PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology
Office of Privacy and Records Management

Privacy Professionalization Training Program

Date: 6/21/2016
TAC-16-29841
PWS Version Number: 1.7

Contents

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), VA Privacy Service is to provide benefits and services to Veterans of the United States. In meeting these goals, OI&T strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

OI&T intends to transition projects from the Project Management Accountability System (PMAS) project management process into the Veteran-focused Integration Process (VIP) project management process in the 2016-2017 timeframe (https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. VIP is the follow-on framework from PMAS for the development and management of IT projects which will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities. The VIP framework unifies and streamlines IT delivery oversight and will deliver IT products more efficiently, securely, and predictably. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence. VIP is a significant evolution from PMAS, creating a more flexible process that has fewer documentation requirements and milestones, and delivers products in shorter increments. VIP is currently undergoing a Pilot Program and is currently in a draft state and will continue to evolve. Once the pilot is complete, requirements outlined in this PWS may be transitioned to the VIP framework during the Period of Performance (PoP) of this contract.

VA Privacy Service is responsible for overseeing, directing, and establishing the long and short-term goals for VA's privacy program. As the impact of privacy issues increase, VA Privacy Service identifies Department-wide privacy needs and implements strategies to meet those needs. VA Privacy Service advises and makes recommendations to senior officials concerning the feasibility of the Department's objectives into overall VA planning, programming, and budgeting processes. While VA Privacy Service develops policies, programs, and materials at a central level, field Privacy Officers around the country are responsible for implementation and distribution.

VA has over 300,000 employees and maintains extensive records on approximately 26 million Veterans. Sound privacy practices are critical to operations as the volume of personal information VA handles continues to grow. VA Privacy Service develops general and specialized privacy training courses for VA staff and contractors to comply with Federal mandates such as the Privacy Act, Health Insurance Portability and Accountability Act, Federal Information Security Management Act, and E-Government

Act. VA Privacy Service is updating its curriculum to address VA's current privacy challenges and recent changes in Federal privacy laws, regulations, and guidance.

This PWS includes the development and implementation of a Department-wide privacy training program to include a professionalization program tailored to VA privacy professionals and officers and comprehensive and job-specific privacy training courses and guidance materials for all personnel that handle personal information; that are directly involved in the administration of personal information or information technology systems; or, have significant privacy responsibilities.

2.0 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, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
8. VA Directive 0710, "Personnel Suitability and Security Program," June 4, 2010, http://www.va.gov/vapubs/
9. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, http://www.va.gov/vapubs
10. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
11. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000
13. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012

18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
19. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
20. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI)”, October, 28, 2015
21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle”, March 22, 2010
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010
24. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011
25. Project Management Accountability System (PMAS) portal (reference https://www.voa.va.gov/pmas/)
26. OI&T ProPath Process Methodology (reference process maps at http://www.va.gov/PROPATH/Maps.asp and templates at http://www.va.gov/PROPATH/Templates.asp
27. One-VA Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.asp)
28. National Institute Standards and Technology (NIST) Special Publications (SP)
29. VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, October 15, 2014
30. VA Directive 6300, Records and Information Management, February 26, 2009
31. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
32. OMB Memorandum, “Transition to IPv6”, September 28, 2010
33. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
34. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014
35. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
36. 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
37. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
38. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
39. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011

40. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
41. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
42. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
43. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
44. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
45. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
46. 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)
47. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
48. 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)
49. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
50. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
51. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
52. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)
53. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
54. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
55. Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015
56. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
57. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
58. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
59. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

60. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
61. VA Directive 6071, Project Management Accountability System (PMAS), February 20, 2013
62. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems", (VAIQ# 7614373) July 9, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
63. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
64. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
65. "Veteran Focused Integration Process Guide 1.0", December, 2015, https://vaww.oit.va.gov/wp-content/uploads/2016/01/VIP_Guide_1_0_v14.pdf
66. "VIP Release Process Guide", Version 1.0, December 2015, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411
67. "POLARIS User Guide", Version 1.2, February 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412

3.0 SCOPE OF WORK

The Contractor shall support the development and implementation of the Department-wide VA Privacy Training program. This includes a professionalization program tailored to VA privacy professionals and officers and comprehensive and job-specific privacy training courses and guidance materials for all personnel that handle personal information; are directly involved in the administration of personal information or information technology systems; or, have significant information security or privacy responsibilities. Also, the Contractor shall develop and update web content for the Privacy intranet and internet sites and support all Privacy Steering Committee and National Privacy Officer Call activities.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The PoP shall be six months from the date of award, with four options for 12 months each.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in VA facilities located in Washington, District of Columbia (DC) at 1100 First Street, NE, Washington, DC 20002. Work may be performed at remote locations with prior approval of the Contracting Officer's Representative (COR).

4.3 TRAVEL

The Government does not anticipate travel under this effort.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN (BASE AND OPTION PERIODS)

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline, and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks, and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the contract. The Contractor shall update and maintain the VA Project Manager (PM) approved CPMP throughout the PoP.

