

**PERFORMANCE WORK STATEMENT (PWS)**

**DEPARTMENT OF VETERANS AFFAIRS**

VA Office of the Chief Technology Officer

Office of the Chief Artificial Intelligence Officer

Artificial Intelligence Pilot Teams

Date**:** 4-16-2024

VA-24-00064764

**PWS Version Number:** 0.1

# BACKGROUND

## Mission of the requesting business office

The Office of the CTO (OCTO) serves the Department of Veterans Affairs Office of Information Technology’s (VA OIT) mission to deliver world-class IT products and services to VA and Veterans. OCTO works closely with core program portfolios across VA to examine the short and long-term needs of the Department, and to identify and fill gaps in VA’s technology portfolio. OCTO takes an approach to problem-solving, teamwork, and leadership that is built on agile development and results in ongoing improvement.

## DESCRIPTION OF THE SPACE

OCTO now serves a dual purpose as the VA Office of the Chief Artificial Intelligence Officer (OCAIO). The mission of OCAIO is to deliver world-class AI-enabled IT products and services to VA and Veterans in a 1) purposely, 2) effective and safe, 3) secure and private, 4) fair and equitable, 5) transparent and explainable, and 6) accountable and monitored fashion. These six pillars comprise the VA Framework for Trustworthy AI.

## Existing relevant documentation

* AI-enabled tools in production at VA must be consistent with the [VA Trustworthy AI Framework](https://department.va.gov/ai/wp-content/uploads/sites/14/2023/09/trustworth-framework.pdf).

# APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541-3549, “Federal Information Security Management Act (FISMA) of 2002”
2. “Federal Information Security Modernization Act of 2014”
3. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules”
4. FIPS Pub 199. “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
5. FIPS Pub 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
6. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
7. 10 U.S.C. § 2224, "Defense Information Assurance Program"
8. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
9. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
10. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
11. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, <https://www.va.gov/vapubs/index.cfm>
12. VA Handbook 0710, “Personnel Security and Suitability Program,” May 2, 2016, <https://www.va.gov/vapubs/index.cfm>
13. VA Directive and Handbook 6102, “Internet/Intranet Services,” August 5, 2019
14. 36 C.F.R. Part 1194 “Information and Communication Technology Standards and Guidelines,” January 18, 2017
15. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
16. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
17. NIST SP 800-66 Rev. 1, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,” October 2008
18. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended, January 18, 2017
19. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
20. VA Directive 6500, “VA Cybersecurity Program,” February 24, 2021

VA Handbook 6500, “Risk Management Framework for VA Information Systems VA Information Security Program,” February 24, 2021

1. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” March 12, 2019
2. VA Handbook 6500.5, “Incorporating Security and Privacy into the System Development Lifecycle,” March 22, 2010
3. VA Handbook 6500.6, “Contract Security,” March 12, 2010
4. VA Handbook 6500.8, “Information System Contingency Planning,” April 6, 2011
5. VA Handbook 6500.10, “Mobile Device Security Policy,” February 15, 2018
6. VA Handbook 6500.11, “VA Firewall Configuration,” August 22, 2017
7. OIT Process Asset Library (PAL), <https://www.va.gov/process/> . Reference Process Maps at <https://www.va.gov/process/maps.asp> and Artifact templates at <https://www.va.gov/process/artifacts.asp>
8. One-VA Technical Reference Model (TRM) (reference at <https://www.va.gov/trm/TRMHomePage.aspx>)
9. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
10. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
11. VA Handbook 6510, “VA Identity and Access Management,” January 15, 2016
12. VA Directive and Handbook 6513, “Secure External Connections,” October 12, 2017
13. VA Directive 6300, “Records and Information Management,” September 21, 2018
14. VA Handbook, 6300.1, “Records Management Procedures,“ March 24, 2010
15. NIST SP 800-37 Rev 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” December 2018
16. NIST SP 800-53 Rev. 5, “Security and Privacy Controls for Federal Information Systems and Organizations,” September 23, 2020 (includes updates as of 12/10/2020)
17. VA Directive 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” October 26, 2015
18. VA Handbook 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” March 24, 2014
19. OMB Memorandum 05-24, “Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,” August 5, 2005
20. OMB Memorandum M-19-17, “Enabling Mission Delivery Through Improved Identity, Credential, and Access Management,” May 21, 2019
21. OMB Memorandum, “Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation,” May 23, 2008
22. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011, (NOTE: Part A of the FICAM Roadmap and Implementation Guidance, v2.0, was replaced in 2015 with an updated Architecture (<https://arch.idmanagement.gov/#what-is-the-ficam-architecture>)
23. NIST SP 800-116 Rev 1, “Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access,“ June 2018
24. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, “Digital Identity Guidelines,” updated March 02, 2020
25. NIST SP 800-157, “Guidelines for Derived PIV Credentials,” December 2014
26. NIST SP 800-164, “Guidelines on Hardware-Rooted Security in Mobile Devices (Draft),” October 2012
27. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981, “Mobile, PIV, and Authentication,” March 2014
28. VA Memorandum, VAIQ #7100147, “Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12),” April 29, 2011 (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
29. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
30. VA Memorandum “Personal Identity Verification (PIV) Logical Access Policy Clarification,” July 17, 2019, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896>
31. Trusted Internet Connections (TIC) 3.0 Core Guidance Documents, <https://www.cisa.gov/publication/tic-30-core-guidance-documents>
32. OMB Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative,” September 12, 2019
33. OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure,” August 22, 2008
34. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
35. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
36. Executive Order 13834, “Efficient Federal Operations,” dated May 17, 2018
37. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
38. VA Directive 0058, “VA Green Purchasing Program,” July 19, 2013
39. VA Handbook 0058, “VA Green Purchasing Program,” July 19, 2013
40. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access,” January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
41. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
42. “Veteran Focused Integration Process (VIP) Guide 4.0,” January 2021, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
43. VA Memorandum “Proper Use of Email and Other Messaging Services,” January 2, 2018, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
44. “DevSecOps Product Line Management Playbook” version 2.0, May 2021, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946>
45. NIST SP 500-267B Revision 1, “USGv6 Profile,” November 2020
46. OMB Memorandum M-21-07, “Completing the Transition to Internet Protocol Version 6 (IPv6),” November 19, 2020
47. Social Security Number (SSN) Fraud Prevention Act of 2017
48. Section 240 of the Consolidated Appropriations Act (CAA) 2018, March 23, 2018
49. Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, December 03, 2020
50. Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023
51. OMB Memorandum M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence, March 28, 2024

