852.204–71 Information and Information Systems Security.

As prescribed in 804.1903 insert the following clause:

Information and Information Systems Security (DATE)

(a) Definitions. As used in this clause—Business Associate means an entity, including an individual (other than a member of the workforce of a covered entity), company, organization or another covered entity, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, that performs or assists in the performance of a function or activity on behalf of the Veterans Health Administration (VHA) that involves the creating, receiving, maintaining, transmitting of, or having access to, protected health information (PHI). The term also includes a subcontractor of a business associate that creates, receives, maintains, or transmits PHI on behalf of the business associate. Business Associate Agreement (BAA) means the agreement, as dictated by the Privacy Rule, between VHA and a business associate, which must be entered into in addition to the underlying contract for services and before any release of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of VHA. Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual. Information technology (see FAR 2.101) also means Information and Communication Technology (ICT). Information technology-related contracts means those contracts which include services (including support services), and related resources for information technology as defined in 802.101. Privacy officer means the VA official with responsibility for implementing and oversight of privacy related policies and practices that impact a given VA acquisition. Sensitive personal information means, with respect to an individual, any information about the individual maintained by VA, including but not limited to the following:

(1) Education, financial transactions, medical history, and criminal or employment history.

(2) Information that can be used to distinguish or trace the individual’s identity, including but not limited to name, social security number, date and place of birth, mother’s maiden name, or biometric records. 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. VA Information Security Rules of Behavior for Organizational Users (VA National Rules of Behavior) means a set of VA rules that describes the responsibilities and expected behavior of users of VA information or information systems. VA sensitive information means all VA data, on any storage media

or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes sensitive personal information. The term includes information where improper use or disclosure could adversely affect the ability of VA to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following:

Individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

(b) General. Contractors, subcontractors, their employees, third-parties, and business associates with access to VA information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, shall adhere to 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.

(c) Access to VA information and VA information systems. (1) Contractors are limited in their request for logical or physical access to VA information or VA information systems for their employees, subcontractors, third parties and business associates to the extent necessary to perform the services or provide the goods as specified in the contracts, agreements, task, delivery or purchase orders.

(2) All Contractors, subcontractors, third parties, and business associates working with VA information are subject to the same investigative requirements as those of VA

appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors to access VA information and VA information systems shall be in accordance with VA Directive and Handbook 0710, Personnel Security and Suitability Program.

(3) Contractors, subcontractors, third parties, and business associates who require access to national security programs must have a valid security clearance.

(4) HIPAA Business Associate Agreement requirement. Contractors shall enter into a Business Associate Agreement with VHA, VA's Covered Entity, when contract requirements and access to protected health information is required and when requested by the Contracting Officer, or the Contracting Officer's Representative (COR) (see VAAR 824.103–70). Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, a Covered Entity (Veterans Health Administration) must have a satisfactory assurance that its protected health information will be safeguarded from misuse. To do so, a Covered Entity enters into a Business Associate Agreement (BAA) with a contractor (now the business associate), which obligates the business associate to only use the Covered Entity's protected health information for the purposes for which it was engaged, provide the same protections and safeguards as is required from the Covered Entity, and agree to the same disclosure restrictions to protected health information (PHI) that is required of the Covered Entity in situations where a contractor—

(i) Creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain health care operations activities or functions on

behalf of the Covered Entity; or

(ii) Provides one or more of the services specified in the Privacy Rule to or for the Covered Entity.

(A) Contractors or entities required to execute BAAs for contracts and other agreements become VHA business associates. BAAs are issued by VHA or may be issued by other VA programs in support of VHA. The HIPAA Privacy Rule requires VHA to execute compliant BAAs with persons or entities that create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of VHA. There may be other VA components or staff offices which also provide certain services and support to VHA and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these

services to VHA, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a BAA.

(B) BAA requirement flow down to subcontractors. A prime Contractor required to execute a BAA shall also obtain a satisfactory assurance, in the form of a BAA, that any of its subcontractors who will also create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA requirements to the same degree as the Contractor. Contractors employing a subcontractor who creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such VHA PHI under a contract or agreement is required to execute a BAA with each of its subcontractors which also obligates the subcontractor (i.e., also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to VHA's PHI that is required of the Covered Entity and the prime Contractor.

