852.239-70 Security Requirements for Information Technology Resources.

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

Security Requirements for Information Technology Resources (FEB 2023)

(a) *Definitions.* As used in this clause—

Information technology has the same meaning in FAR 2.101 and also *means* Information and Communication Technology (ICT).

Information system security plan means a formal document that provides an overview of the security equirements for an information system and describes the security controls in place or planned for meeting those requirements.

(b) *Responsibilities.* The Contractor shall be responsible for information system security for all systems connected to a Department of Veterans Affairs (VA) network or operated by the Contractor for VA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or other system access to VA information that directly supports the mission of VA. Examples of tasks that require security provisions include—

(1) Hosting of VA e-Government sites or other information technology operations;

(2) Acquisition, transmission, or analysis of data owned by VA with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to VA general support systems/major applications at a level beyond that granted the general public, *e.g.,* bypassing a firewall.

(c) *Information system security plan.* The Contractor shall develop, provide, implement, and maintain an Information System Security Plan. VA information systems must have an information system security plan that provides an overview of the security requirements for the system and describes the security controls in place or the plan for meeting those requirements. This plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of information system resources developed, processed, or used under this contract. The information system security plan should include implementation status, responsible entities, resources, and estimated completion dates. Information system security plans may also include, but are not limited to, a compiled list of system characteristics, and key security-related documents such as a risk assessment, PIA, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. The plan shall address the specific contract requirements regarding information systems related support or services included in the contract, to include the performance work statement (PWS) or statement of work (SOW). The Contractor's Information System Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Modernization Act (FISMA) of 2014 and the E-Government Act of 2002. The plan shall meet information system security requirements in accordance with Federal and VA policies and procedures, and as amended during the term of this contract, and include, but are not limited to the following.

(1) OMB Circular A-130, Managing Information as a Strategic Resource;

(2) National Institute of Standards and Technology (NIST) Guidelines; and

(3) VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, Personnel Security and Suitability Program, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting VA information, information systems (see 802.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems.

(d) *Submittal of plan.* Within 90 days after contract award, the Contractor shall submit the Information System Security Plan to the Contracting Officer for review and approval.

(e) *Security accreditation.* As required by current VA policy, the Contractor shall submit written proof of information system security accreditation to the Contracting Officer for non-VA owned systems. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with VA policy available from the Contracting Officer upon request. The Contractor shall submit for acceptance by the Contracting Officer along with this accreditation a final information system security plan, such as a risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. The accreditation and the final information system security plan and the accompanying documents, such as a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan.

(f) *Annual validation.* On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the Information System Security Plan remains valid.

(g) *Banners.* The Contractor shall ensure that the official VA banners are displayed on all VA systems (both public and private) operated by the Contractor that contain Privacy Act information before allowing anyone access to the system. The Office of Information Technology will make official VA banners available to the Contractor.

(h) *Screening and access.* The Contractor shall screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for VA or interconnected to a VA network in accordance with VA Directives and Handbooks referenced in paragraph (c) of this clause.

(i) *Training.* The Contractor shall ensure that its employees performing services under this contract complete VA security awareness training on an annual basis. This includes signing an acknowledgment that they have read, understand, and agree to abide by the VA Information Security Rules of Behavior (VA National Rules of Behavior) as required by 38 U.S.C. 5723; FAR 39.105, Privacy; clause 852.204-71, Information and Information Systems Security, and this clause on an annual basis.

(j) *Government access.* The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. The Contractor shall provide access to enable a program of information system inspection (to include vulnerability testing), investigation and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of VA data or to the function of

information systems operated on behalf of VA), and to preserve evidence of computer crime.

(k) *Notification of termination of employees.* The Contractor shall immediately notify the Contracting Officer when an employee who has access to VA information systems or data terminates employment.

(l) *Subcontractor flow down requirement.* The Contractor shall incorporate and flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

Parent topic: Subpart 852.2—Text of Provisions and Clauses