Deliverable:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS (BASE AND OPTION PERIODS)

The Contractor shall provide the COR with Weekly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding week.

The Weekly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all Electronic and Information Technology (EIT) deliverables and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall conduct weekly teleconference progress meetings with the VA COR and PM to discuss work status.

Deliverable:

A. Weekly Progress Report

5.2 PRIVACY OFFICER PROFESSIONALIZATION PROGRAM (BASE AND OPTION PERIODS)

The Contractor shall conduct a comprehensive review and assessment of VA's Privacy Officer Professionalization Program. The review shall include a comprehensive department-wide review of the VA's existing privacy officer training programs, identify gaps in training design and update the existing framework (to include handbooks and procedures, definitions, concepts, applications of U.S. privacy laws and practices) and provide technical documentation used as supplemental guidance to existing policies.

The Contractor shall coordinate, develop, and prepare processes and plans that shall provide VA employees and its privacy professionals with tools and materials that are useful to day-to-day work activities demonstrating the knowledge, understanding, and skills to implement the privacy requirements for certified privacy professionals and those assigned privacy functions as a collateral duty. The Contractor shall develop all training and educational materials to improve an understanding of key privacy definitions and concepts from Federal laws, regulations, and guidance; VA directives, handbooks, and guidance; and Federal and industry best practices to further leverage privacy as being an essential discipline in VA. The core of privacy project and program development supports the Privacy Officer's professional understanding of their duties, and provides the foundation for them to pursue the other privacy certifications at the Federal level assisting them in their job and gaining a greater career value and mobility within established privacy communities of practice.

The Contractor shall provide communications for privacy steering committees, privacy groups, forums, and team meetings and develop and implement marketing strategies to communicate new requirements to and among VA offices and with other Federal agencies. The Contractor shall conduct assessments and identify all near-term and future planning training goals, document privacy framework, and provide the needed updates and mapping requirements. The Contractor shall develop technical documentation, procedures, and guides for end user support. The Contractor shall design, develop, and prepare implementation guidance to support VA privacy responsibilities as outlined in VA's Strategic Plan, Chief Information Officer (CIO)/OI&T implementation plans, and related privacy requirements that are identified in the OI&T Enterprise Strategic Plan.

5.2.1 GAP ASSESSEMENT REPORT (BASE AND OPTION PERIODS)

The Contractor shall review and conduct a comprehensive gap assessment of existing Privacy Service professionalization activities. The Contractor shall review and assess internal and external privacy professionalization (training) programs and learning resources to include the current VA-specific Privacy Officer Training, International Association of Privacy Professionals certification program, and other Federal privacy training efforts. The Contractor shall utilize the VA Privacy Framework, VA Strategic Plan, CIO/OI&T implementing plans, OI&T Enterprise Strategic Plan, VA directives and handbooks, and applicable compliance and audit reports in the assessment. The Contractor shall obtain and incorporate feedback from internal and external stakeholders (to include VA privacy and training professionals and Federal privacy and training experts) in the assessment report. The Contractor shall provide detailed recommendations on how to improve and enhance the current training program to include specific recommendations related to program design, training content and curriculum, and integration and adoption of the program within the VA Administrations and Staff Offices. The Contractor shall provide the Gap Assessment Report in a report format and update and maintain it throughout the PoP.

Deliverable:

A. Gap Assessment Report
B.

5.2.2 PRIVACY OFFICER PROFESSIONALIZATION FRAMEWORK (BASE AND OPTION PERIODS)

The Contractor shall update the Privacy Officer Professionalization Program Framework. This framework serves as the analytical basis for developing training materials associated with the VA's Privacy Officer's Professionalization Program. The framework shall be based on the latest Gap Assessment Report (Deliverable 5.2.1) in addition to applicable Federal laws, regulations, and guidance; VA directives, handbooks, and guidance; and Federal and industry best practices. The framework shall include a written multi-level training curriculum in the areas of privacy and information assurance (security); long and short-term program goals, objectives and performance metrics; and, an explanation of how VA Administration and Staff Office-specific privacy training and related educational efforts will integrate into VA's Privacy

Officer Professionalization Program. The Contractor shall provide the Updated Privacy Officer Professionalization Program Framework in a report format and Model(s) which shall include a graphical representation of the framework and its components. The Contractor shall update and maintain the Privacy Officer Professionalization Program Framework throughout the PoP.

Deliverable:

A. Updated Privacy Officer Professionalization Program Framework Report and Model(s)

5.2.3 IMPLEMENTATION PLAN (BASE AND OPTION PERIODS)

The Contractor shall design, develop, and prepare a Two-Year Phase-Level Implementation Plan to support the execution of the VA Privacy Officer Professionalization Program. The Contractor shall ensure this plan aligns with the VA privacy responsibilities outlined in VA's Strategic Plan, CIO/OI&T implementation plans and related privacy requirements outlined in the OI&T Enterprise Strategic Plan, VA policies, and Federal guidance. The Two-Year Phase-Level Implementation Plan shall include a program execution schedule, task list, task descriptions, and responsible office(s). The Contractor shall update and maintain the implementation plan throughout the PoP.

