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.