

Health and Human Services

352.237-72

the age of 18. The statutory prohibition also applies to indoor facilities that are constructed, operated, or maintained with Federal funds.

(b) By acceptance of this contract or order, the Contractor agrees to comply with the requirements of the Act. The Act also applies to all subcontracts awarded under this contract for the specified children's services. Accordingly, the Contractor shall ensure that each of its employees, and any subcontractor staff, is made aware of, understand, and comply with the provisions of the Act. Failure to comply with the Act may result in the imposition of a civil monetary penalty in an amount not to exceed \$1,000 for each violation and/or the imposition of an administrative compliance order on the responsible entity. Each day a violation continues constitutes a separate violation.

(End of clause)

352.237-71 Crime Control Act—reporting of child abuse.

As prescribed in 337.103-70(b), the Contracting Officer shall insert the following clause:

CRIME CONTROL ACT OF 1990—REPORTING OF CHILD ABUSE (JANUARY 2006)

(a) *Public Law 101-647, also known as the Crime Control Act of 1990 (Act)*, imposes responsibilities on certain individuals who, while engaged in a professional capacity or activity, as defined in the Act, on Federal land or in a Federally-operated (or contracted) facility, learn of facts that give the individual reason to suspect that a child has suffered an incident of child abuse.

(b) The Act designates “covered professionals” as those persons engaged in professions and activities in eight different categories including, but not limited to, physicians, dentists, medical residents or interns, hospital personnel and administrators, nurses, health care practitioners, chiropractors, osteopaths, pharmacists, optometrists, podiatrists, emergency medical technicians, ambulance drivers, alcohol or drug treatment personnel, psychologists, psychiatrists, mental health professionals, child care workers and administrators, and commercial film and photo processors. The Act defines the term “child abuse” as the physical or mental injury, sexual abuse or exploitation, or negligent treatment of a child.

(c) Accordingly, any person engaged in a covered profession or activity under an HHS contract or subcontract, regardless of the purpose of the contract or subcontract, shall immediately report a suspected child abuse incident in accordance with the provisions of the Act. If a child is suspected of being harmed, the appropriate State Child Abuse Hotline, local child protective services

(CPS), or law enforcement agency shall be contacted. For more information about where and how to file a report, the Childhelp USA, National Child Abuse Hotline (1-800-4-A-CHILD) shall be called. Any covered professional failing to make a timely report of such incident shall be guilty of a Class B misdemeanor.

(d) By acceptance of this contract or order, the Contractor agrees to comply with the requirements of the Act. The Act also applies to all applicable subcontracts awarded under this contract. Accordingly, the Contractor 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)

352.237-72 Crime Control Act—requirement for background checks.

As prescribed in 337.103-70(c), the Contracting Officer shall insert the following clause:

CRIME CONTROL ACT OF 1990—REQUIREMENT FOR BACKGROUND CHECKS (JANUARY 2006)

(a) *Public Law 101-647, also known as the Crime Control Act of 1990 (Act)*, requires that all individuals involved with the provision of child care services to children under the age of 18 undergo a criminal background check. “Child care services” include, but are not limited to, social services, health and mental health care, child (day) care, education (whether or not directly involved in teaching), and rehabilitative programs. Any conviction for a sex crime, an offense involving a child victim, or a drug felony, may be grounds for denying employment or for dismissal of an employee providing any of the services listed above.

(b) The Contracting Officer will provide the necessary information to the Contractor regarding the process for obtaining the background check. The Contractor may hire a staff person provisionally prior to the completion of a background check, if at all times prior to the receipt of the background check during which children are in the care of the newly-hired person, the person is within the sight and under the supervision of a previously investigated staff person.

(c) By acceptance of this contract or order, the Contractor agrees to comply with the requirements of the Act. The Act also applies to all applicable subcontracts awarded under this contract. Accordingly, the Contractor 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).