Deliverable:

A. Two-Year Phase-Level Implementation Plan

5.2.4 COMMUNICATIONS AND MEDIA SUPPORT (BASE AND OPTION PERIODS)

The Contractor shall support all Privacy Steering Committee and National Privacy Officer Call activities. The Contractor shall draft and send Communications to include agendas, documents, releases and important updates to VA components regarding the Privacy Steering Committee and National Privacy Officer Call activities. The Contractor shall engage, attend, record, coordinate, and assist in organizing events to increase awareness or knowledge of privacy activities. The Contractor shall support all communications, facilitation, and administrative needs for monthly Privacy Steering Committee and monthly National Privacy Officer Call meetings. This shall include coordination of meeting logistics, sending invites and other required communications to stakeholders, preparing and sending out meeting materials, documenting Meeting Minutes, and supporting the implementation of recommendations to improve meeting execution. The Contractor shall draft recommendations and control information input and output to assist in promotion of cooperative relationships between Privacy Steering Committee members and National Privacy Officer Call attendees, respectively, VA privacy office, and those who use privacy services. The Contractor shall use available VA communications and public relations products and coordinate all services with the established VA offices handling communicating information internal and external to VA. The Contractor shall provide all draft Communications releases and Meeting Minutes for review prior to release. The Contractor shall incorporate comments received and revise, restructure, reformat, and submit the final materials.

Deliverables:

A. Communications
B. Meeting Minutes

5.2.5 INDIVIDUAL DEVELOPMENT PLANS (OPTION PERIODS)

The Contractor shall develop and update existing Individual Development Plans (IDPs). The IDPs shall serve as an action plan to guide development and assess progress towards privacy career goals and training objectives. The Contractor shall develop two separate IDP action plans, one to identify those career goals, training objectives, and behavior indicators for the privacy professional and one to identify those career goals, training objectives, and behavior indicators for the employees who perform privacy officer functions as a collateral duty. VA has an existing IDP that can be used to develop the privacy professional IDP.

The Contractor shall incorporate all updates and comments received and provide the IDPs. The Contractor shall update and maintain the IDPs throughout the PoP. The Contractor shall work with IT Workforce Development and VA Learning University personnel and upload the latest IDPs for the Privacy Officer Professionalization Program in the VA Talent Management System (TMS).

Deliverable:

A. Individual Development Plans

5.2.6 PRIVACY OFFICER BODY OF KNOWLEDGE (OPTION PERIODS)

The Contractor shall design, develop and implement a one-stop Electronic Privacy Resource Center (EPRC) as an electronic privacy body of knowledge for the Privacy Officer Professionalization Program utilizing VA's Microsoft SharePoint platform. The Contractor shall document the EPRC design in a SharePoint Design Document. The Privacy Officer body of knowledge shall serve as an electronic comprehensive reference guide for Privacy Officers and shall reflect the competencies and content presented in the training curriculum. VA has an existing privacy SharePoint site that can be used to develop the EPRC. The Contractor shall provide guidance on the components and operational tasks in draft form to the VA COR and PM for review. The Contractor shall incorporate recommendations, revise, restructure, reformat, and submit (if required) and demonstrate new operational components until approved by the VA COR/PM. In addition, the Contractor shall also produce and record an online tutorial of the operational components of the resource center. The Contractor shall make the tutorial available to all users of the EPRC. The Contractor shall ensure that all final and updated versions of the PWS task documents (deliverables in Sections 5.2 through 5.5) are uploaded into the EPRC.

Deliverables:

A. SharePoint Design Document
B. Electronic Privacy Resource Center

5.2.7 MARKETING STRATEGY AND IMPLEMENTATION (OPTION PERIODS)

The Contractor shall implement, support, and maintain the Privacy Officer Professionalization Program. The Contractor shall develop a Marketing Strategy for the

Professionalization Program. The Marketing Strategy will serve as a plan to disseminate information to VA leadership, employees, and other key privacy stakeholders and obtain buy-in for the program. The Marketing Strategy shall include Job Aids and Associated Training Materials for VA Privacy Officers, supervisors, and employees to support their understanding of the components of the program and how to utilize the program to build and improve privacy-related competencies. The content of the Marketing Strategy shall include methods and metrics to monitor, assess, and evaluate the program's success with VA stakeholders. The Contractor shall support the implementation of this plan to include the communications support and the development of related Meeting Materials. The Contractor shall incorporate all updates and comments received and provide theMarketing Strategy to VA. The Contractor shall update and maintain the Marketing Strategy throughout the PoP.