# SCOPE OF WORK

## Product vision

AI instituted in a responsible manner has enormous potential to benefit Veterans, VA healthcare providers, and VA employees. Our vision is for VA to be a national leader in responsible use of AI to reduce healthcare provider burnout, improve Veteran and VA employee experience, and provide higher quality care for Veterans.

## Desired user outcomes

### Example user outcomes are as follows:

### Reducing healthcare provider burnout

### Time spent on clinical documentation decreases from X to Y.

### Time spent on clinical documentation after hours (“pajama time”) decreases from X to Y.

### Veteran satisfaction with clinical encounters increases from X to Y.

### % of providers experiencing symptoms of burnout decreases from X to Y.

### Improving Veteran and VA Employee experience

### Time spent per specific administrative task decreases from X to Y.

### Employee satisfaction increases from X to Y.

### Accuracy in completed specific administrative task increases from X to Y.

### Number of days needed for Veteran to receive response to Ask VA query decreases from X to Y.

### Better care for Veterans

### Adherence to evidence-based clinical guidelines increases from X to Y.

### Backlog of Community Care records to be summarized and/or ingested into VA electronic health record decreases from X to Y.

## Desired business outcomes

Example outcomes for some of the problem focus areas described above are as follows:

1. Reducing healthcare provider burnout
   1. Turnover of healthcare providers reduces from X to Y due to reduced levels of burnout.
   2. Access to care for Veterans increases due to increased provider capacity, evidenced by reduced appointment wait time from X to Y.
2. Improving Veteran and VA Employee experience
   1. Time spent per specific administrative task decreases from X to Y.
   2. Employee satisfaction increases from X to Y; employee turnover reduces from X to Y.
   3. Accuracy in completed specific administrative task increases from X to Y.
   4. Number of manual interventions needed per benefits claims decision decreases from X to Y.
3. Better care for Veterans
   1. Adherence to evidence-based clinical guidelines increases from X to Y.

## Outcomes we want to avoid

We aim to avoid the following outcomes:

1. Deploying AI without a clear purpose or meaningful outcome.
2. Deploying AI that poses unnecessary or unacceptable risk to Veterans or VA employees.
3. Deploying solutions that are not adopted by end users given lack of workflow integration.

## Overview of work

The Contractor shall support a variety of initiatives related to the focus areas for problems to solve in section 3.1-3.3 above. In general, VA requires contractor support with prioritizing, designing, and executing AI-enabled pilot projects raised by stakeholders across VA. Work to be completed may include, but is not limited to:

* Developing deep understanding of user problems and potential areas for impact. Potentially conducting interviews with stakeholders, surveys, and observational research to gain insights about user perspectives, needs, problems, behaviors.
* Assist VA in prioritizing amongst problems to solve and assisting VA in determining where to invest effort in piloting.
* Assisting VA in determining whether an AI-enabled approach to specific problems is appropriate, and if applicable, which specific Machine Learning (ML)-based approaches could be leveraged. Providing input to VA stakeholders about where AI-enabled approaches may and may not be appropriate.
* Setting measurable goals and supporting metrics collection. Developing deep understanding of relevant data available.
* Developing solution prototypes and minimum viable products for testing with users.
* Developing and releasing solutions to production for live pilots with users.
* Where applicable, conducting research with VA stakeholders to develop machine learning models to support their use cases.
* Where applicable, conducting research with VA stakeholders to engineer prompts for large language model (LLM)-based tools to support their use cases.
* Creating user-facing educational and training materials on the AI-enabled solutions developed.
* Integrating third party and/or homegrown AI-enabled solutions with existing VA systems, including but, not limited to, VistA/CPRS, Oracle Health, Ask VA, VA Chatbot, employee-facing customer support interfaces, employee-facing benefits adjudication interfaces.
* Monitoring performance of solutions developed.
* Collecting user feedback on solutions developed and iterating upon solutions accordingly.
* Ensuring solutions are consistent with VA Trustworthy AI Framework.

