DEPAR **8320-01**

48 CFR Parts 802, 804, 811, 812, 824, 839, and 852

RIN 2900-AQ41

VA Acquisition Regulation: Acquisition of Information Technology; and Other Contracts for Goods and Services involving Information, VA Sensitive Information, and Information Security; and Liquidated Damages Requirements for Data Breach

AGENCY: Department of Veterans Affairs.

ACTION: Final rule.

SUMMARY: The Department of Veterans Affairs (VA) is issuing a final rule amending the VA Acquisition Regulation (VAAR). This rulemaking revises the VAAR by adding a part covering Acquisition of Information Technology and revising coverage concerning Other Contracts for Goods and Services involving mandatory information, privacy, and security requirements to include policy concerning VA sensitive personal information, information security, and liquidated damages requirements for data breach in the following parts: Administrative and Information Matters; Describing Agency Needs; Protection of Privacy and Freedom of Information; as well as Acquisition of Commercial Products and Commercial Services. It also revises affected parts concerning Definitions of Words and Terms, and Solicitation Provisions and Contract Clauses.

DATES: Effective **[Insert date 30 days after date of publication in the *FEDERAL REGISTER*]**.

FOR FURTHER INFORMATION CONTACT: Ms. Glacia A. Holbert, Senior Procurement Analyst, Procurement Policy and Warrant Management Services, 003A2A, 810 Vermont Avenue NW, Washington, DC 20420, (202) 697-3614. (This is not a toll-free number.)

SUPPLEMENTARY INFORMATION:

Background

VA published a proposed rule in the Federal Register at 86 FR 64132 on November 17, 2021, to amend the VAAR to implement and supplement the Federal Acquisition Regulation (FAR). VA provided a 60-day comment period for the public to respond to the proposed rule and submit comments. The public comment period closed on January 18, 2022. VA received ten comments from two respondents.

This rulemaking is issued under the authority of the Office of Federal Procurement Policy (OFPP) Act which provides the authority for an agency head to issue agency acquisition regulations that implement or supplement the FAR.

The VAAR has been revised to add new policy or regulatory requirements, to update existing policy, and to remove any redundant guidance where it may exist in affected parts, and to place guidance that is applicable only to VA's internal operating processes or procedures in the VA Acquisition Manual (VAAM).

This rule adopts as a final rule the proposed rule published in the Federal Register on November 17, 2021, except for revisions to respond to the public comments as discussed below, and other technical non-substantive changes to update terminology in accordance with FAR final rules and other minor administrative amendments as shown below.

Discussion and Analysis of Public Comments

The first respondent references two VA information technology and security publications and observed that as the field of technology grows, fraudulent activity rises and notes that the proposed rule provides a layer of uniform security. The respondent goes on to note that liquidated damages are instrumental.

VA appreciates the comment on the proposed rule. One of the VA Acquisition Regulation rewrite project objectives is to incorporate any new agency-specific regulations or policies to implement statutory and other requirements, to ensure VA can

effectively execute its mission to serve Veterans. VA believes the regulation appropriately implements specific liquidated damages statutory requirements in the event of a data breach. The comments do not require the VA to make any revisions to the proposed rule. Therefore, VA is taking no action to revise the proposed rule based on these comments.

Another respondent recommends revising the proposed notification and reporting of security and privacy incidents from “within 1 hour of discovery to the contracting officer” to “notification of within 24 hours of identification” as being a more reasonable timeline.

VA appreciates the comment and has considered the respondent’s suggestion. VA is required to ensure immediate notification in the event of discovery so that action can be initiated. VA has determined that waiting until 24 hours vs. the originally specified “within 1 hour of discovery” as set forth in the rule would potentially put Veteran’s data at further risk. The one-hour notification requirement is consistent with existing VA policy that all contractors must currently comply with. In order to ensure VA continues to protect Veteran’s data, the current reporting requirement is necessary. Therefore, VA is taking no action to revise the proposed rule based on these comments.

The same respondent requests that VA elaborate on the liquidated damages that are proposed for contracts that will be subject to the clause. The respondent asked, “How will such damages be assessed and enforced and is there potential for mitigation of any such damages?”

As stated in the preamble of the proposed rule, the VA Secretary is required by statute (38 U.S.C. 5725(a)-(c)) to ensure that if a contract is entered into for the performance of any Department function that requires access to sensitive personal information that VA shall include, as a condition of the contract, that a contractor shall not, directly or through an affiliate of the contractor, disclose such information to any

other person unless the disclosure is lawful and is expressly permitted under the contract. This statute also requires that each such contract be subject to liquidated damages to be paid by the contractor to VA in the event of a data breach of any sensitive personal information processed or maintained by the contractor or any subcontractor under the contract. The liquidated damages collected will be used for the purpose of VA providing credit protection services. The clause that sets forth the requirement is found in the proposed rule at section 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs. The clause states that if the contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach, the contractor shall, in place of actual damages, pay to the Government liquidated damages of [Contracting Officer inserts amount] per affected individual in order to cover costs related to the notification, data breach analysis and credit monitoring. The amount to be inserted by the contracting officer will be set forth in VA internal policy as the amount may change each year and would be inserted in the clause prior to contract award so contractors subject to the clause are aware. As stated in the clause, in the event the contractor provides payment of actual damages in an amount determined to be adequate by the contracting officer, the contracting officer may forgo collection of liquidated damages. Each situation will be handled by the contracting officer on a case-by-case basis under the terms and conditions of the clause as set forth in each contract.

The comments do not require VA to make any revisions to the proposed rule. Therefore, VA is taking no action to revise the rule based on these comments.

The respondent asks whether a contractor may defer to their own internal annual training programs already in place versus using VA furnished content.

VA has considered the respondent’s request to permit a contractor to use their own training in lieu of VA-specific training. However, to comply with Federal policy and

requirements, VA implementing directives and policy require VA organizational users (to include contractors, employees, subcontractors, and associates) and nonorganizational users to adhere to prescribed VA Privacy and Information Security Awareness and Rules of Behavior training. This training is the same training VA employees are required to take. Therefore, all contractors, contractor employees, subcontractors and associates are required to take the VA specific training and submit certificates when required by the contract where access to VA information, information systems, and VA sensitive information is required as set forth in the applicable clause(s) that are inserted in solicitations and contracts. The training is specific to VA requirements in order to protect VA information, VA sensitive information and VA information systems.
Therefore, VA is making no changes to the proposed rule as a result of this comment.

