shall ensure that each of its employees, and any subcontractor staff, is made aware of, understand, and comply with the provisions of the Act.

(End of clause)

352.239–70 Standard for security configurations.

As prescribed in *339.101(d)(1)*, the Contracting Officer shall insert the following clause:

STANDARD FOR SECURITY CONFIGURATIONS (JANUARY 2010)

(a) The Contractor shall configure its computers that contain HHS data with the applicable Federal Desktop Core Configuration (FDCC) (*see http://nvd.nist.gov/fdcc/index.cfm*) and ensure that its computers have and maintain the latest operating system patch level and anti-virus software level.

NOTE: FDCC is applicable to all computing systems using Windows XP™ and Windows Vista™, including desktops and laptops—regardless of function—but not including servers.

(b) The Contractor shall apply approved security configurations to information technology (IT) that is used to process information on behalf of HHS. The following security configuration requirements apply:

NOTE: The Contracting Officer shall specify applicable security configuration requirements in solicitations and contracts based on information provided by the Project Officer, who shall consult with the OPDIV/STAFFDIV Chief Information Security Officer.

(c) The Contractor shall ensure IT applications operated on behalf of HHS 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—*see http://nvd.nist.gov/validation.cfm*. 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 products meet the latest FDCC major version and subsequent major versions.

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

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

(f) The Contractor shall (1) include Federal Information Processing Standard (FIPS) 201-compliant (*see http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf*), Homeland Security Presidential Directive 12 (HSPD–12) card readers with the purchase of servers, desktops, and laptops; and (2) comply with FAR Subpart 4.13, *Personal Identity Verification*.

(g) The Contractor shall ensure that its subcontractors (at all tiers) which perform work under this contract comply with the requirements contained in this clause.

(End of clause)

[74 FR 62398, Nov. 27, 2009, as amended at 75 FR 21511, Apr. 26, 2010]

352.239–71 Standard for encryption language.

As prescribed in *339.101(d)(2)*, the Contracting Officer shall insert the following clause:

STANDARD FOR ENCRYPTION LANGUAGE (JANUARY 2010)

(a) The Contractor shall use Federal Information Processing Standard (FIPS) 140–2-compliant encryption (Security Requirements for Cryptographic Module, as amended) to protect all instances of HHS sensitive information during storage and transmission. (NOTE: The Government has determined that HHS information under this contract is considered ''sensitive'' in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.)

(b) The Contractor shall verify that the selected encryption product has been validated under the Cryptographic Module Validation Program (*see 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 the Contracting Officer and the Contracting Officer's Technical Representative.

(c) The Contractor shall use the Key Management Key (*see* FIPS 201, Chapter 4, as amended) 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 (*see http://csrc.nist.gov/drivers/documents/ombencryption-guidance.pdf*). The Contractor shall notify the Contracting Officer and the Contracting Officer's Technical Representative of personnel authorized to decrypt and recover all encrypted information.

(d) The Contractor shall securely generate and manage encryption keys to prevent unauthorized decryption of information in accordance with FIPS 140–2 (as amended).

(e) The Contractor shall ensure that this standard is incorporated into the Contractor's property management/control system or establish a separate procedure to account for all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive HHS information.

(f) The Contractor shall ensure that its subcontractors (at all tiers) which perform work under this contract comply with the requirements contained in this clause.

(End of clause)

[74 FR 62398, Nov. 27, 2009, as amended at 75 FR 21511, Apr. 26, 2010]

352.239–72 Security requirements for Federal information technology resources.

As prescribed in *339.7103*, the Contracting Officer shall insert the following clause:

SECURITY REQUIREMENTS FOR FEDERAL INFORMATION TECHNOLOGY RESOURCES (JANUARY 2010)

(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 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) Web site.

(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 (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, 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