## Transition Support (Optional Task 1)

Transition of a product to a new contractor or the Government is sometimes necessary. It is critical to the continued functionality of OCTO products that all contractors are diligent in transitions between teams to ensure there is no disruption in Veteran services. The most important factors in these transitions are the availability of well written documentation and good faith communications. This optional task shall be for a period of up to 60 days, if exercised by the Government. The Contractor must submit a Transition Support Package within (7) days upon optional task exercise. The Transition Support Package shall consist of at least the following, and is critical to the successful transition in OCTO, and must be available in the relevant GithHub repository:

1. All documentation
2. All access to the platform (if applicable) and anything interacting with the platform or application, for which the incoming vendor will require access
3. All relevant information necessary for Developer onboarding – interaction with 3rd party tools, downstream services, application interactions outside va.gov

In consult with the relevant OCTO Product Owner and COR, the Contractor shall create a list of all relevant stakeholders both inside OCTO, across VA, and outside VA (if relevant). The contractor shall ensure frank and open communication between all staff of the exiting and incoming contractors. At a minimum the outgoing contractor shall ensure the incoming contractor has access to the following:

1. Product documentation including product outlines/briefings, objectives and key results (OKRs), roadmaps and active epics/stories, stakeholder landscape maps, decision records, and analytics
2. Developer documentation including READMEs, set-up instructions, diagrams, relevant databases and services.
3. Design documentation including prototypes, user research reports, design decisions for products in production, early designs for incomplete products, content strategy, and records of interactions with the collaboration cycle.
4. Access to accounts for third-party products such as tooling or SaaS products that will be taken over by the new team.

Although not exhaustive, the following are typical interactions which the contractor shall support during transition:

1. A handoff coordination meeting between the leads of the incoming and outgoing teams
2. Community of Practice specific orientations to the available documentation allowing the outgoing team to ask questions
3. Conversations about the stakeholder landscape and typical communication patterns
4. Demonstrations of specific functionality in the application

**Deliverable:**

* + 1. Transition Support Package

## ADDITIONAL PRODUCT AND DEVELOPMENT SUPPORT (OPTIONAL TASK 2)

The optional tasks will be used to provide increased capacity to deliver features related to Artificial Intelligence Pilot Teams as described in this PWS. Upon execution of this optional task, the Contractor shall provide additional feature and product development support. These optional tasks may be exercised for a quantity of additional support not to exceed the limit set forth in the Price Schedule in both the Base Period and the Option Period. The specific scope of functionality to be delivered for each optional task exercise will be agreed to by the VA Program Manager/Product Owner and Contracting Officer’s Representative (COR) prior to exercise of the optional tasks by the CO based on current business priorities. The Contractor shall provide a proposal for the requested support including by a Level of Effort (LOE) made up of the required level of resources with appropriate technical skill sets, limited to the Labor Categories included in Attachment A. Prior to each exercise of this Optional Task, the Contractor shall provide a short description of what work will be completed, a list of all deliverables, and a schedule for implementation including milestones for delivery and associated milestone payments. The Government will review and agree to the proposal, after which a modification will be made to the contract adding the proposal, providing funding, and reducing the available ceiling on the line item accordingly.

## Development methodology and working principles

The Contractor’s support and solutions shall follow the practices described in the Digital Services Playbook (<https://playbook.cio.gov>). The Contractor shall be familiar with the concepts in each play and implement them in its approaches and support. The Contractor shall deliver modern digital services that use DevOps techniques that embrace Continuous Integration / Continuous Delivery (CI/CD). The Contractor shall deliver secure and tested modern web application designs using automated testing frameworks.

The Contractor shall provide VA with teams that shall deliver viable, digital solutions in support of VA’s strategic mission and objectives. Specifically, the Contractor shall:

1. Deliver high-quality, functional products that are measured by user feedback from surveys, research, etc.
2. Follow the practices described in the “Digital Services Playbook” (<https://playbook.cio.gov>).
3. Be agile. Incorporate Agile methodologies and ceremonies into work, such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities.
4. Actively involve users in the design of all solutions. Incorporate best practices for modern user research and usability testing, such as (but not limited to) creating user personas, problem space definitions, affinity maps, user flow diagrams, wireframes, information architecture diagrams, design prototypes, user research plans, conversation guides, and user research synthesis.
5. Maintain a consistent look, feel, and voice across user facing sites and services. Incorporate best practices defined in the VA Design System and VA Content Style Guide (<https://design.va.gov/>).
6. Personalize solutions for the individual or team using the product (<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/>, <https://www.whitehouse.gov/wp-content/uploads/2018/06/s280.pdf>)
7. Optimize web applications for mobile-first operation, with all solutions being equally available on both mobile and desktop whenever possible. Incorporate robust accessibility principles into design, development and testing for all web applications to deliver high-quality digital experiences to users of assistive devices.
8. Protect user information with best-in-class security, given the constraints of the environment.
9. Use DevOps techniques of CI/CD across all environments including, at a minimum, development, staging, and production. (<http://github.com/department-of-veterans-affairs/va.gov-team/tree/master/platform/engineering/>)
10. Use automated testing frameworks to create unit tests, integration tests, functional/black box tests, and load tests (or their equivalents as applicable) to test 100% of functionality delivered. Strive for compliance with Test Driven Development practices.
11. Ensure configuration and sensitive data, including data the VA defines as sensitive, are not present in source code, and are stored in encrypted credential management systems.
12. Deliver all code not containing configuration or sensitive data to an open source repository per Office of Management and Budget Guidance M-16-21.
13. Cultivate a positive, trusting, and cooperative working relationship with the Government and all other vendors supporting this work.