The respondent also requests VA provide more specific requirements for background screening.

Separately, specific requirements for background screening are set forth as applicable in each solicitation and contract. As this question is outside the scope of this proposed rule, VA is making no changes to the rule as a result of this comment.

The respondent asks if the definition of the initiation of a Business Associate Agreement (BAA) criteria differ from the HHS language?

To address the inquiry regarding the definition, VA refers the respondent to the definition of “Business Associate Agreement (BAA)” as set forth at VAAR 802.101. A Business Associate Agreement (BAA) means the agreement, as dictated by the Health Insurance Portability and Accountability Act of 1996 (HIAPA) Privacy Rule (45 CFR part 160), between the Veterans Health Administration (VHA) and a business associate, which must be entered into in addition to the underlying contract for services and before any release of protected health information (PHI) can be made to the business

associate, in order for the business associate to perform certain functions or activities on behalf of VHA. VA applies the criteria as set forth in the HIPAA Privacy Rule.

In VAAR section 824.103-70, Protection of privacy—general requirements and procedures related to Business Associate Agreements, VA policy states that to ensure compliance with unique responsibilities to protect PHI, contractors performing under VA contracts subject to unique PHI and HIPAA shall comply with requirements and the clause prescribed at section 804.1903, 852.204-71, Information and Information Systems Security.

The respondent also inquires whether VA will require BAAs to be executed in exclusive support of this contract and held separate from the support of other organizational business?

To address the inquiry regarding the definition, VA refers the respondent to the definition of “Business Associate Agreement (BAA)” as set forth at VAAR section 802.101. A BAA means the agreement, as dictated by the HIPAA Privacy Rule (45 CFR part 160), between VHA and a business associate, which must be entered into in addition to the underlying contract for services and before any release of protected health information (PHI) can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of VHA. VA applies the criteria as set forth in the HIPAA Privacy Rule.

In VAAR section 824.103-70, Protection of privacy—general requirements and procedures related to Business Associate Agreements, VA policy states that to ensure compliance with unique responsibilities to protect protected health information PHI, contractors performing under VA contracts subject to unique PHI and HIPAA shall comply with requirements and the clause prescribed at section 804.1903, 852.204-71, Information and Information Systems Security.

To address the respondent's second inquiry whether VA will require BAAs to be executed in exclusive support of a contract, as stated at VAAR section 824.103-70 of the rule, paragraph (a), which describes HIPAA Business Associate Agreement requirements, providing that, under the HIPAA Privacy and Security Rules (see 45 CFR part 160), a covered entity (VHA) must have a satisfactory assurance that its protected health information will be safeguarded from misuse. To do so, a covered entity enters into a BAA with a contractor (now the business associate), which obligates the business associate to only use the covered entity's PHI 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 PHI that is required of the covered entity. This specific VA requirement is in concert with the specified HIPAA Privacy Rule (see 45 CFR part 160).

The public is also invited to see VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, as referenced at paragraph (c). Contractors will be required to execute BAAs as required by the contract. Contractors should contact the cognizant contracting officer and contracting officer's representative, as required, for questions regarding BAAs which may have previously been executed and filed with the VHA (the only administration of the Department of Veterans Affairs that is a HIPAA covered entity under the HIPAA Privacy Rule).

The comments do not require the VA to make any revisions to the proposed rule. Therefore, VA is taking no action to revise the rule based on these comments.

The respondent requests that VA elaborate on the details of what would be expected to be included in the Information Technology Security Plan.

VA has considered the respondent's comment and is slightly editing the clause at 852.239-70, Security Requirements for Information Technology Resources, to ensure the requirement for a plan is understood by revising the title of the plan and its use,

including in the clause at 852.239-73, Information System Hosting, Operation, Maintenance, or Use, both prescribed in VAAR part 839. The title of the required plan referenced in the clause at 852.239-70, Security Requirements for Information Technology Resources, is revised from “Information Technology Security Plan” to “Information System Security Plan” to better reflect the underlying content submittal requirements. In the clause at 852.239-70, paragraph (c) states that, generally, the 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. It should include implementation status, responsible entities, resources, and estimated completion dates. An “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. Information system 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, Privacy Impact 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 system security and related support or services included in the contract, to include the performance work statement (PWS) or statement of work (SOW). The plan shall also 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 plan requirements (describing the security controls in place or planned for meeting those requirements) in accordance with Federal and VA policies and procedures, and as amended during the term of a contract, and include, but are not limited to the following:

(1) Office of Management and Budget (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) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems.

VA has updated the VAAR text prescribing the clause, and the clause at 852.239-70, Security Requirements for Information Technology Resources.

The respondent asks VA with respect to the clause at 852.239-73, Information System Hosting, Operation, Maintenance, or Use, to provide more details on the VA systems control procedures as well as what might be expected to be included in the PIA.

VA has considered the respondent's request to further elaborate on the requirement for a PIA. In order to provide clarity to the public, VA is incorporating non-substantive technical amendments to the clauses at 852.239-70, Security Requirements for Information Technology Resources, and 852.239-73, Information System Hosting, Operation, Maintenance, or Use, to clarify that when VA is referring to a "security plan" the requirement is for an "information system security plan." VA has made the

corresponding revisions to the clauses and applicable VAAR text where that term is included to clarify this. VA is also clarifying for the public via the clause at 852.239-70, paragraph (e), Security accreditation, that VA is referring to non-VA owned systems.

In the clause at 852.239-73, Information System Hosting, Operation, Maintenance, or Use, VA is also clarifying in paragraph (c), Collecting, processing, transmitting, and storing of VA sensitive information, that VA is referring to a broader category of VA sensitive information of which Personally Identifiable Information (PII) is a subset and has revised the clause at 852.239-73, Information System Hosting, Operation, Maintenance, or Use, to reflect “VA sensitive information” in lieu of “PII” in the paragraph to ensure clarity.

And, in paragraph (g), Disposal or return of electronic storage media on non-VA leased or non-VA owned IT equipment, VA has added a key specific reference to the National Institute of Standards (NIST) 800-88, Rev. 1, “Guidelines for Media Sanitization,” and VA Directive 6500, VA Cybersecurity Program, paragraph 2(b)(5), Media Sanitization, to provide the public more information on what electronic media sanitization requirements apply.

These technical revisions of the rule align the two clauses and ensures the public is aware that PII is considered a subset for VA sensitive information and the requirements for protecting and safeguarding the same are clearly identified and understood.