Deliverables:

A. Marketing Strategy
B. Job Aids and Associated Training Materials
C. Meeting Materials

5.3 PRIVACY TRAINING DEVELOPMENT AND SUPPORT (OPTION PERIODS)

The Contractor shall develop training materials and support the implementation of the Privacy Officer Professionalization Program. Based on the latest version of the Two-Year Phase-Level Implementation Plan, the Contractor shall provide training support for the implementation of various teaching and learning methods. The Contractor shall outline innovative ways and methods that are flexible and adaptable to various environments to support those employees who have privacy responsibilities but are not identified as privacy professional. The Contractor shall develop and conduct (virtually) monthly Webinars and develop associated course content, Student Handbooks tailored to course content, and the related Instructor Training Guides that can be used to conduct face-to-face and virtual training sessions. The Contractor shall develop Webinars Training Materials to include course content, Frequently Asked Questions (FAQs), slide decks, transcripts, recordings of the training, and communications (Section 5.2.4 Communications and Media Support) and marketing strategies (Section 5.2.7 Marketing Strategy and Implementation) and speaker's notes. The Contractor shall provide support related to training development and support efforts to include coordination of webinar logistics, sending invites and other required communications to attendees, documenting meeting minutes and supporting the implementation of recommendation and lessons learned to improve the execution and quality of training.

Deliverables:

A. Student Handbooks
B. Instructor Training Guides
C. Webinars Training Materials

5.4 TECHNICAL DOCUMENTATION (OPTION PERIODS)

The Contractor shall develop Technical Documentation, Procedures, Papers, and Guides for end user support. The Contractor shall develop approximately one to two supporting documents monthly for privacy-related VA Directives and Handbooks (there are approximately 35 privacy-related VA Directives and Handbooks). These written documents will serve as supplemental guidance and instructions that can be readily used by employees needing interpretative guidance. The documents can be in the form of issue papers, quick notes, and other technical interpretive instructions that can be used to support the day-to-day work requirements, duties, and functions of VA privacy officers and those employees who perform privacy functions as a collateral duty. The Contractor shall review newly released, published policies and guidance and provide simplified interpretive instructions applicable to the user in carrying out their duties. The Contractor shall incorporate updates as the privacy related VA directives and handbooks change.

Deliverable:

A. Technical Documentation, Procedures, Papers, and Guides

5.5 PRIVACY INTRANET/INTERNET CONTENT DEVELOPMENT (OPTION PERIODS)

The Contractor shall develop new and update existing content for Office of Privacy and Records Management Intranet and Internet websites. There are approximately 153 web pages and it is anticipated that 20 percent of the web pages require updates monthly. The Contractor shall proofread and edit new content and existing website content submitted by VA in order to ensure accuracy of information and application of plain language principles. The Contractor shall ensure the tone, voice, and messaging of all content developed and updated is consistent and aligned with VA and OI&T's mission and values (reference http://www.va.gov/about_va/mission.asp and http://www.oit.va.gov/), quality expectations (reference Section 2.0 Applicable Documents #10. VA Directive and Handbook 6102), and brand identity (style guides). The Contractor shall utilize VA directives, handbooks, Federal laws and regulations, surveys of users or trainees or other sources to develop the Web content. The Contractor shall conduct research of academia sources, other industry privacy programs, interest groups, expert and knowledge based sources, and state and local entities to provide users and stakeholders with a comprehensive knowledge of current and active privacy issues, policies, and documents from reliable and approved sources. The Contractor shall review all Federal guidance and posted relevant information and content consistent with existing laws and policies as prescribed by privacy laws and regulations. The content shall be written in plain language, accurate, from updated sources, and aligned with VA policies and procedures for Web development for VA websites. The Contractor shall incorporate all updates and comments received and provide the electronic drafts to the VA COR and PM for review. The Contractor shall revise, restructure, reformat, and submit the updated draft materials via email until approved by the VA COR/PM. The Contractor shall provide the electronic final documents via email.

Deliverable:

A. New and Updated Content for Privacy Intranet/Internet

5.6 OPTION PERIOD ONE

If Option Period One is exercised by VA, the Contractor shall perform all tasks within the Sections and Sub-sections of 5.1, 5.2, 5.3, 5.4, and 5.5.

5.7 OPTION PERIOD TWO

If Option Period Two is exercised by VA, the Contractor shall perform all tasks within the Sections and Sub-sections of 5.1, 5.2, 5.3, 5.4, and 5.5.

5.8 OPTION PERIOD THREE

If Option Period Three is exercised by VA, the Contractor shall perform all tasks within the Sections and Sub-sections of 5.1, 5.2, 5.3, 5.4, and 5.5.

5.9 OPTION PERIOD FOUR

If Option Period Four is exercised by VA, the Contractor shall perform all tasks within the Sections and Sub-sections of 5.1, 5.2, 5.3, 5.4, and 5.5.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-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. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, 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 Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf), M-05-24 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf), M-11-11 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance with the USGv6: A Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm) and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html), shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

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 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the

VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the 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) specific to the particular client operating system being used.

The Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project. It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their VIP and PMAS-compliant work.

6.2 SECURITY AND PRIVACY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	Tier 1 / National Agency Check with Written Inquiries (NACI) A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Moderate / Tier 2	Tier 2 / Moderate Background Investigation (MBI) A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	Tier 4 / Background Investigation (BI) A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	☒	☐	☐
5.2	☒	☐	☐
5.3	☒	☐	☐
5.4	☒	☐	☐
5.5	☒	☐	☐

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.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. 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.

b. The Contractor shall bear the expense of obtaining background investigations.
c. 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 ProPath template. 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.