# PERFORMANCE DETAILS

## Period of performance (PoP) and budget estimate

The Period of Performance (PoP) shall be one (1) 12-month Base Period, with one (1) 12-month Option Period, and two Optional Tasks.

## Place of performance

Efforts under this task order can be performed at any location within the United States. All work locations must be able to accommodate the Hours of Work specified in Section 7.3.

## Travel

Travel shall be reimbursed on a Time & Materials basis in accordance with the Federal Travel Regulations and requires advanced concurrence by the COR. Contractor travel within the local commuting area will not be reimbursed.   
  
While the Government cannot accurately estimate the amount of travel to an extent it can be firm fixed price, the following was used as the basis for the Government’s cost estimate: Travel is expected for a yearly in-person planning meeting during the Base Period and Option Period, including the full contract team, within the Continental United States for a period of approximately 3 days.

## Hours of work

The contractor shall set their own work hours within the following parameters: contractors may be required to attend meetings with Government personnel between standard east coast work hours (typically 9am – 5pm ET) monitoring and production support will be required between 7am – 8pm ET.

## Contract type

The effort shall be proposed on a Time and Materials (T&M) basis and Firm Fixed Price (FFP) basis. All labor shall be FFP per sprint while all travel shall be on a T&M basis.

The Anticipated LoE for this Task Order is 11 full time equivalents.

## Key personnel

**Senior Product Manager**

* + Experience with developing product requirements documents, product roadmaps, and associated artifacts, including proven experience in leading cross-functional teams and driving product development from concept to launch.
  + Experience performing research, developing a deep understanding of the customer, working with and eliciting information from diverse groups of stakeholders and developing clear technical, actionable requirements.
  + Experience launching products leveraging artificial intelligence, to include generative AI and large language models.
  + Ability to effectively articulate a product vision and strategy.
  + Preferred: Strong understanding of health IT data privacy and security practices.
  + Preferred: Experience developing Veteran-facing and/or employee-facing products for VA.

**Engineering lead**

* + Experience building end-to-end data science solutions, including operationalizing models.
  + Experience in designing overarching GenAI system architecture.
  + Strong proficiency in Python, R, SQL, and experience with libraries/frameworks such as PyTorch, TensorFlow, and Scikit-learn.
  + Experience with cloud and modern data science tools and platforms such as Databricks MLFlow and Azure ML.
  + Ability to guide and manage an engineering team effectively.
  + Preferred: Strong understanding of health IT data privacy and security practices.
  + Preferred: Experience developing Veteran-facing and/or employee-facing products for VA.

**Senior data analyst, healthcare**

* + Data management experience; knowledgeable in database rules, writing queries, and relational database creation and management (create, query, relate)
  + Experience in the development of algorithms leveraging R, Python, or SQL/NoSQL
  + Experience with deriving insights from unstructured and structured healthcare data, and ability to effectively communicate those insights to stakeholders and clinical leaders.
  + Experience working with healthcare terminology standards, e.g. ICD-10, CPT, LOINC, RxNorm, SNOMED.
  + Preferred: Experience working with healthcare data from VHA.

**Additional Information**

SCRUM teams will be considered acceptable when they can effectively work. This may include some resources that are staffed, but not cleared. This will be case by case and worked with the COR. For the initial team to be deemed ready to work, all members of the team will have a Personal Security Adjudication Center letter in order to obtain access to working tools such as GitHub and Slack that do not require VA network access. Access to Amazon Web Services requires an Electronic Questionnaires for Investigations Processing release date.

## Kickoff meeting

The Contractor shall hold a kickoff meeting within 10 days after task order award. The Contractor shall present, for review and approval by the Government, at a minimum the details of the intended approach, work plan, and onboarding plan. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least five calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite the Contracting Officer, Contract Specialist, COR and the VA Program Manager/Product Owner.

# Quality Assurance Surveillance Plan (QASP)

## Product specific objectives and key results

The Government is open to discussion with the vendor about appropriate QASP metrics for this task order after award.

## Recurring deliverables

**Delivery and Monitoring Report and Roster:** The Contractor shall provide a single monthly report, detailing and providing links to all stories, epics and other work completed. This includes a plain language description of all work accepted by the Government Product Owner and COR at the end of each sprint. This report shall include, in plain language, additional details about the project status, sprint team velocity, sprint team goal completion, and highlight project risks. The report shall also highlight and provide links to key infrastructure and application monitoring data. The report shall also include details with links to documentation for any critical incidents or outage events that resulted in service outages or significant service degradations. The Contractor shall attach or provide links to postmortem documentation for all critical incidents or outage events. Should there not be any reported incidents during the reporting period, a link to the relevant monitoring tools is sufficient. The specific data points and format of this monthly report shall be determined by the Contractor in collaboration with the VA Program Manager/Product Owner and COR. Lastly, the Contractor shall submit a roster to the COR that includes the Status of Government Furnished Equipment (GFE) for all GFE all staff, as applicable.