(d) Contractor operations required to be in United States. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practicable. If such services are proposed to be performed outside the continental United States, and are not otherwise disallowed by other Federal law, regulations or policy, or other VA policy or other mandates as stated in the contract, specifications, statement of work or performance work statement (including applicable Business Associate Agreements), the Contractor/subcontractor must state in its proposal where all non-U.S. services are provided. At a minimum, the Contractor/subcontractor must include a detailed Information Technology Security Plan, for review and approval by the Contracting Officer, specifically to address mitigation of the resulting problems of communication, control, and data protection. (e) Contractor/subcontractor employee reassignment and termination notification. Contractors and subcontractors shall provide written notification to the Contracting Officer and Contracting Officer's Representative (COR) immediately, and not later than four (4) hours, when an employee working on a VA information system or with access to VA information is reassigned or leaves the Contractor or subcontractor's employment on the cognizant VA contract. The Contracting Officer and COR must also be notified immediately by the Contractor or subcontractor prior to an unfriendly termination.

(f) VA information custodial requirements.

(1) Release, publication, and use of data. Information made available to a Contractor or subcontractor by VA for the performance or administration of a contract or information developed by the Contractor/subcontractor in performance or administration of a contract shall be used only for the stated contract purpose and shall not be used in any other way without VA's prior written approval. This clause expressly limits the

Contractor's/subcontractor's rights to use data as described in Rights in Data—General, FAR 52.227–14(d).

(2) Media sanitization. VA information shall not be co-mingled with any other data on the Contractors/subcontractor's information systems or media storage systems in order to ensure federal and VA requirements related to data protection, information segregation, classification requirements, and media sanitization can be met (see VA Directive 6500, VA Cybersecurity Program). VA reserves the right to conduct scheduled or unscheduled on-site inspections, assessments, or audits of Contractor and subcontractor IT resources, information systems and assets to ensure data security and privacy controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with Federal and VA requirements. The Contractor and subcontractor will provide all necessary access and support to VA and/or GAO staff during periodic control assessments or audits.

(3) Data retention, destruction and contractor self-certification. The Contactor and its subcontractors are responsible for collecting and destroying any VA data provided, created, or stored under the terms of this contract, to a point where VA data or materials are no longer readable or reconstructable to any degree, in accordance with VA Directive 6371, Destruction of Temporary Paper Records, or subsequent issue. Prior to termination or completion of this contract, the Contractor/subcontractor must provide its plan for destruction of all VA data in its possession according to VA Handbook 6500, and VA Cybersecurity Program, including compliance with National Institute of Standards and Technology (NIST) 800–88, Guidelines for Media Sanitization, for the purposes of media sanitization on all IT equipment. The Contractor must certify in writing to the Contracting Officer within 30 days of termination of the contract that the data destruction requirements in this paragraph have been met.

(4) Return of VA data and information. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to the VA (as stipulated by the Contracting Officer or the COR) or the Contractor/subcontractor must hold it until otherwise directed. Items returned will be hand carried, securely mailed, emailed, or securely electronically transmitted to the Contracting Officer or to the address as provided in the contract or by the assigned COR, and/or accompanying BAA. Depending on the method of return, Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract using VA-approved encryption tools that are, at a minimum, validated under FIPS 140–3 (or its successor). If mailed, Contractor/subcontractor must send via a trackable method (USPS, UPS, Federal Express, etc.) and immediately provide the Contracting Officer with the tracking information. No information, data, documentary material, records or

equipment will be destroyed unless done in accordance with the terms of this contract and the VHA Records Control Schedule 10–1.

(5) Use of VA data and information. The Contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if the National Institute of Standards and Technology (NIST) issues or updates applicable Federal Information Processing Standards (FIPS) or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies for this contract as a result of any updates, if required.

(6) Copying VA data or information. The Contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the contract or to preserve electronic information stored on Contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

(7) Violation of information custodial requirements. If VA determines that the Contractor has violated any of VA's information confidentiality, privacy, or security provisions, it shall be sufficient grounds for VA to withhold payment to the Contractor or third-party or terminate the contract for default in accordance with FAR part 49 or terminate for cause in accordance with FAR 12.403.