The respondent asks a final question with respect to the proposed clause at 852.239-74, Security Controls Compliance Testing, and specifically if VA can provide more details on the items to be included in a security control assessment. The respondent noted that they have concerns that it may be difficult to complete the assessment depending on the timing of any advance notification.

VA refers the public to more information on security control assessments that can be found in NIST SP 800-53A Rev. 5. The comments do not require the VA to make any revisions to the rule on the basis of the specific comment. However, VA is making one minor revision to the clause in the first sentence to provide clarity. The sentence is being revised from…. "VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor..." to "VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security and privacy controls implemented by the Contractor...".

Summary of Revisions to the Rule

Based on the review of public comments and to provide clarity as discussed above under the analysis of public comments, VA is summarizing the technical revisions to address the comments as follows:

1. At section 839.106-70, the heading of the section is changed to "Information system security and privacy contract clauses," in lieu of "Information technology security and privacy clauses." And in paragraph (a), the heading for the clause at 852.239-71 is revised from "Information Technology Security Plan and Accreditation" to "Information System Security Plan and Accreditation."
2. In the clause at 852.239-70, Security Requirements for Information Technology Resources, the following clarifying edits were made:
    a. In paragraph (a), the definition for "Security plan" is revised slightly to now read "Information system security plan" and an unnecessary reference to "or an information security program and" is removed for clarity.
    b. In paragraph (b), in the first sentence the phrase "information technology security" is revised to read "information system security…".

c. In paragraph (c), the heading of the paragraph is revised to read “Information system security plan” in lieu of “Information technology security plan.” Other conforming edits are made to revise the use from “security plan” to read “information system security plan”, and to remove the term “technology” where not appropriate. The paragraph is also updated in the fifth sentence to remove the phrase “or qualities required for system registration” as unnecessary.

d. In paragraph (d), the required number of calendar days for submittal of an Information System Security Plan is increased from “30 days after contract award” to read “90 days after contract award.” This provides more time for contractors to accomplish the required submittal.

e. In paragraph (e), dealing with security accreditation, the phrase “information technology security accreditation” is revised to read “information system security accreditation” in the first sentence. It is also clarified by adding the phrase “for non-VA owned systems” to make this clear. And the second to last and the last sentence are edited to improve the flow of information.

f. In paragraph (f), the referenced “IT Security Plan” is revised to reflect the updated usage of “Information System Security Plan” as contained within the rest of the clause.

g. In paragraph (j), dealing with Government access, the phrase “information technology inspection” is revised to reflect “information system inspection” to reflect the more accurate terminology. And the word “technology” is removed in the last sentence after the word “information” so that it now reads “…information systems operated on behalf of VA),…”.

3. In the clause at 852.239-73, Information System Hosting, Operation, Maintenance, or Use, the following editorial revisions are made for clarity and to

incorporate the appropriate use of the term “information system security plan” in lieu of “security plan.”

a. In paragraph (a), the definition for “Security plan” is revised slightly to now read “Information system security plan” and an unnecessary reference to “or an information security program and” is removed for clarity.

b. In paragraph (c), dealing with collecting, processing, transmitting, and storing of PII, the heading is revised to reflect “VA sensitive information” in lieu of PII as the more appropriate term to use that would encompass PII. The heading for this paragraph would now read “Collecting, processing, transmitting, and storing of VA sensitive information.” An unnecessary phrase “as determined by the VA Privacy Service” is removed. The phrase “Privacy Impact Assessment” is deleted, and the phrase “Information System Security Plan” is inserted in its place as the more accurate term. And the requirement that a Plan of Action and Milestones (POA&M) must be submitted and approved is expanded from just prior to “collection of PII” to prior to “collecting, processing, transmitting, and storing of VA sensitive information” to comply with requirements already described elsewhere in the rule.

c. In paragraph (g), concerning disposal or return of electronic storage media on non-VA leased or non-VA owned IT equipment, VA is adding the required specific references to the existing language as follows: “NIST 800-88, Rev. 1, “Guidelines for Media Sanitization,” and VA Directive 6500, VA Cybersecurity Program, paragraph 2(b)(5), Media Sanitization…”.

4. In the clause at 852.239-74, Security Controls Compliance Testing, VA is making a minor edit to revise the phrase “all of the security controls and privacy practices” to “all of the security and privacy controls” in the first sentence.

Technical Non-Substantive Changes to the Rule

This rule makes 12 non-substantive changes to the rule to provide clarity, eliminate confusion, and to ensure compliance with the FAR. Specifically, VA is revising the term “commercial items” to reflect either “commercial products and commercial services” or “commercial products or commercial services” in alignment with FAR final rule, Federal Acquisition Regulation: Revision of Definition of “Commercial Item”, RIN 9000-AN76, effective December 6, 2021. There are 14 mentions of the legacy term “commercial items” that were identified in this rule’s amendatory language in the following VAAR parts, subparts, and sections, to include headings as well as the underlying text. The legacy term “commercial items” was also referenced in two FAR clause references where the FAR heading has also been revised because of the referenced FAR final rule. The respective VAAR part 812 table of contents also has the legacy term “Commercial Item” and will also be updated with this final rule.

Accordingly, VA is revising the final rule to reflect the updated terminology in accordance with the FAR final rule and as reflected in the amendatory text as follows (items number 1 – 9 below):

1. At section 804.1902, Applicability, VA is revising the phrase in the section from “acquisition of commercial items” to “acquisition of commercial products or commercial services.”
2. At section 811.503-70, Contract clause, paragraph (b), VA is revising the phrase “in commercial items” to read “for commercial products or commercial services…”.
3. At section 811.503-70, Contract clause, paragraph (c), VA is revising the phrase “commercial items” to read “commercial products or commercial services…”.