# Data and Open Source Requirements

The Government shall receive Unlimited Rights to data first produced in performance of this contract in accordance with FAR 52.227-14, “Rights In Data-General” (MAY 2014). This includes all rights to source code and any and all documentation created in support thereof. License rights in any Commercial Computer Software shall be governed by FAR 52.227-19, “Commercial Computer Software License” (DEC 2007). Any data delivered shall be submitted and protected in accordance with VA handbook 6500.

VA intends that the software delivered under this task order will be publicly posted without restriction. To the extent that the Contractor(s) seeks to incorporate into the software delivered under this task order any software that was not first produced in the performance of this task order, VA encourages the Contractor(s) to incorporate either software that is in the public domain, or free and open source software that qualifies under the Open Source Definition promulgated by the Open Source Initiative. In any event, the Contractor(s) must promptly disclose to VA in writing, and list in the documentation, any software incorporated in the delivered software that is subject to a license fee.

# Other Administrative Items

# GENERAL REQUIREMENTS

## ENTERPRISE AND IT FRAMEWORK

### VA TECHNICAL REFERENCE MODEL

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OIT Technical Reference Model (VA TRM). The VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. Moreover, the VA TRM, which includes the Standards Profile and Product List, serves as a technology roadmap and tool for supporting OIT. Architecture & Engineering Services (AES) has overall responsibility for the VA TRM.

### FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM)

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), [https://www.ea.oit.va.gov/EAOIT/VA\_EA/Enterprise\_Technical\_Architecture.asp](https://www.ea.oit.va.gov/EAOIT/VA_EA/Enterprise_Technical_Architecture.asp" \o "Link to One-VA Enterprise Technical Architecture), and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, <https://www.oit.va.gov/library/recurring/edp/index.cfm>. The Contractor shall ensure all Contractor delivered applications and systems comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in VA Handbook 6510 VA Identity and Access Management, VA Handbook 0735 Homeland Security Presidential Directive 12 (HSPD-12) Program, and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, VA Handbook 6500 Appendix F, “VA System Security Controls”, and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV card and/or Common Access Card (CAC), as determined by the business need.

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-05-24, M-19-17, and NIST Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-05-24 and M-19-17 can be found at: <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf>, and <https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf> respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

The Contractor shall ensure all Contractor delivered applications and systems support:

1. Automated provisioning and are able to use enterprise provisioning service.
2. Interfacing with VA’s Master Person Index (MPI) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion-based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VIEWS 00155984, PIV Logical Access Policy Clarification <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896>.

The required Assurance Levels for this specific effort are Identity Assurance Level 3, Authenticator Assurance Level 3, and Federation Assurance Level 3.

### INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support Internet Protocol Version 6 (IPv6) based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020 (<https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf>). IPv6 technology, in accordance with the USGv6 Program [(https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1](file://R04.med.va.gov/V03/EAS/Users/vhaeasWymbsk/TEMPLATES--NEW%20TAC%20PROCESS/PWS%20TEMPLATE%20(DO%20NOT%20TOUCH)%20-%20In%20Process%20Revisions/DO%20NOT%20TOUCH%20(next%20version/IPv6/(https:/www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1)), NIST Special Publication (SP) 500-267B Revision 1 “USGv6 Profile” (<https://doi.org/10.6028/NIST.SP.500-267Br1>), and NIST SP 800-119 “Guidelines for the Secure Deployment of IPv6” (<https://doi.org/10.6028/NIST.SP.800-119>), compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and dual stack (IPv6 / IPv4) operations.

### TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative“ (<https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf>), VA Directive 6513 “Secure External Connections”, and shall comply with the TIC 3.0 Core Guidance Documents, including all Volumes and TIC Use Cases, found at the Cybersecurity & Infrastructure Security Agency (CISA) (<https://www.cisa.gov/publication/tic-30-core-guidance-documents>). Any deviations must be approved by the VA TIC 3.0 Working Group at [vaoisesatic30team@va.gov](mailto:vaoisesatic30team@va.gov).

