852.239-73 Information System Hosting, Operation, Maintenance, or Use.

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

Information System Hosting, Operation, Maintenance, or Use (FEB 2023)

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

Assessment and Authorization (A&A) means the process used to ensure information systems including Major Applications and General Support Systems have effective security safeguards which have been implemented, planned for, and documented in an Information Technology Security Plan. The A&A process per applicable VA policies and procedures is the mechanism by which VA provides an Authorization to Operate (ATO), the official management decision given by the VA to authorize operation of an information system (see VA Handbook 6500 for additional details).

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

(b) *Hosting, operation, maintenance, or use at non-VA facilities.* For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/subcontractors are fully responsible and accountable for ensuring compliance with the applicable Health Insurance Portability and Accountability (HIPAA) Act of 1996 (HIPAA) Privacy and Security Rules, the Privacy Act and other required VA confidentiality statutes included in VA's mandatory yearly training and privacy handbooks, Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent to or exceed, those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to approval to operate. All external internet connections to VA's network involving VA information must be in accordance with the Trusted internet Connections (TIC) Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

(c) *Collecting, processing, transmitting, and storing of VA sensitive information.* Adequate security controls for collecting, processing, transmitting, and storing of VA sensitive information, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the Information System Security Plan and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection, processing, transmitting, and storing of VA sensitive information.

(d) *Annual FISMA security controls assessment.* The Contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the Privacy Impact Assessment. Any deficiencies noted during this

assessment must be provided to the Contracting Officer for entry into VA's POA&M management process. The Contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes specified by the VA in the performance work statement (PWS) or statement of work (SOW), or in the approved remediation plan through the VA POA&M process. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/subcontractor activities must also be subject to such assessments. The results of an annual review or a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500. This may require reviewing and updating all of the documentation as described in VA Handbook 6500.6 (*e.g.,* System Security Plan, Contingency Plan). See VA Handbook 6500.6 for a list of documentation. The VA Information System Risk Management (ISRM) office can provide guidance on whether a new A&A would be necessary.

(e) *Annual self-assessment.* The Contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. VA reserves the right to conduct such an assessment using government personnel or another Contractor/subcontractor. The Contractor/subcontractor must take appropriate and timely action, as may be specifically addressed in the contract, to correct or mitigate any weaknesses discovered during such testing, at no additional cost to the Government to correct Contractor/subcontractor systems and outsourced services.

(f) *Prohibition of installation and use of personally-owned or Contractor-owned equipment or software on VA networks.* VA prohibits the installation and use of personally-owned or Contractor/subcontractor-owned equipment or software on VA networks. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, PWS, SOW or contract. All of the security controls required for government furnished equipment (GFE) must also be utilized in approved other equipment (OE) at the Contractor's expense. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

(g) *Disposal or return of electronic storage media on non-VA leased or non-VA owned IT equipment.* All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with NIST 800-88, Rev. 1, “Guidelines for Media Sanitization,” and VA Directive 6500, VA Cybersecurity Program, paragraph 2(b)(5), Media Sanitization including upon -

(1) Completion or termination of the contract; or

(2) Disposal or return of the IT equipment by the Contractor/subcontractor or any person acting on behalf of the Contractor/subcontractor, whichever is earlier. Media (*e.g.,* hard drives, optical disks, CDs, back-up tapes) used by the Contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the Contractor/subcontractor must self-certify that the media has been disposed of per VA Handbook 6500.1 requirements. This must be completed within 30 days of termination of the contract.

(h) *Bio-Medical devices and other equipment or systems.* Bio-Medical devices and other equipment or systems containing media (*e.g.,* hard drives, optical disks) with VA sensitive information will not be returned to the Contractor at the end of lease, for trade-in, or other purposes. For purposes of these devices and protection of VA sensitive information the devices may be provided back to the Contractor under one of three scenarios -

(1) The Contractor must accept the system without the drive;

(2) A spare drive must be installed in place of the original drive at time of turn-in if VA's initial medical device purchase included a spare drive; or

(3) The Contractor may request reimbursement for the drive at a reasonable open market replacement cost to be separately negotiated by the Contracting Officer and the Contractor at time of contract closeout.

(End of clause)

Parent topic: Subpart 852.2 - Text of Provisions and Clauses