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306
        b) VA Form 0710
        c) DVA Memorandum – Electronic Fingerprints
f. 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).
g. 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 eQIP).
h. 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.

i. 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) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." 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 the Office of Personnel Management (OPM).
j. 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.
k. 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.
l. 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:

A. Contractor Staff Roster

6.3 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: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance

A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

The COR will utilize a 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.

6.5 FACILITY/RESOURCE PROVISIONS

The Government will provide office space, a desk, 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. The Contractor shall provide its own desktop computer systems or laptops, and associated peripherals (this includes all IT equipment and all consumables) as described in Section 6.5.1. The Government

will provide all applicable software applications and access to VA documents and manuals needed by the Contractor to perform the work.

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 will provide remote access to VA specific systems/network as required for execution of the task(s) 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, ProPath, 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, document 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.

In accordance with the VA Media Sanitization policy, if the Contractor is utilizing its own computer equipment, then all hard drives shall be delivered to VA for destruction at the conclusion of the contract or upon demand by VA, whichever comes first.

6.5.1 CONTRACTOR ACQUIRED PROPERTY

The Contractor shall procure and provide its own laptops or desktop computer systems and associated peripherals (this includes all IT equipment and all consumables), which will not be reimbursed as a direct cost to this effort. The minimum configuration of the computer is shown in the following table.

General Requirement		**Minimum Requirements**	
Req #	**Parameter**	**Attribute**	**Government Value**
1	Processor	Minimum Speed (Ghz)	2.5 Ghz
2		Trusted Platform Module (TPM) Support: Desktop and Mobile Architecture for System Hardware (DASH) 1.1 or equivalent to include either Intel's vPro or AMD's DASH 1.1 compliant	YES
3		Minimum Number of Cores	4
4		Processor Cache	4 Mb
5	Memory	Minimum Speed (Mhz)	1333 Minimum
6		Minimum (GB)	16
7	Display / Graphics	Screen Size, Minimum (inches)	14
8		Minimum Resolution (pixels, h x v)	1366X768
9		Acceptable aspect ratios	16:9 or 16:10
10		Integrated graphics acceptable	YES
11		Dedicated video memory required	NO
12		Shared video memory accepted	YES
13		Graphics memory, minimum	512 MB
14		Dual-head/link support	YES
15	Networking	Wireless	802.11g/n
16		Network Interface Controller (NIC) speed, minimum (gbps)	1 GB
17		Support for FIPS 140-2 and IEEE 802.11	YES
18	Monitor	Privacy Filter	YES
19	Speaker	Internal	YES
20	Keyboard	Smart keyboard	YES
21		USB connect capable	YES

22	Integrated Features	Hot buttons/hot key sequence to permit enabling/disabling of wireless networks, speaker, external monitor	YES
23		Hot button/hot key sequence to permit enabling/disabling of touchpad	YES
24	Mouse	Multi-touch touchpad/pointer stick	YES
25	Keyboard Illumination	Backlit or other integrated keyboard lighting system	YES
27	USB 2.0	Number of ports, minimum	3
28	Primary Hard Drive	Interface	SATA
29		Capacity, minimum (GB)	250
30		RPM, minimum	7200
31		Non Self-encrypting Hard Drive	YES
32	Optical Device	8X DVD +/- RW	YES (Internal or external)
33	Battery/AC Adapter	Cells, minimum	cell count required to support a minimum run time, on battery, of 5 hours
34		EPA Energy Star rated	YES
35	Security	Smart card reader (Internal)	YES
36	Operating Systems Supported	Windows 7, Enterprise Ed.	YES
37		MS Certified for Win 7 (32 and 64 bit)	YES
38	Docking Station	Interface for port replicator	YES
39		* VA requires 2 video outputs, either one of each or one VGA and multiple on the Digital on the larger docks is acceptable.	YES

The Contractor shall deliver the computers that meet the above specified minimum requirements to VA within 30 days of award. The Contractor shall provide the COR with the make and model of the intended computer to be provided prior to procurement. The COR shall have up to five business days to review and approve the make and model. These five days shall not count towards the 30 days the Contractor has to provide VA with computers. All computers imaged by VA shall become VA property at the end of the period of performance. VA may provide the Contractor with computers during the initiation period of the contract for the purposes of not impeding Contractor accomplishments while the computers are provided, imaged, inventoried, and issued to the Contractor staff.

The Contractor shall provide VA with the computers for imaging prior to use on the VA network. VA will maintain full administrative permissions to the computers. VA will approve Contractor elevated permissions beyond regular user permissions on a case by case basis.

No third party applications shall be loaded on these computers. The Contractor shall coordinate through the COR to ensure all equipment is properly processed within VA inventory protocols. The Contractor is required to provide a staff roster outlining assignment of computers and serial number identification for the purpose of tracking the computer with the VA image in its property inventory system to the COR.