(8) Encryption. The Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract, using cryptography, and VA-approved encryption tools that are, at a minimum, validated under FIPS 140–3 (or its successor).

(9) Firewall and web services security controls. The Contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

(10) Disclosure of VA data and information. Except for uses and disclosures of VA information authorized in a cognizant contract for performance of the contract, the Contractor/subcontractor may use and disclose VA information only in two other situations:

(i) Subject to paragraph 10 of this section, in response to a court order from a court of competent jurisdiction, or

(ii) with VA's prior written approval. The Contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the Contracting Officer for response. If the Contractor/subcontractor is in receipt of a court order or other request or believes it has a legal requirement to disclose VA information, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response. If the Contractor or subcontractor discloses information on behalf of VHA, the Contractor and/or subcontractor must maintain an accounting of disclosures. Accounting of Disclosures documentation maintained by the Contractor/subcontractor will include the name of the individual to whom the information pertains, the date of each disclosure, the nature or description of the information disclosed, a brief statement of the purpose of each disclosure or, in lieu of such statement, a copy of a written request for a disclosure, and the name and address of the person or agency to whom the disclosure was made. The Contractor/subcontractor will provide its Accounting of Disclosures upon request and within 15 calendar days to the assigned COR and Privacy Officer. Accounting of disclosures should be provided electronically via encrypted email to the COR and designated VA facility Privacy Officer as provided in the contract, BAA, or by the Contracting Officer. If providing the Accounting of disclosures electronically cannot be done securely, the Contractor/subcontractor will provide copies via trackable methods (UPS, USPS, Federal Express, etc.) immediately, providing the designated COR and Privacy Officer with the tracking information.

(11) Compliance with privacy statutes and applicable regulations. The Contractor/subcontractor shall not disclose VA information protected by any of VA's privacy statutes or applicable regulations including but not limited to: The Privacy Act of 1974, 38 U.S.C. 5701, confidential nature of claims, 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus or the HIPAA Privacy Rule. If the Contractor/subcontractor is in receipt of a court order or other requests for VA information or has questions if it can disclose information protected under the abovementioned confidentiality statutes because it is required by law, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response.

(g) Report of known or suspected security/privacy incident. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify VA immediately via the Contracting Officer and the COR or within one (1) hour of an

incident which is an occurrence (including the discovery or disclosure of successful exploits of system vulnerability) that

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or the availability of its data and operations, or of its information or information system(s); or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. See VA Data Breach Response Service at https://www.oprm.va.gov/dbrs/about_dbrs.aspx. Report all actual or suspected security/privacy incidents and report the information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than __ days [Fill in: Contracting Officer fills in the number of days]. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (e.g., Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to VA that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within __ [Fill in: Contracting Officer fills in the number of days in consultation with requiring activity].

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, but within 60 days of discovery or disclosure. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of VA) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the VA Assistant Secretary for Office of Information and Technology. These exceptions will be tracked by the Contractor in concert with the Government in accordance with VA Directive 6500.6 and related VA Handbooks.

(h) Security and privacy incident investigation. (1) The term ‘‘privacy incident’’ means the unauthorized disclosure or use of VA information protected under a confidentiality statute or regulation. (2) The term ‘‘security incident’’ means an occurrence that

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies. The Contractor/subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected security or privacy incident, or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(2) To the extent known by the Contractor/subcontractor, the Contractor/subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(3) With respect to unsecured protected health information, the Business Associate is deemed to have discovered a security incident as defined above when the Business Associate either knew, or by exercising reasonable diligence should have been known to an employee of the Business Associate. Upon discovery, the Business Associate must notify VHA of the security incident immediately within one hour of discovery or suspicion as agreed to in the Business Associate Agreement (BAA).

(4) In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and the VA Office of Security and Law Enforcement. The Contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident. (i) Data breach notification requirements.

(A) This contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach involving any VA sensitive personal information the Contractor/Subcontractor processes or maintains under the contract as set forth in clause 852.211–76, Liquidated Damages—Reimbursement for Data Breach Costs.