4. Under part 812, Acquisition of Commercial Items, VA is revising the heading from “Acquisition of Commercial Items” to “Acquisition of Commercial Products and Commercial Services”.
5. At subpart 812.3, VA is revising the heading from “Solicitation Provisions and Contract Clauses for the Acquisition of Commercial Items” to read “Solicitation Provisions and Contract Clauses for the Acquisition of Commercial Products and Commercial Services.”
6. At section 812.301, VA is revising the heading from “Solicitation provisions and contract clauses for the acquisition of commercial items” to read “Solicitation provisions and contract clauses for the acquisition of commercial products and commercial services.”
7. Under section 812.301, at paragraphs (f)(1) and (2), VA is revising the heading to the FAR provision at 52.212-1 to read “Instruction to Offerors - Commercial Products and Commercial Services,” and the heading to the FAR provision at 52.212-2 to read “Evaluation – Commercial Products and Commercial Services.”
8. At section 852.211-76, Liquidated Damages – Reimbursement for Data Breach Costs, the following revisions are made:

   a. In the Alternate I paragraph, the phrase, “commercial items” is revised to read “commercial products or commercial services,” and in paragraph (e) under Alternate I, the referenced heading for the FAR clause at 52.212-4 is revised to read “Contract Terms and Conditions – Commercial Products and Commercial Services.”

   b. In the Alternate II paragraph, the phrase, “commercial items” is revised to read “commercial products or commercial services,” and in paragraph (e) under Alternate II, the referenced heading for the FAR clause at 52.212-4 is

revised to read “Contract Terms and Conditions – Simplified Acquisitions (Other Than Commercial Products and Commercial Services).”

Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, and other advantages; distributive impacts; and equity). E.O. 13563 (Improving Regulation and Regulatory Review) emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility. The Office of Information and Regulatory Affairs has determined that this rule is a significant regulatory action under Executive Order 12866.

The Regulatory Impact Analysis associated with this rulemaking can be found as a supporting document at www.regulations.gov.

Paperwork Reduction Act

This final rule includes provisions constituting a new collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3521) that require approval by OMB. Accordingly, under 44 U.S.C. 3507(d), VA has submitted a copy of this rulemaking action to OMB for review and approval, including all comments received on the proposed information collections and any changes made in response to comments. OMB has reviewed and assigned four new OMB Control Numbers, which are detailed below. In accordance with 5 CFR part 1320, the new OMB control numbers and the information collections are not approved at this time. OMB has up to 30 days to approve these information collections after the final rule publishes.

- OMB Control Number 2900-0895 for section 839.106-70, Information security and privacy clauses, and the VAAR clauses at 852.239-70, Security Requirements for Information Technology Resources, 852.239-72, Information System Design and Development, and 852.239-73, Information System Hosting, Operation, Maintenance or Use.
- OMB Control Number 2900-0900 for section 804.1970, Information security policy—contractor general responsibilities, and the VAAR clause at 852.204-71, Information and Information System Security.
- OMB Control Number 2900-0901 for section 811.503-70, Contract clause, and the VAAR clause at 852.211-76, Liquidated Damages-Reimbursement for Data Breach Costs.
- OMB Control Number 2900-0902 for section 812.301(f), Solicitation provisions and contract clauses for the acquisition of commercial products or commercial services, and the VAAR clauses at 852.212-71, Gray Market and Counterfeit Items, and 852.212-72, Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts.

If OMB does not approve the collections of information as requested, VA will immediately remove the provisions containing a collection of information or take such other action as is directed by OMB.

Regulatory Flexibility Act

The Secretary hereby certifies that this final rule will not have a significant economic impact on a substantial number of small entities as they are defined in the Regulatory Flexibility Act (5 U.S.C. 601–612). The factual basis for this certification is based on the information set forth in this section. Therefore, pursuant to 5 U.S.C.

605(b), the initial and final regulatory flexibility analysis requirements of 5 U.S.C. 603 and 604 do not apply.

This rulemaking does not change VA's policy regarding small businesses and does not have a significant economic impact to individual businesses. The overall impact of the proposed rule would be of benefit to small businesses owned by Veterans or service-disabled Veterans as the VAAR is being updated to provide needed guidance to ensure VA's contractors properly protect and safeguard VA sensitive information, which includes Veteran's sensitive personal information. This rulemaking adds a new VAAR part concerning Acquisition of Information Technology that codifies information collection burdens. VA's requirement to collect the information is the result of existing requirements to ensure compliance across the Federal government and specifically when VA contractors, subcontractors, business associates and their employees require access to VA information (including VA sensitive information) or information systems. VA is merely adding existing and current regulatory requirements to the VAAR and placing guidance that is applicable only to VA's internal operation processes or procedures into a VA Acquisition Manual. VA estimates no substantial cost impact to individual businesses will result from these rule updates already required to be considered by both large and small businesses to receive an award from VA or another Federal agency. There are costs associated with this rulemaking pertaining to the codification of an information collection request in order to comply with VA's responsibilities under the Federal Information Security Modernization Act of 2014. Each agency of the Federal Government must provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. By statute, VA is required to ensure that its contractors, subcontractors, business associates, and their employees operating under contracts at VA shall be subject to the same Federal

laws, regulations, policies or procedures as VA and VA personnel. While this requirement adds some burden in annual costs and hours to firms already awarded and performing contracts at VA, the overall cost is considered *de minimis*, for either large or small contractors, in relation to the potential impact and harm to Veterans and VA information and information systems should a contractor not comply. Properly setting forth the requirements will provide clarity to the public and ensure appropriate safeguards are in place to ensure protection of VA's information (in particular VA sensitive personal information) and information systems. In total, this rulemaking does not change VA's policy regarding small businesses, does not have a substantial economic impact to individual businesses, and does not significantly increase or decrease costs small business were already required to bear when performing contracts which required the access, maintenance, process, or utilization of VA sensitive information or information systems.

Unfunded Mandates

The Unfunded Mandates Reform Act of 1995 requires, at 2 U.S.C. 1532, that agencies prepare an assessment of anticipated costs and benefits before issuing any rule that may result in the expenditure by State, local, and tribal Governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any one year. This rule would have no such effect on State, local, and tribal Governments or on the private sector.

Congressional Review Act

Pursuant to the Congressional Review Act (5 U.S.C. 801 et seq.), the Office of Information and Regulatory Affairs designated this rule as not a major rule, as defined by 5 U.S.C. 804(2).

List of Subjects

48 CFR Parts 802, 804, 811, and 812

Government procurement.

48 CFR Part 824

Freedom of information, Government procurement, Privacy.

48 CFR Part 839

Computer technology, Government procurement.

48 CFR Part 852

Government procurement, Reporting and recordkeeping requirements.

Signing Authority:

Denis McDonough, Secretary of Veterans Affairs, approved this document on December 19, 2022, and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs.

Consuela Benjamin,

Regulation Development Coordinator

Office of Regulation Policy & Management,

Office of General Counsel,

Department of Veterans Affairs.

For the reasons set forth in the preamble, VA amends 48 CFR chapter 8 as follows:

PART 802—DEFINITIONS OF WORDS AND TERMS

1. The authority citation for part 802 continues to read as follows:

Authority: 40 U.S.C. 121(c); 41 U.S.C. 1121(c)(3); 41 U.S.C. 1702; and 48 CFR 1.301 through 1.304.