### STANDARD COMPUTER CONFIGURATION

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 10 (64bit), Edge (Chromium based), and 365 Apps for enterprise.  Applications delivered to VA and intended to be deployed to Windows 10 workstations shall be delivered as a signed .msi package with switches for silent and unattended installation and updates shall be delivered in signed .msp file formats for easy deployment using Microsoft Endpoint Configuration Manager (CM) VA’s current desktop application deployment tool.  Signing of the software code shall be through a vendor provided certificate that is trusted by VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign.  The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

### VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM)

The Contractor shall support VA efforts IAW the updated Veteran Focused Integration Process (VIP) and Product Line Management (PLM). The major focus of the new VIP is on Governance and Reporting and is less prescriptive, with a focus on outcomes and continuous delivery of value. Product Line Management (PLM) is a framework that focuses on delivering functional products that provide the highest priority work to customers while delivering simplified, reliable, and practical solutions to the business, medical staff, and our Veterans. The VIP Guide is a companion guide to the PLM Playbook and can be found at: <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371> and the PLM Playbook can be found at <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946>. The PLM Playbook pivots from project-centric to product-centric delivery and contains descriptive practices that focuses on outcomes. The PLM Playbook contains a set of “plays” that implement Development, Security, and Operations (DevSecOps) principles and processes such as automated development, continuous integration/continuous delivery, and release on demand. The PLM Playbook details how product lines implement Lean-Agile principles, methods, practices, and techniques through levels of maturity. VIP and PLM are the authoritative processes that IT projects must follow to ensure development and delivery of IT products.

### PROCESS ASSET LIBRARY (PAL)

The Contractor shall perform their duties consistent with the processes defined in the OIT Process Asset Library (PAL).  The PAL scope includes the full spectrum of OIT functions and activities, such as VIP project management, operations, service delivery, communications, acquisition, and resource management. PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards and guides to assist the OIT workforce, Government and Contractor personnel. The Contractor shall follow the PAL processes to ensure compliance with policies and regulations and to meet VA quality standards.  The PAL includes the contractor onboarding process consistent with Section 6.2.2 and can be found at <https://www.va.gov/PROCESS/artifacts/maps/process_CONB_ext.pdf>. The main PAL can be accessed at [www.va.gov/process](http://www.va.gov/process).

### AUTHORITATIVE DATA SOURCES

The VA Enterprise Architecture Repository (VEAR) is one component within the overall EA that establishes the common framework for data taxonomy for describing the data architecture used to develop, operate, and maintain enterprise applications. The Contractor shall comply with the department’s Authoritative Data Source (ADS) requirement that VA systems, services, and processes throughout the enterprise shall access VA data solely through official VA ADSs where applicable, see below.  The Information Classes which compose each ADS are located in the VEAR, in the Data & Information domain. The Contractor shall ensure that all delivered applications and system solutions support:

1. Interfacing with VA’s Master Person Index (MPI) (formerly the Master Veteran Index (MVI)) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
2. Interfacing with Capital Asset Inventory (CAI) to conduct real property record management actions, if the solution relies on real property records data. CAI is the authoritative source for VA real property record management data.
3. Interfacing with electronic Contract Management System (eCMS) for access to contract, contract line item, purchase requisition, offering vendor and vendor, and solicitation information above the micro-purchase threshold, if the solution relies on procurement data. ECMS is the authoritative source for VA procurement actions data.
4. Interfacing with HRSmart Human Resources Information System to conduct personnel action processing, on-boarding, benefits management, and compensation management, if the solution relies on personnel data. HRSmart is the authoritative source for VA personnel information data.
5. Interfacing with Vet360 to access personal contact information, if the solution relies on VA Veteran personal contact information data. Vet360 is the authoritative source for VA Veteran Personal Contact Data.
6. Interfacing with VA/Department of Defense (DoD) Identity Repository (VADIR) for determining eligibility for VA benefits under Title 38, if the solution relies on qualifying active duty military service data. VADIR is the authoritative source for Qualifying Active Duty military service in VA.

### SOCIAL SECURITY NUMBER (SSN) REDUCTION

The Contractor solution shall support the Social Security Number (SSN) Fraud Prevention Act (FPA) of 2017 which prohibits the inclusion of SSNs on any document sent by mail. The Contractor support shall also be performed in accordance with Section 240 of the Consolidated Appropriations Act (CAA) 2018, enacted March 23, 2018, which mandates VA to discontinue using SSNs to identify individuals in all VA information systems as the Primary Identifier. The Contractor shall ensure that any new IT solution discontinues the use of SSN as the Primary Identifier to replace the SSN with the ICN in all VA information systems for all individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA Master Person Index (MPI) for identity traits to include the use of the ICN as the Primary Identifier. The Contractor solution may only use a Social Security Number to identify an individual in an information system if and only if the use of such number is required to obtain information VA requires from an information system that is not under the jurisdiction of VA.

### SOFTWARE AND LICENSING REQUIREMENTS

The Contractor shall be responsible for the provision of all software licenses and any associated licensing maintenance required for any development, delivery, integration, operation, and/or maintenance associated with its proposed application(s), software products, software solution, and/or system including, but not limited to, any and all application(s), software and/or software products that comprise, are a part of, or integrate with the Contractor’s proposed application(s), software products, software solution, and/or system for the life of any resulting contract.

## SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.

## POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity, and the level of background investigation commensurate with the required level of access for tasks within the PWS. All tasks are considered **Tier 2 / Moderate Risk** unless otherwise specified in the table below.