The computers shall be scanned by the VA facility and provide a Property pass, which permits authorization of the computer for use at that VA facility. Under circumstances of Contractor reassignment of resources, the computer may be transferred to the new Contractor employee, with a re-scan and a new Property pass. The staff roster must remain updated accordingly and provided to the COR. If the computer is no longer in use, the COR shall be notified in order to take possession of the computer.

While in use, the computer will remain in the local facility's inventory until the end of the PoP.

VA will provide access to VA specific systems/network access as required for execution of the tasks via remote access technology, if applicable.

The Contractor shall utilize Government-provided software development and test accounts, document 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 in accordance with (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 ATOs for all systems/Local Area Networks (LAN's) accessed while performing the tasks detailed in this PWS.

6.6 GOVERNMENT FURNISHED PROPERTY

In limited instances, as approved on a case-by-case basis by the COR, Government Furnished Equipment laptops may be provided to address security, access, testing, or other instances where Contractor furnished equipment is limited. Contractor furnishing the equipment shall remain as precedence over this method.

6.7 SHIPMENT OF HARDWARE OR EQUIPMENT

Inspection: Destination
Acceptance: Destination
Free on Board (FOB): Destination

Ship To and Mark For:

	Primary		Alternate
Name:	Lori E. Russell	Name:	Kimberly Hollingsworth
Address:	810 Vermont Avenue	Address:	810 Vermont Avenue

	Primary		Alternate
	(005R1A) Washington, DC 20002		(005R1A) Washington, DC 20002
Voice:	(202) 632-7499	Voice:	(202) 632-8414
Email:	Lori.Russell@va.gov	Email:	Kimberly.Hollingsworth@va.gov

Special Shipping Instructions:

Prior to shipping, Contractor shall notify Site POCs, by phone followed by email, of all incoming deliveries including line-by-line details for review of requirements. Contractor shall not make any changes to the delivery schedule at the request of Site POC.

Contractors shall coordinate deliveries with Site POCs before shipment of laptop(s) to ensure sites have adequate storage space.

All shipments, either single or multiple container deliveries, shall bear the VA IFCAP Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA IFCAP PO number shall indicate total number of containers for the complete shipment (e.g. “Package 1 of 2”), clearly readable on manifests and external shipping labels.

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: _____ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))
Project Description: (e.g. Privacy Professionalization Training Program)

Total number of Containers: Package ___ of ___. (e.g., Package 1 of 3)

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

A1.0 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 certification and accreditation.

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, 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), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS 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.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-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.

A2.1. 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): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

A3.1. Section 508 – Electronic and Information Technology (EIT) Standards

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards and http://www.section508.gov/content/learn/standards. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

- ☐ § 1194.21 Software applications and operating systems
- ☒ § 1194.22 Web-based intranet and internet information and applications
- ☐ § 1194.23 Telecommunications products
- ☒ § 1194.24 Video and multimedia products
- ☐ § 1194.25 Self contained, closed products

☐ § 1194.26 Desktop and portable computers
☒ § 1194.31 Functional Performance Criteria
☒ § 1194.41 Information, Documentation, and Support

A3.2. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

A3.3. Compatibility with Assistive Technology

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

A3.4. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at http://www.section508.va.gov/section508/Resources.asp.

Deliverables:

A. Final Section 508 Compliance Test Results

A4.0 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.

A5.0 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 to Protected 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:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. 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.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.
8. 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.
9. 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.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements . The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives

2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

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

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE*, *VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. 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.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. 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).

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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 Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. 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.

9. 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.

10. 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.

11. 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.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service 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.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Not applicable

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

Not applicable

B6. SECURITY INCIDENT INVESTIGATION

a. 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.

b. 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.

c. 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.

d. 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.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

a. 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.

b. 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.

c. 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:

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3) Number of individuals affected or potentially affected;

4) Names of individuals or groups affected or potentially affected;

5) 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;

6) Amount of time the data has been out of VA control;

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

8) Known misuses of data containing sensitive personal information, if any;

9) Assessment of the potential harm to the affected individuals;

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and

11) 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.

d. 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.

B8. SECURITY CONTROLS COMPLIANCE TESTING

Not applicable

B9. TRAINING

a. 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:

1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.

2) 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.]

b. 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 1 week of the initiation of the contract and annually thereafter, as required.

c. 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.

Notes to the Contracting Officer

(This section to be removed from PWS before solicitation)

TYPE OF CONTRACT(S)

(Choose the type of contract that applies by selecting the checkbox, or, if a hybrid, select all that apply)

- ☒ Firm Fixed Price
- ☐ Cost Reimbursement
- ☐ Labor-Hour
- ☐ Time-and-Materials
- ☐ Other _____

SCHEDULE FOR DELIVERABLES

Note: Days used in the table below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

(Indicate delivery dates in terms of number of days after (DAC) award. If a deliverable is requested in draft, and then final submission-the deliverable line item is complete, no further update can be requested. Continued reporting should be a separate line item. A Mark For and Ship To address (including Inspection/Acceptance requirements) must be provided for all hardware deliverables. Electronic submission of S/W or paper deliverables should be the norm unless otherwise stated. Email addresses must be provided. Although email addresses are provided below for all POC's, table must be clear as to who receives the deliverables.)