Subpart 802.1—Definitions

2. Section 802.101 is amended by adding definitions for “Business associate”, “Business Associate Agreement”, “Gray market items”, “Information system”, “Information technology”, “Information technology-related contracts”, “Privacy officer”, “Security plan”, “Sensitive personal information”, “VA Information Security Rules of Behavior for Organizational Users / VA National Rules of Behavior”, and “VA sensitive information” in alphabetical order to read as follows:

802.101 Definitions.

* * * * *

Business associate (or *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) (Pub. L. 104-191) Privacy Rule (45 CFR part 160), 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), or that provides to or for VHA, certain services as specified in the HIPAA Privacy Rule that involve the disclosure of PHI to a contractor by VHA. The term also includes a subcontractor of a business associate that creates, receives, maintains, or transmits PHI or that stores, generates, accesses, exchanges, processes, or utilizes such PHI on behalf of the business

associate.

Business Associate Agreement (BAA) means the agreement, as dictated by the HIPAA Privacy Rule (45 CFR part 160), 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.

* * * * *

Gray market items means original equipment manufacturer goods intentionally or unintentionally sold outside an authorized sales territory or sold by non-authorized dealers in an authorized sales territory.

* * * * *

Information system means, pursuant to 38 U.S.C. 5727, 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 this section.

* * * * *

Privacy officer means the VA official with responsibility for implementing and oversight of privacy related policies and practices that impact a given VA acquisition.

* * * * *

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.

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.

* * * * *

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.

* * * * *

PART 804—ADMINISTRATIVE AND INFORMATION MATTERS

3.The authority citation for part 804 is revised to read as follows:

Authority: 38 U.S.C. 5723-5724, 5725(a)–(c); 40 U.S.C. 121(c); 41 U.S.C. 1702; and 48 CFR 1.301 through 1.304.

4. Subpart 804.19 is added to read as follows:

Subpart 804.19—Basic Safeguarding of Covered Contractor Information Systems

Sec.

Subpart 804.19—Basic Safeguarding of Covered Contractor Information Systems

804.1900-70 Scope of this subpart.

This subpart prescribes policies and procedures for information security and protection of VA information, information systems, and VA sensitive information, including sensitive personal information.

804.1902 Applicability.

This subpart applies to all VA acquisitions, including acquisitions of commercial products or commercial services other than commercially available off-the-shelf items, when a contractor's information system may contain VA information.

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 Veterans Health Administration (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) (Pub. L. 104-191), and the Privacy Act of 1974 (as amended) (5 U.S.C. 522a);

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

(c) Complete VHA's Privacy and 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, and the clause at 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 Rules (see 45 CFR part 160) 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.

804.1903 Contract clause.

When the clause at FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems is required to be included in accordance with FAR 4.1903, the contracting officer shall insert the clause at 852.204-71, Information and Information Systems Security.

PART 811—DESCRIBING AGENCY NEEDS

5. The authority citation for part 811 is revised to read as follows:

Authority: 38 U.S.C. 5723-5724, 5725(a)–(c); 40 U.S.C. 121(c); 41 U.S.C. 1303, 1702; and 48 CFR 1.301 through 1.304.

6. Subpart 811.5 is added to read as follows:

Subpart 811.5—Liquidated Damages

Sec.

Subpart 811.5—Liquidated Damages

811.500 Scope.

This subpart prescribes policies and procedures for using a liquidated damages clause in solicitations and contracts that involve VA sensitive personal information. This also pertains to any solicitations and contracts involving VA sensitive personal information issued by another agency for or on behalf of VA through an interagency acquisition in accordance with FAR subpart 17.5 and subpart 817.5.

811.501-70 Policy—statutory requirement.

(a) Contracting officers are required to include a liquidated damages clause in contracts for the performance of any Department function which requires access to VA sensitive personal information (*see* the definition in 802.101), in accordance with 38 U.S.C. 5725(b). The liquidated damages are to be paid by the contractor to the Department of Veterans Affairs in the event of a data breach involving sensitive personal information maintained, processed, or utilized by contractors or any subcontractors.

(b) The purpose of the liquidated damages to be paid for by the contractor in the event of a data breach of personal sensitive information is for VA to provide credit protection services to affected individuals pursuant to 38 U.S.C. 5724(a)-(b).

811.503-70 Contract clause.

(a) Insert the clause at 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs, in all solicitations, contracts, or orders, where VA requires access to sensitive personal information for the performance of a Department function where—

(1) Sensitive personal information (*see* the definition in 802.101) will be created, received, maintained, or transmitted, or that will be stored, generated, accessed, or exchanged such as protected health information (PHI) or utilized by a contractor,

subcontractor, business associate, or an employee of one of these entities; or,

(2) When VA information systems will be designed or developed at non-VA facilities where such sensitive personal information is required to be created, received, maintained, or transmitted, or that will be stored, generated, accessed, exchanged, processed, or utilized.

(b) Insert the clause at 852.211-76 with its Alternate I in all solicitations, contracts, or orders, for commercial products or commercial services acquisitions awarded under the procedures of FAR part 8 or 12.

(c) Insert the clause at 852.211-76 with its Alternate II, in all solicitations, contracts, or orders, in simplified acquisitions exceeding the micro-purchase threshold that are for other than commercial products or commercial services awarded under the procedures of FAR part 13 (*see* FAR 13.302-5(d)(1) and the clause at FAR 52.213-4).

PART 812—ACQUISITION OF COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

7. The authority citation for part 812 continues to read as follows:

Authority: 38 U.S.C. 8127-8128; 40 U.S.C. 121(c); 41 U.S.C. 1702 and 48 CFR 1.301 through 1.304.

8. The heading for part 812 is revised to read as set forth above.

9. Subpart 812.3 is revised to read as follows:

Subpart 812.3—Solicitation Provisions and Contract Clauses for the Acquisition of Commercial Products and Commercial Services

812.301 Solicitation provisions and contract clauses for the acquisition of commercial products and commercial services.

(f)(1) Contracting officers shall insert the clause at 852.212-71, Gray Market and Counterfeit Items, in solicitations and contracts for new medical supplies, new medical

equipment, new information technology equipment, and maintenance of medical or information technology equipment that includes replacement parts if used, refurbished, or remanufactured parts are unacceptable, when the associated solicitation includes FAR 52.212-1, Instruction to Offerors - Commercial Products and Commercial Services, and 52.212-2, Evaluation – Commercial Products and Commercial Services.

