<?xml encoding="UTF-8">

852.239-72 Information System Design and Development.

As prescribed in 839.106-70, insert the following clause:

Information System Design and Development (FEB 2023)

(a) *Design or development at non-VA facilities.* Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with the Federal Information Security Modernization Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA) regulations, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic protected health information (PHI), outlined in 45 CFR part 164, subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization and the Trusted Internet Connections (TIC) Reference Architecture).

(b) *Privacy Impact Assessment.* During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

(c) *Security of procured or developed systems and technologies.* The Contractor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of the contract and any extension, warranty, or maintenance periods. This includes, but is not limited to, workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the Contractor anywhere in the Systems, including Operating Systems and firmware. The Contractor shall ensure that Security Fixes shall not negatively impact the Systems.

(d) *Subcontract flow down requirements.* The Contractor shall include the clause at 52.224-1, Privacy Act Notification, in every solicitation and/or subcontract awarded by the Contractor when the clause FAR 52.224-1 is included in its contract.

(End of clause)

Parent topic: Subpart 852.2 - Text of Provisions and Clauses