Task	Deliverable ID	Deliverable Description
0	A	**Contractor Project Management Plan (Base, Option Year 1, 2, 3 and 4)** Due 30 days after contract award and updated monthly thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	A	**Weekly Progress Reports (Base, Option Year 1, 2, 3 and 4)** Due every Thursday after contract award throughout the period of performance (PoP). Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
0	A	**Gap Assessment Report** Draft due 150 days after contract award and updated quarterly throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	A	**Updated Privacy Officer Professionalization Program Framework Report and Model(s) (Option Year 1, 2, 3 and 4)** Due 30 days after initial submission of the Gap Assessment Reportand updated quarterly throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	A	**Two-Year Phase-Level Implementation Plan (Option Year 1, 2, 3 and 4)** Final due 30 days after initial submission of the Gap Assessment Report and updated quarterly throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	A	**Communications (Base and Option Years 1, 2, 3 and 4)** Draft due the third Tuesday of each month after contract award and as required throughout the PoP; Final due five days after receipt of VA comments. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	B	**Meeting Minutes** Draft due five business days after each meeting; Final due five days after receipt of VA comments. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	A	**Individual Development Plans (Option Year 1, 2, 3 and 4)** Due 90 days after exercising Option Period 1 and updated monthly throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	A	**SharePoint Design Document (Option Year 1)** Due 90 days after exercising Option Period 1. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	B	**Electronic Privacy Resource Center (Option Year 1, 2, 3 and 4)** Due 60 days after Task 5.2.6 SharePoint Design Document is accepted by VA and updated weekly thereafter throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
0	A	**Marketing Strategy (Option Years 1, 2, 3 and 4)** Due 120 days after exercising Option Period 1 and updated quarterly throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	B	**Job Aids and Associated Training Materials (Option Years 1, 2, 3 and 4)** Due 30 days after the acceptance by VA of the initial submission of the Marketing Strategy and updated as required throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	C	**Meeting Materials (Option Years 1, 2, 3 and 4)** Due 7 days prior to any scheduled meeting and updated as required throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	A	**Student Handbooks (Option Year 1, 2, 3 and 4)** Due 15 days prior to the scheduled webinar(s) and updated as required throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	B	**Instructor Training Guides (Option Year 1, 2, 3 and 4)** Due 15 days prior to the scheduled webinar(s) and updated as required throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	C	**Webinars Training Materials (Option Year 1, 2, 3, and 4)** Due 10 days prior to the scheduled webinar(s) and updated as required throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
0	A	**Technical Documentation, Procedures, Papers, and Guides (Option Year 1, 2, 3 and 4)** First set of (one to two) documents supporting a VA directive or handbook due 30 days after initial submission of the IDPs and additional sets of documents due every month thereafter until all are completed; all documents shall be updated monthly as the directives and handbooks change. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5	A	**New and Updated Content for Privacy Intranet/Internet (Option Years 1, 2, 3 and 4)** Due 30 days after exercising Option Period 1 and every month thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
6.2.2	A	**Contractor Staff Roster** Due three days after contract award and updated throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
A3.4	A	**Final Section 508 Compliance Test Results** Due upon delivery of each deliverable. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

POINTS OF CONTACT

(Identify POCs for this effort for distribution of deliverables)

VA Program Manager:
Name: Lori Russell
Address: 1100 1st ST NE Washington, DC 20002
Voice: (202) 632-7499
Email: lori.russell@va.gov

Contracting Officer's Representative:
Name: Lori Russell
Address: 1100 1st ST NE, Washington DC 20002
Voice: (202) 632-7499
Email: lori.russell@va.gov

Contracting Officer:
Name: Debra Clayton
Address: 23 Christopher Way, Eatontown, NJ 07724
Voice: (732) 795-1015
Email: Debra.Clayton2@va.gov

ADDITIONAL ITEMS
SPECIAL INSTRUCTIONS/REMARKS

SPECIAL CLAUSES, ETC. TO BE INCLUDED IN THE SOLICITATION

(Choose Special Clause(s), etc., if applicable, by selecting the checkbox and modifying as necessary)

☐ Transition clause required? (Insert FAR clause, Continuity of Services, FAR 52.237-3)

☐ Intellectual Property/Technical Data Rights Clause required?
☐ OCI Clause required?
☐ Government Furnished Material/Equipment: CO should add a special clause to the contract citing the Title of the material/equipment, Identifier (Serial Number), Quantity, Purpose, and Date required by Contractor.
☐ BAA required **for an OI&T Contract on behalf of VHA?**

If the answer to Question 4 of the Security Checklist is a "yes" and the Contractor will provide a service, function, or activity **to OI&T, on behalf of VHA**, then it must be determined if protected health information (PHI) is disclosed or accessed, if so, a BAA is required. (The "Decision Tree for Business Associate Agreements" can be used by the requiring activity (with help from their OI&T Privacy Officer [Garnett Best/Rita Grewal] if needed) to determine if a BAA is required, see VHA Handbook 1605.05, Business Associate Agreements, Appendix A, (http://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3027)).

