contract.

Rehabilitation Act Section 508 Compliance

Section 508 of the Rehabilitation Act requires that, unless certain exceptions apply, when Federal agencies develop, acquire, maintain, or use Electronic and Information Technology (EIT) products and services:

(1) individuals with disabilities who are Federal employees have access to and use of information and data that is comparable to the access to and use of the information and data by Federal employees who are not individuals with disabilities; and

(2) individuals with disabilities who are members of the public seeking information or services from a Federal department or agency have access to and use of information and data that is comparable to the access to and use of the information and data by such members of the public who are not individuals with disabilities (FAR 39.201 and 36 CFR 1194.1).