**Position Sensitivity and Background Investigation Requirements by Task**

|  |  |  |  |
| --- | --- | --- | --- |
| **Task Number** | **Tier 1/ Low Risk** | **Tier 2 / Moderate Risk** | **Tier 4 / High Risk** |
| Across all tasks | ☐ | ☐ | ☒ |

The Tasks identified above, and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working.  The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

### CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

**Contractor Responsibilities:**

1. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak, and understand the English language.
2. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor’s Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
3. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
4. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
5. Optional Form 306
6. Self-Certification of Continuous Service
7. VA Form 0710
8. Completed SIC Fingerprint Request Form
9. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management’s (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
10. The Contractor employee shall certify and release the e-QIP document, print, and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a “click to sign” process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
11. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
12. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed “Contractor Rules of Behavior”, and with a valid, operational PIV credential for PIV-only logical access to VA’s network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.
13. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
14. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
15. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

**Deliverable:**

1. Contractor Staff Roster

## METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: Microsoft 365, MS Word 2000/2003/2007/2010/2019, MS Excel 2000/2003/2007/2010/2019, MS PowerPoint 2000/2003/2007/2010/2019, MS Project 2000/2003/2007/2010/2019, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010/2019, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

## PERFORMANCE METRICS

Performance metrics will be determined collaboratively with the contractor after award.

The COR will utilize the Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

## FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA’s network. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print, or save any VA information accessed via CAG at any time. VA prohibits remote access to VA’s network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, PAL, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, documents, and requirements repositories, etc. as required for the development, storage, maintenance, and delivery of products within the scope of this effort.  The Contractor shall not transmit, store, or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP’s) and Authority to Operate (ATO)’s for all systems/LAN’s accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

## GOVERNMENT FURNISHED PROPERTY

The Government has multiple remote access solutions available to include Citrix Access Gateway (CAG), Site-to-Site Virtual Private Network (VPN), and RESCUE VPN.

The Government’s issuance of Government Furnished Equipment (GFE) is limited to Contractor personnel requiring direct access to the network to: development environments; install, configure and run Technical Reference Model (TRM) approved software and tools (e.g., Oracle, Fortify, Eclipse, SoapUI, WebLogic, LoadRunner); upload/download/ manipulate code, run scripts, and apply patches; configure and change system settings; check logs, troubleshoot/debug, and test/QA.

When necessary, the Government will furnish desktops or laptops, for use by the Contractor to access VA networks, systems, or applications to meet the requirements of this PWS. The overarching goal is to determine the most cost-effective approach to providing needed access to the VA environment coupled with the need to ensure proper Change Management principles are followed. Contractor personnel shall adhere to all VA system access requirements for on-site and remote users in accordance with VA standards, local security regulations, policies, and rules of behavior. GFE shall be approved by the COR and Program Manager on a case-by-case basis prior to issuance.

Based upon the Government assessment of remote access solutions and requirements of this effort, the Government estimates that the following GFE will be required by this effort:

1. 38 Standard Laptops

The Government will not provide IT accessories including but not limited to Mobile Wi-Fi hotspots/wireless access points, additional or specialized keyboards or mice, laptop bags, extra charging cables, extra Personal Identity Verification card readers, peripheral devices, or additional Random Access Memory (RAM). The Contractor is responsible for providing these types of IT accessories in support of this effort as necessary and any VA installation required for these IT accessories shall be coordinated with the COR.

Additionally, the Contractor shall provide a status of all reportable GFE as part of the deliverables in PWS 6.2.  For purposes of this report, reportable GFE includes equipment that is furnished by the Government as tangible “personal” property which the Contractor takes possession of, physically leaves a Government facility, and needs to be returned the end of Contractor performance.  The following information shall be provided for each piece of GFE:

1. Name of Contractor employee assigned to the GFE
2. Type of Equipment (Make and Model)
3. Tracking Number/Serial Number
4. VA Bar Code
5. Location
6. Value
7. Total Value of Equipment
8. Anticipated Transfer Date to Government
9. Anticipated Transfer Location

# ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

1. Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations.  The Contractor’s firewall and web server shall meet or exceed VA minimum requirements for security.  All VA data shall be protected behind an approved firewall.  Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible.  The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to assessment and authorization and continuous monitoring

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE).  Security Requirements include:  a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal.  The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, “Contract Security,” March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, “Contract Security” shall also be included in every related agreement, contract, or order.  The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS) 2.0, and will be tracked therein. The TMS 2.0 may be accessed at [h](https://www.tms.va.gov/SecureAuth35/" \o "Link to TMS 2.0 Homepage)[ttps://www.tms.va.gov/SecureAuth35/](https://www.tms.va.gov/SecureAuth35/" \o "Link to TMS 2.0 Homepage)

. If you do not have a TMS 2.0 profile, go to

<https://www.tms.va.gov/SecureAuth35/>

and click on the “Create New User” link on the TMS 2.0 to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

1. VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with VA Enterprise Architecture (EA), available at <http://www.ea.oit.va.gov/index.asp> in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP).  VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

* 1. **VA Internet and Intranet Standards**

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor’s work includes managing, maintaining, establishing, and presenting information on VA’s Internet/Intranet Service Sites.  This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): <https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1056&FType=2>

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): <https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1055&FType=2>

1. Notice of the Federal Accessibility Law Affecting All Information and Communication Technology (ICT) Procurements (Section 508)

On January 18, 2017, the Architectural and Transportation Barriers Compliance Board (Access Board) revised and updated, in a single rulemaking, standards for electronic and information technology developed, procured, maintained, or used by Federal agencies covered by Section 508 of the Rehabilitation Act of 1973, as well as our guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

* 1. Section 508 – Information and Communication Technology (ICT) Standards

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>. A printed copy of the standards will be supplied upon request.