(2) Contracting officers shall insert the clause at 852.212-72, Gray Market and Counterfeit Items - Information Technology Maintenance Allowing Other-than-New Parts, in solicitations and contracts for the maintenance of information technology equipment that includes replacement parts, if used, refurbished, or remanufactured parts are acceptable, when the associated solicitation includes FAR 52.212-1, Instruction to Offerors - Commercial Products and Commercial Services, and 52.212-2, Evaluation – Commercial Products and Commercial Services.

PART 824—PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION

10. The authority citation for part 824 is revised to read as follows:

Authority: 5 U.S.C. 552a; 38 U.S.C. 5723-5724, 5725(a)–(c); 40 U.S.C. 121(c); 41 U.S.C. 1121(c), 1702; 38 CFR 1.550 through 1.562 and 1.575 through 1.584; and 48 CFR 1.301 through 1.304.

Subpart 824.1— Protection of Individual Privacy

11. Sections 824.103-70 and 824.103-71 are added to read as follows:

824.103-70 Protection of privacy—general requirements and procedures related to Business Associate Agreements.

To ensure compliance with unique responsibilities to protect protected health information (PHI), contractors performing under VA contracts subject to unique PHI and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall comply with requirements and the clause (852.204-71, Information and Information Systems Security) prescribed at 804.1903.

(a) *HIPAA Business Associate Agreement requirement*. Under the HIPAA

Privacy and Security Rules (see 45 CFR part 160), a covered entity (Veterans Health Administration (VHA)) must have a satisfactory assurance that its PHI 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 PHI 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 PHI that is required of the covered entity in situations where a contractor —

(1) 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

(2) Provides one or more of the services specified in the HIPAA Privacy Rule to or for the covered entity.

(b) *Veterans Health Administration (VHA)—a HIPAA covered entity*. VHA is the only administration of the Department of Veterans Affairs that is a HIPAA covered entity under the HIPAA Privacy Rule.

(c) *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.

(1) 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.

(2) Contractors or other entities supporting VHA required to create, receive, maintain, or transmit VHA PHI shall be required to execute a BAA as mandated by the HIPAA Privacy Rule and requested by the contracting officer, the contracting officer's representative (COR) or the cognizant privacy officer—

(i) Whether via a contract or agreement with VHA; or

(ii) Whether provided from or through another VA administration or staff activity contract for supplies, services or support that involves performing a certain activity, function or service to, for, or on behalf of VHA (*see* VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management).

(d) *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. A contractor 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.

824.103-71 Liquidated damages—protection of information.

(a) *Purpose*. As required by 38 U.S.C. 5725 any contracts where sensitive personal information such as PHI must be disclosed to the contractor for the contractor

to perform certain functions or services on behalf of VHA shall include a liquidated damages clause as prescribed at 811.503-70.

(b) *Applicability to contracts requiring Business Associate Agreements*. A liquidated damages clause is required (*see* 811.503-70) when performance under a contract requires a contractor to enter into a Business Associate Agreement with VHA because the contractor or its subcontractor is required to create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI, for certain services or functions, on behalf of VHA. The liquidated damages clause shall be added even in situations where the prime contractor never directly receives VA's sensitive personal information and the same flows directly to the prime contractor's subcontractor.

12. Part 839 is added to read as follows:

PART 839—ACQUISITION OF INFORMATION TECHNOLOGY

Authority**:** 38 U.S.C. 5723-5724, 5725(a)–(c); 40 U.S.C. 121(c), 11319(b)(1)(C); 41 U.S.C. 1121(c)(3), 1303 and 1702; and 48 CFR 1.301 through 1.304.

839.000 Scope of part.

This part prescribes acquisition policies and procedures for use in acquiring VA

information technology and information technology-related contracts (*see* 802.101) and applies to both VA-procured information technology systems as well as interagency acquisitions defined in FAR part 17 and part 817.

Subpart 839.1—General

839.101 Policy.

(a)(1) In acquiring information technology, including information technology-related contracts which may involve services (including support services), and related resources (*see* the definition at FAR 2.101), contracting officers and requiring activities shall include in solicitations and contracts the requirement to comply with the following directives, policies, and procedures in order to protect VA information, information systems, and information technology—

(i) VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series, to include, but not limited to, VA Handbook 6500.6, Contract Security, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive orders, policies, regulations, standards, and guidance for protecting and controlling VA sensitive information and ensuring that security requirements are included in acquisitions, solicitations, contracts, purchase orders, and task or delivery orders.

(ii) The VA directives, security requirements, procedures, and guidance in paragraph (a)(1)(i) of this section apply to all VA contracts and to contractors, subcontractors, and their employees in the performance of contractual obligations to VA for information technology products purchased from vendors, as well as for services acquired from contractors and subcontractors or business associates, through contracts and service agreements, in which access to VA information, VA sensitive information or sensitive personal information (including protected health information (PHI))—

(A) That is created, received, maintained, or transmitted, or that will be stored,

generated, accessed, exchanged, processed, or utilized by VA, a VA contractor, subcontractor, or third-party servicers or associates, or on behalf of any of these entities, in the performance of their contractual obligations to VA; and

(B) By or on behalf of any of the entities identified in this section, regardless of—

(*1*) Format; or

(*2*) Whether it resides on a VA or a non-VA system, or with a contractor, subcontractor, or third-party system or electronic information system(s), including cloud services, operating for or on the VA's behalf or as required by contract.

(c) Contractors, subcontractors, and third-party servicers or associates providing support to or on behalf of the entities identified in this section, shall employ adequate security controls and use appropriate common security configurations available from the National Institute of Standards and Technology (*see* FAR 39.101(c)) as appropriate in accordance with VA regulations in this chapter, directives, handbooks, and guidance, and established service level agreements and individual contracts, orders, and agreements. Contractors, subcontractors, and third-party servicers and associates will ensure that VA information or VA sensitive information that resides on a VA system or resides on a contractor/subcontractor/third-party entities/associates information and communication technology (ICT) system(s), operating for or on VA's behalf, or as required by contract, regardless of form or format, whether electronic or manual, and information systems, are protected from unauthorized access, use, disclosure, modification, or destruction to ensure information security (*see* FAR 2.101) is provided in order to ensure the integrity, confidentiality, and availability of such information and information systems.

839.105 Privacy.

839.105-70 Business Associate Agreements, information technology-related contracts and privacy.

