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 (DATE)

(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).

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

(b) Responsibilities. The Contractor shall be responsible for information technology 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 technology security plan. The Contractor shall develop, provide, implement, and maintain an Information Technology Security Plan. VA information system and platform information technology systems must have a 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. Generally, this plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of information technology resources developed, processed, or used under this contract. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a compiled list of system characteristics or qualities required for system registration, 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 technology and

information technology related support or services included in the contract, to include the PWS or SOW. The Contractor's Information Technology 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 technology 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 30 days after contract award, the Contractor shall submit the Information Technology 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 technology security accreditation to the Contracting Officer. 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 security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. The accreditation and accompanying documents, to include a final security plan, 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 IT 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).

(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 technology 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 technology 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)

852.239–72 Information System Design and Development.

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

Information System Design and Development (DATE)

(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 of 2014 and Federal Information Security Management 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.

(1) 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)

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 (DATE)

(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). Security plan means a formal document that provides an overview of the security requirements for an information system or an information security program 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 all applicable Health Insurance Portability and Accountability (HIPAA) Act of 1996 (HIPAA) regulations, the Privacy Act and other required VA confidentiality statutes included in VA's mandatory yearly training and privacy handbooks, FISMA, NIST, 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 PII. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, 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 Privacy Impact Assessment 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 of PII.

(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 or statement of work, 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 reauthorized 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 VA directives and handbooks 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)