(B) The Contractor/subcontractor shall provide notice to VA of a privacy or security incident as set forth in the Security and Privacy Incident Investigation section of this clause. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing

sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. The Contractor shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

(C) The Contractor/subcontractor shall fully cooperate with VA or any Government agency conducting an analysis regarding any notice of a data breach or potential data breach or security incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for VA, and shall address all relevant information concerning the data breach, including the following:

(1) Nature of the event (loss, theft, unauthorized access).

(2) Description of the event, including—

(i) Date of occurrence;

(ii) Date of incident detection;

(iii) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(iv) Number of individuals affected or potentially affected.

(v) Names of individuals or groups affected or potentially affected.

(vi) Ease of logical data access to the lost, stolen or improperly accessed data in light of

the degree of protection for the data, e.g., unencrypted, plain text.

(vii) Amount of time the data has been out of VA control.

(viii) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons).

(ix) Known misuses of data containing sensitive personal information, if any.

(x) Assessment of the potential harm to the affected individuals.

(xi) Data breach analysis as outlined in 6500.2 Handbook, Management of Breaches Involving Sensitive Personal Information, as appropriate.

(xii) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

(xiii) Steps taken in response to mitigate or prevent a repetition of the incident.

(j) Training. (1) All Contractor employees and subcontractor employees requiring access to VA information or VA information systems shall complete the following before being granted access to VA information and its systems:

(i) On an annual basis, successfully complete the VA Privacy and Information Security Awareness and VA Information Security Rules of Behavior training.

(ii) On an annual basis, sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security Rules of Behavior for Organizational Users, relating to access to VA information and information systems.

(iii) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access.

(2) The Contractor shall provide to the Contracting Officer and/or the COR a copy of the training certificates and affirmation that VA Information Security Rules of Behavior for Organizational Users signed by each applicable employee have been completed and submitted within five (5) days of the

initiation of the contract and annually thereafter, as required.

(3) Failure to complete the mandatory annual training and acknowledgement of the VA Information Security Rules of Behavior, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

(k) Subcontract flow down. The Contractor shall include the substance of this clause, including this paragraph (k), in subcontracts, third-party agreements, and business associate agreements, of any amount and in which subcontractor employees, third-party servicers/employees, and business associates will perform functions where they will have access to VA information (including VA sensitive information, i.e., sensitive personal information and protected health information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see VAAR 802.101 definition of information technology-related contracts.)

(End of clause)

804.1970 Information security policy—contractor general responsibilities.

Contractors, subcontractors, business associates and their employees who are users of VA information or information systems, or have access to VA information and VA sensitive information shall—

(a) Comply with all VA information security and privacy program policies, procedures, practices and related contract requirements, specifications and clauses, this includes complying with VA privacy and confidentiality laws and implementing VA and VHA regulations (see 38 U.S.C. 5701, 5705, 5721–5728 and 7332; 38 CFR 1.460 through 1.496, 1.500 through 1.527, and 17.500 through 17.511), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974 (as amended);

(b) Complete VA security awareness training on an annual basis;

(c) Complete VHA's Privacy and Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Training on an annual basis when access to protected health information (PHI) is required;

(d) Report all actual or suspected security/privacy incidents and report the information to the contracting officer and contracting officer's representative (COR), as identified in the contract or as directed in the contract, within one hour of discovery or suspicion;

(e) Comply with VA policy as it relates to personnel security and suitability program requirements for background screening of both employees and non-employees who have access to VA information systems and data;

(f) Comply with directions that may be issued by the contracting officer or COR, or from the VA Assistant Secretary for Information and Technology or a designated representative through the contracting officer or COR, directing specific activities when a security/privacy incident occurs;

(g) Sign 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, and clause 852.204–71, Information and Information Systems Security, on an annual basis. The VA Information Security Rules of Behavior describe the responsibilities and expected behavior of contractors, subcontractors, business associates and their employees who are users of VA information or information systems, information assets and resources, or have access to VA information;

(h) Maintain records and compliance reports regarding HIPAA Security and Privacy Rule compliance in order to provide such information to VA upon request to ascertain whether the business associate is complying with all applicable provisions under both rules' regulatory requirements; and

(i) Flow down requirements in all subcontracts and Business Associate Agreements (BAAs), at any level, as provided in the clause at 852.204–71, Information and Information Systems Security.