In accordance with 824.103-70, contracting officers and contracting officer representatives (CORs) shall ensure that contractors, their employees, subcontractors, and third-parties under the contract complete Business Associate Agreements for—

(a) Information technology or information technology-related service contracts subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) where HIPAA PHI is created, received, maintained, or transmitted, or that will be stored, generated, accessed, exchanged, processed, or utilized in order to perform certain health care operations activities or functions on behalf of the Veterans Health Administration (VHA) as a covered entity (*see* 802.101 for the definition of information technology-related contracts); or

(b) Contractors supporting other VA organizations which support VHA in this regard and which would therefore require Business Associate Agreements in accordance with 824.103-70.

839.105-71 Liquidated damages—protection of information in information technology related contracts.

Contracting officers shall insert in information technology related contracts the liquidated damages clause as prescribed at 811.503-70.

839.106-70 Information security and privacy contract clauses.

(a) Contracting officers shall insert the clause at 852.239-70, Security Requirements for Information Technology Resources, and the clause at 852.239-71, Information System Security Plan and Accreditation, in all solicitations, contracts, and orders exceeding the micro-purchase threshold that include information technology services.

(b) Contracting officers shall insert the clause at 852.239-72, Information System Design and Development, in solicitations, contracts, orders, and agreements where services to perform information system design and development are required.

(c) Contracting officers shall insert the clause at 852.239-73, Information System Hosting, Operation, Maintenance or Use, in solicitations, contracts, orders, and agreements where services to perform information system hosting, operation, maintenance, or use are required.

(d) Contracting officers shall insert the clause at 852.239-74, Security Controls Compliance Testing, in solicitations, contracts, orders, and agreements, when the clause at 852.239-72 or 852.239-73 is inserted.

Subpart 839.2—Information and Communication Technology

839.201 Scope of subpart.

This subpart applies to the acquisition of Information and Communication Technology (ICT) supplies and services. It concerns the access to and use of information and data by both Federal employees with disabilities and members of the public with disabilities in accordance with FAR 39.201. This subpart implements VA policy on section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) and 36 CFR parts 1193 and 1194 as it applies to contracts and acquisitions when developing, procuring, maintaining, or using ICT.

839.203 Applicability.

(a) *General*. Solicitations for information technology (IT) (*i.e.*, ICT) or IT-related supplies and services shall require the contractor to submit a VA Section 508 Checklist (*see* https://www.section508.va.gov/).

839.203-70 Information and communication technology accessibility standards—contract clause and provision.

(a) The contracting officer shall insert the provision at 852.239-75, Information and Communication Technology Accessibility Notice, in all solicitations.

(b) The contracting officer shall insert the clause at 852.239-76, Information and Communication Technology Accessibility, in all contracts and orders.

PART 852—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

13. The authority citation for part 852 continues to read as follows:

Authority: 38 U.S.C. 8127-8128 and 8151-8153; 40 U.S.C. 121(c); 41 U.S.C. 1121(c)(3); 41 U.S.C. 1303; 41 U.S.C. 1702; and 48 CFR 1.301 through 1.304.

Subpart 852.2—Texts of Provisions and Clauses

14. Section 852.204-71 is added to read as follows:

852.204-71 Information and Information Systems Security.

As prescribed in 804.1903, insert the following clause:

INFORMATION AND INFORMATION SYSTEMS SECURITY (FEB 2023)

(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 (BAA) 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 HIPAA Privacy and Security Rules, a Covered Entity (VHA) must have a satisfactory assurance that its PHIwill be safeguarded from misuse. To do so, a Covered Entity enters into a BAA with a contractor (now the business associate), which obligates the business associate to only use the Covered Entity's PHI 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 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 Federal Information Processing Standards (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 NIST issues or updates applicable 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 (f)(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 above-mentioned 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.

(3) 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.

(4) With respect to unsecured PHI, 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 BAA.

(5) 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*. (1) 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.

(2) 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.

(3) 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:

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

(ii) Description of the event, including—

(A) Date of occurrence;

(B) Date of incident detection;

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

(D) Number of individuals affected or potentially affected.

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

(F) 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.

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

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

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

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

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

(L) 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.

(M) 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 BAAs, 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)

15. Section 852.211-76 is added to read as follows:

852.211-76 Liquidated Damages—Reimbursement for Data Breach Costs.

As prescribed in 811.503-70, insert the following clause:

LIQUIDATED DAMAGES—REIMBURSEMENT FOR DATA BREACH COSTS (FEB 2023)

(a) *Definition*. As used in this clause, “contract” means any contract, agreement, order or other instrument and encompasses the definition set forth in FAR 2.101.

(b) *Non-disclosure requirements*. As a condition of performance under a contract, order, agreement, or other instrument that requires access to sensitive personal information as defined in VAAR 802.101, the following is expressly required—

(1) The Contractor, subcontractor, their employees or business associates shall not, directly or through an affiliate or employee of the Contractor, subcontractor, or business associate, disclose sensitive personal information to any other person unless the disclosure is lawful and is expressly permitted under the contract; and

(2) The Contractor, subcontractor, their employees or business associates shall immediately notify the Contracting Officer and the Contracting Officer’s Representative (COR) of any security incident that occurs involving sensitive personal information.

(c) *Liquidated damages*. If the Contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach, the Contractor shall, in place of actual damages, pay to the Government liquidated damages of _____ [*Contracting Officer insert amount*] per affected individual in order to cover costs related to the notification, data breach analysis and credit monitoring. In the event the Contractor provides payment of actual damages in an amount determined to be adequate by the Contracting Officer, the Contracting Officer may forgo collection of liquidated damages.

(d) *Purpose of liquidated damages*. Based on the results from VA's determination that there was a data breach caused by Contractor's or any of its agents' failure to protect or otherwise engaging in conduct to cause a data breach of VA sensitive personal information, and as directed by the Contracting Officer, the Contractor shall be responsible for paying to the VA liquidated damages in the amount of _____ [*Contracting Officer insert amount*] per affected individual to cover the cost of the following:

(1) Notification related costs

(2) Credit monitoring reports.

(3) Data breach analysis and impact.

(4) Fraud alerts.

(5) Identity theft insurance.

(e) *Relationship to termination clause, if applicable*. If the Government terminates this contract, purchase order, or agreement, in whole or in part under clause 52.249-8, Default—Fixed-Price Supply and Service, or any other related FAR or VAAR clause included in the contract, in addition to the required liquidated damages for data breach-related expenses specified in paragraph (c) above, the Contractor is liable for excess

costs for those supplies and services for repurchase as may be required under the Termination clause.