If it is determined that a BAA is required, the CO must, in eCMS, insert the BAA Document below as a "Clause" into Section D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS of the solicitation manually by performing the following instructions:

1. Open the below embedded "VA Subcontractor BAA with OI&T" Template file, insert a brief description of the services involved in the effort within the "Scope" Section, and the VA Program Manager information in the VA Signature block at the end of the form, replacing the **<RED TEXT>** within the template. Once complete, save the "Business Associate Agreement" file to your computer.
2. Create a solicitation document in eCMS
3. Click on the 'Content Manager' link and highlight Section D, Contract Documents, Exhibits, or Attachments.
4. Click on the "Insert" tab in the top left corner to insert an "External File" after the selected clause.
5. Upload the "Business Associate Agreement" file you saved to your computer.

The Business Associate Agreement file is the text of the eCMS VHA Clause 1605.05, tailored for the individual effort, and is essentially the Business Associate Agreement language itself, and needs to be seen by the bidders in the solicitation (if a BAA is required).

VA Subcontractor BAA with OI&T

☐ BAA required **for a Veterans Health Administration (VHA) Contract?**

If the answer to Question 4 of the Security Checklist is a "yes" and the Contractor will provide a service, function, or activity **to VHA or on behalf of VHA**, then it must be determined if protected health information (PHI) is disclosed or accessed and if a BAA is required. The "Decision Tree for Business Associate Agreements" should be used by the requiring activity (with help from their Privacy Officer if needed [the VHA Privacy Service -Stephania Griffin/ Andrea Wilson can advise] to determine if a BAA is required, see VHA Handbook 1605.05, Business Associate Agreements, Appendix A, (http://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3027). If it is determined that a BAA is required, the CO must, in eCMS, insert the VHA clause 1605.05 into Section D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS of the solicitation. This can be accomplished by performing the following in eCMS:

1. Insert the 1605.05 clause through the Clause Library (or by answering "Yes, access to PHI is necessary and a BAA is required," to the Dialog Session question that asks, "Will the contractor require access to Protected Health Information to perform the functions or services required in this acquisition?")
2. After inserting the clause, double-click on the clause and use the "Fill-in" field in the "Scope" section to add a description of the service(s) being performed.
3. In the MS Word version of your solicitation, manually input "Contractor" throughout the document where it has been blanked out. The embedded file below shows the locations of the "blanks" (showing codes from eCMS in red instead of "blanks") to assist you in adding the missing information properly. The eCMS VHA Clause 1605.05 text is the BAA itself and needs to be seen by the bidders if a BAA is required. **Note:** The actual Contractor's Name will automatically populate in the appropriate sections of the BAA clause from the Data Values upon creation of the award document.

VHA 1605.05
BUSINESS ASSOCIAT

☐ Other _____
☐ Other _____

FOR TAC USE ONLY---SECURITY RELATED GUIDANCE

☒ ***(Always Checked for Services)*** Addendum B Security Requirement guidance to CO within Addendum B, Section B9 Training, Para. a) Sub Para. 2,

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 contracting officer 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.]***

☒ ***(Always Checked for Services)*** Contractor Rules of Behavior-Appendix D in Handbook 6500.6 – ***(CO to add to solicitation, CO to ensure Contractor signs and acknowledges (electronically through VA Privacy and Information Security Awareness and Rules of Behavior course TMS #10176) understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix D relating to access to VA information and information systems.)***

ADDITIONAL NOTES TO PREPARER

1. ***Run Spell Check and Grammar Check in document for final review. Simple and easy tool to utilize and benefit from.***
2. ***When listing/itemizing points, keep the outline consistent (use appropriate number or letter, versus a bullet).***
3. ***If deliverables need to be submitted in draft form, timeframes must be stated. Reference example provided in the table above.***
4. ***Other submissions may be required but not held to draft/comment/final submissions. For example, monthly status reports are due 5 days after the conclusion of the reporting period (end of month).***
5. ***Customer must identify which deliverables continue if option years are exercised. Not all deliverables would necessarily repeat. Certain deliverables are final in the base year.***
6. ***Do not put due dates in "Deliverables:" section of task, rather include timeframes/due dates in "Schedule for Deliverables" table above. Also ensure customer deliverables are detailed in the narrative of the task to include format and content requirements.***
7. ***Ensure deliverables in tasks match deliverables in table.***
8. ***If VIP applies, ensure deliverables are delivered in 3 month increments or less within an agile framework.***
9. ***Deliverable due dates should be in terms of number of days after award or based on an event.***
10. ***If for some reason the deliverable must be submitted in hard copy or on CD, be sure to specify the requirement within the line item. Also, in this case identify number of copies and mailing address.***

11. ***Each deliverable line item must cite inspection and acceptance criteria; Inspection: Origin or Destination; Acceptance: Origin or Destination (most likely destination on both).***
12. ***Update the Table of Contents by hitting F9.***