Federal agencies must comply with the updated Section 508 Standards beginning on January 18, 2018. The Final Rule as published in the Federal Register is available from the Access Board: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule>.

The Contractor shall comply with “508 Chapter 2: Scoping Requirements” for all electronic ICT and content delivered under this contract. Specifically, as appropriate for the technology and its functionality, the Contractor shall comply with the technical standards marked here:

E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)

E204 Functional Performance Criteria

E206 Hardware Requirements

E207 Software Requirements

E208 Support Documentation and Services Requirements

* 1. Compatibility with Assistive Technology

The standards do not require installation of specific accessibility-related software or attachment of an assistive technology device. Section 508 requires that ICT be compatible with such software and devices so that ICT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

* 1. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the Section 508 Chapter 2: Scoping Requirements standards identified above.

The Government reserves the right to test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

1. Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property.  Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed.  It is the responsibility of the Contractor to park in the appropriate designated parking areas.  VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.
6. Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access toProtected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”).  Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA.  These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA.  Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38.  Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information.  Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities.  Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract.  Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature.  If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information.  Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives.  The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
8. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
9. Controlled access to system and security software and documentation.
10. Recording, monitoring, and control of passwords and privileges.
11. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
12. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
13. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
14. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
15. Contractor does not require access to classified data.
16. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements.  All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none.  The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
17. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed.  In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

# ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

1. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS
   1. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.
   2. All Contractors, Subcontractors, and third-party servicers and 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 must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.
   3. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.
   4. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.
   5. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor’s employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.
2. VA INFORMATION CUSTODIAL LANGUAGE
3. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
4. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor’s information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA’s sanitization requirements. VA reserves the right to conduct on-site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
5. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.
6. 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 VA information or information systems after execution of the contract, or if 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 in this contract.
7. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement 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.
8. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.
9. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Directive 1605.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
10. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.
11. The Contractor/Subcontractor’s firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.
12. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA 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 VA CO for response.
13. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 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. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above-mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.
14. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.
15. INFORMATION SYSTEM DESIGN AND DEVELOPMENT
16. 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 FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. 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 (reference VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). 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 Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.*
17. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 10 and future versions, as required.
18. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.
19. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
20. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information* *Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.
21. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.
22. The Contractor/Subcontractor agrees to:
    1. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:
       1. The Systems of Records (SOR); and
       2. The design, development, or operation work that the Contractor/Subcontractor is to perform;
    2. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and
    3. Include this Privacy Act clause, including this subparagraph (c), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.
23. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.
    1. “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.
    2. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.
    3. “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
24. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, 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 vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.
25. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical***,*** based on the severity of the incident.
26. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.
27. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.
28. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE
    1. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor’s security control procedures must be equivalent, to 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 operational approval. All external Internet connections to VA network involving VA information must be in accordance with the 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).
    2. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.
    3. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires A&A of the Contractor’s systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection security agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.
    4. 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 PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA 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 approved by the Government. 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. 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 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.
    5. 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. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.
    6. VA prohibits the installation and use of personally owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. 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.
    7. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) 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 (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.
    8. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:
29. Vendor must accept the system without the drive;
30. VA’s initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
31. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
32. Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;
33. The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
34. Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
35. A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.
36. SECURITY INCIDENT INVESTIGATION
    1. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.
    2. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.
    3. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.
    4. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and 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.
37. LIQUIDATED DAMAGES FOR DATA BREACH
    1. Consistent with the requirements of 38 U.S.C. §5725, a 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 or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.
    2. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. 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. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.
    3. Each risk analysis shall address all relevant information concerning the data breach, including the following:
       1. Nature of the event (loss, theft, unauthorized access);
       2. Description of the event, including:
       3. date of occurrence;
       4. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
       5. Number of individuals affected or potentially affected;
       6. Names of individuals or groups affected or potentially affected;
       7. 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;
       8. Amount of time the data has been out of VA control;
       9. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
       10. Known misuses of data containing sensitive personal information, if any;
       11. Assessment of the potential harm to the affected individuals;
       12. Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
       13. 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.
    4. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
       1. Notification;
       2. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
       3. Data breach analysis;
       4. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
       5. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
       6. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.
38. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, 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 under the clauses contained within the contract. With 10 working-day’s 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.

1. TRAINING
2. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
3. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security Rules of Behavior, relating to access to VA information and information systems;
4. Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS 2.0 # VA 10176) and complete this required privacy and information security training annually;
5. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]
6. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.
7. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, 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.

POINTS OF CONTACT

**Contracting Officer:**

Name: Jeffrey Bishop

Voice: 512-364-8944

Email: [jeffrey.bishop3@va.gov](mailto:jeffrey.bishop3@va.gov)

**Contract Specialist:**

Name: Michael Berberich

Voice: 878-377-5162

Email: [Michael.berberich@va.gov](mailto:Michael.berberich@va.gov)