(End of clause)

Alternate I (FEB 2023). In commercial products or commercial services acquisitions awarded under the procedures of FAR part 8 or 12, substitute this paragraph (e) in lieu of paragraph (e) in the basic clause:

(e) *Relationship to termination clause, if applicable*. If the Government terminates this contract in whole or in part under the Termination for cause paragraph, FAR 52.212-4(m), Contract Terms and Conditions—Commercial Products and Commercial Services, the Contractor is liable for damages accruing until the Government reasonably obtains delivery or performance of similar supplies or services. These damages are in addition to costs of repurchase as may be required under the Termination clause.

Alternate II (FEB 2023). In simplified acquisitions exceeding the micro-purchase threshold that are for other than commercial products or commercial services awarded under the procedures of FAR part 13 (*see* FAR 13.302-5(d)(1) and the clause at FAR 52.213-4), substitute this paragraph (e) in lieu of paragraph (e) in the basic clause:

(e) *Relationship to termination clause, if applicable*. If the Government terminates this contract in whole or in part under the Termination for cause paragraph, FAR 52.213-4(g), Terms and Conditions – Simplified Acquisitions (Other Than Commercial Products and Commercial Services), or any other applicable FAR or VAAR clause, the Contractor is liable for damages accruing until the Government reasonably obtains delivery or performance of similar supplies or services. These damages are in addition to costs of repurchase as may be required under the Termination clause.

852.212-70 [Removed and Reserved]

16. Section 852.212-70 is removed and reserved.

17. Section 852.212-71 is revised to read as follows:

852.212-71 Gray Market and Counterfeit Items.

As prescribed in 812.301(f), insert the following clause:

GRAY MARKET AND COUNTERFEIT ITEMS (FEB 2023)

(a) No used, refurbished, or remanufactured supplies or equipment/parts shall be provided. This procurement is for new Original Equipment Manufacturer (OEM) items only. No gray market items shall be provided. Gray market items are OEM goods intentionally or unintentionally sold outside an authorized sales territory or sold by non-authorized dealers in an authorized sales territory.

(b) No counterfeit supplies or equipment/parts shall be provided. Counterfeit items include unlawful or unauthorized reproductions, substitutions, or alterations that have been mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitutions include used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

(c) Vendor shall be an OEM, authorized dealer, authorized distributor, or authorized reseller for the proposed equipment/system, verified by an authorization letter or other documents from the OEM. All software licensing, warranty and service associated with the equipment/system shall be in accordance with the OEM terms and conditions.

(End of clause)

18. Section 852.212-72 is added to read as follows:

852.212-72 Gray Market and Counterfeit Items—Information Technology Maintenance Allowing Other-than-New Parts.

As prescribed in 812.301(f), insert the following clause:

GRAY MARKET AND COUNTERFEIT ITEMS—INFORMATION TECHNOLOGY MAINTENANCE ALLOWING OTHER-THAN-NEW PARTS (FEB 2023)

(a) Used, refurbished, or remanufactured parts may be provided. No gray market supplies or equipment shall be provided. Gray market items are Original Equipment Manufacturer (OEM) goods intentionally or unintentionally sold outside an authorized sales territory or sold by non-authorized dealers in an authorized sales territory.

(b) No counterfeit supplies or equipment shall be provided. Counterfeit items include unlawful or unauthorized reproductions, substitutions, or alterations that have been mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitutions include used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

(c) Vendor shall be an OEM, authorized dealer, authorized distributor or authorized reseller for the proposed equipment/system, verified by an authorization letter or other documents from the OEM. All software licensing, warranty and service associated with the equipment/system shall be in accordance with the OEM terms and conditions.

(End of clause)

19. Section 852.239-70 is added to read as follows:

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 s*ecurity 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) *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)

20. Section 852.239-71 is added to read as follows:

852.239-71 Information System Security Plan and Accreditation.

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

INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION (FEB 2023)

All offers submitted in response to this solicitation or request for quotation shall address the approach for completing the security plan and accreditation requirements in clause 852.239-70, Security Requirements for Information Technology Resources.

(End of provision)

21. Section 852.239-72 is added to read as follows:

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)

22. Section 852.239-73 is added to read as follows:

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)

23. Section 852.239-74 is added to read as follows:

852.239-74 Security Controls Compliance Testing.

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

SECURITY CONTROLS COMPLIANCE TESTING (FEB 2023)

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security and privacy controls implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector

General. The government may conduct a security control assessment on shorter notice, to include unannounced assessments, as determined by VA in the event of a security incident or at any other time.

(End of clause)

24. Section 852.239-75 is added to read as follows:

852.239-75 Information and Communication Technology Accessibility Notice.

As prescribed in 839.203-70(a), insert the following provision:

INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE (FEB 2023)

(a) Any offeror responding to this solicitation must comply with established VA Information and Communication Technology (ICT) (formerly Electronic and Information (EIT)) accessibility standards. Information about Section 508 is available at http://www.section508.va.gov/.

(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 852.239-75, Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit appropriate VA Section 508 Checklists, in accordance with the checklist completion instructions. The purpose of the checklists is to assist VA acquisition and program officials in determining whether proposed ICT supplies, or information, documentation and services conform to applicable Section 508 accessibility standards. The checklists allow offerors or developers to self-evaluate their supplies and document—in detail—whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues.

(c) Respondents to this solicitation must identify any exception to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, *i.e.*, after award of

a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(End of provision)

25. Section 852.239-76 is added to read as follows:

852.239-76 Information and Communication Technology Accessibility.

As prescribed in 839.203-70(b), insert the following clause:

INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2023)

(a) All information and communication technology (ICT) (formerly referred to as electronic and information technology (EIT)) supplies, information, documentation and services support developed, acquired, maintained or delivered under this contract or order must comply with the ‘‘Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards’’ (*see* 36 CFR part 1194). Information about Section 508 is available at http://www.section508.va.gov/.

(b) The Section 508 accessibility standards applicable to this contract or order are identified in the specification, statement of work, or performance work statement. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) The Section 508 accessibility standards applicable to this contract are: _____ [*Contracting Officer: insert the applicable Section 508 accessibility standards*].

(d) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the Contractor submit a completed VA Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed VA Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(End of clause)

[FR Doc. 2023-00586 Filed: 1/24/2023 8:45 am; Publication Date: 1/25/2023]