



PERFORMANCE WORK STATEMENT (PWS) DEPARTMENT OF VETERANS AFFAIRS

Office of Procurement, Acquisition and Logistics (OPAL)

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services**

**Date: June 21, 2018
TAC-18-50524**

PWS Version Number: 2.0

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

Contents

1.0	BACKGROUND.....	4
2.0	APPLICABLE DOCUMENTS.....	5
3.0	SCOPE OF WORK.....	8
4.0	PERFORMANCE DETAILS.....	9
4.1	PERFORMANCE PERIOD.....	9
4.2	PLACE OF PERFORMANCE.....	9
4.3	TRAVEL.....	10
5.0	SPECIFIC TASKS AND DELIVERABLES.....	11
5.1	PROJECT MANAGEMENT.....	12
5.1.1	TECHNICAL KICKOFF MEETING.....	12
5.1.2	PROGRAM RELATED MEETINGS.....	12
5.1.3	REPORTING REQUIREMENTS.....	12
5.1.4	KEY PERSONNEL.....	13
5.2	SUPPORT TO OPAL CONTRACTING TEAMS.....	13
5.2.1	OPAL eCMS HELP DESK SUPPORT.....	13
5.2.2	ENTERPRISE ACQUISITION SYSTEM (EAS) REFERRALS.....	14
5.2.3	OPAL eCMS CONTRACTING SYSTEM SUPPORT.....	14
5.2.4	OPAL eCMS APPLICATION SUPPORT.....	14
5.2.5	BEST PRACTICES AND STANDARD OPERATING PROCEDURES (SOPs).....	15
5.3	REPORTING SUPPORT.....	15
5.4	TRAINING SUPPORT.....	17
5.5	ADDITIONAL LOCATIONS TIER 1 ECMS SUPPORT SERVICES (OPTIONAL TASK ONE).....	18
5.6	DASHBOARD REPORTS (OPTIONAL TASK TWO).....	18
5.7	OPTION PERIODS ONE - FOUR.....	18
6.0	GENERAL REQUIREMENTS.....	19
6.1	ENTERPRISE AND IT FRAMEWORK.....	19
6.1.1	ONE-VA TECHNICAL REFERENCE MODEL.....	19
6.1.2	FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM).....	19
6.1.3	INTERNET PROTOCOL VERSION 6 (IPV6).....	21
6.1.4	TRUSTED INTERNET CONNECTION (TIC).....	21
6.1.5	STANDARD COMPUTER CONFIGURATION.....	21
6.1.6	VETERAN FOCUSED INTEGRATION PROCESS (VIP).....	22
6.1.7	PROCESS ASSETT LIBRARY (PAL).....	22
6.2	SECURITY AND PRIVACY REQUIREMENTS.....	22
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S).....	22
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS.....	23
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES.....	25
6.4	PERFORMANCE METRICS.....	25

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

6.5	FACILITY/RESOURCE PROVISIONS.....	29
6.6	GOVERNMENT FURNISHED PROPERTY	30
6.7	ORGANIZATIONAL CONFLICT OF INTEREST	31
ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED		36
ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.....		43

DRAFT

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

1.0 BACKGROUND

The Department of Veterans Affairs (VA) Office of Procurement, Acquisition and Logistics (OPAL) primary mission is to provide contracting support to VA Central Office and the entire VA enterprise. The use of the Electronic Contract Management System (eCMS) is a mandatory requirement for all acquisitions over \$3,000.00. Based on the mandatory requirement for the use of eCMS, OPAL has a requirement for Tier 1 eCMS support services to assist the acquisition workforce in the use of eCMS.

Based on the use of eCMS, all OPAL organizations require support services for a broad range of eCMS actions that shall include training and user support, application administration, and reporting. eCMS links to all Integrated Acquisition Environment (IAE) systems: Federal Procurement Data System (FPDS), Office of Research Compliance and Assurance (ORCA), General Service Administration (GSA) eBuy, Federal Business Opportunities (FBO), and the contractor is expected to reconcile data between eCMS and Virtual Office of Acquisition (VOA), /Forecast of Opportunities and Requirements Center for Excellence (FORCE).

In performance of the tasks in this Performance Work Statement (PWS), the Contractor shall use and have expertise in the following technologies and applications:

- a. eCMS
 1. Automated Acquisition Management Solution (AAMS) Contracting Module
 2. Electronic Contracting Officer Representative File (eCOR)
 3. Forecast of Opportunities and Requirements Center for Excellence (FORCE)
 4. Planning Module
 5. Evaluate Solicitations Module
 6. Vendor Portal
 7. Ordering Officer Designation Module (OOD)
 8. Task Order Management System (TOMS)
- b. Microsoft SharePoint 2010, 2013 or later
- c. MicroStrategy
- d. General Services Administration (GSA) eBuy
- e. Federal Procurement Data System (FPDS)
- f. Forecast of Opportunities (FCO)
- g. National Acquisition Center Contract Management (NAC CM)
- h. Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP)
- i. System for Award Management (SAM)
- j. FedBizOpps (FBO)
- k. Virtual Office of Acquisition (VOA)
- l. VOA Adhoc Reporting Tool
- m. VOA Acquisition Task Order Management System (ATOMS)
- n. SQL Server 2012

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

1. Reporting tools including SQL Server Reporting Services (SSRS)

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this PWS, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541-3549, "Federal Information Security Management Act (FISMA) of 2002"
2. "Federal Information Security Modernization Act of 2014"
3. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
4. FIPS Pub 199. Standards for Security Categorization of Federal Information and Information Systems, February 2004
5. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2016
6. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
7. 10 U.S.C. § 2224, "Defense Information Assurance Program"
8. 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
9. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
10. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
11. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
12. VA Directive 0710, "Personnel Security and Suitability Program," June 4, 2010, <http://www.va.gov/vapubs/>
13. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
14. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
15. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
16. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
17. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
18. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
19. 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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

20. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
21. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
22. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
23. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
24. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)," July 28, 2016
25. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
26. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
27. VA Handbook 6500.6, "Contract Security," March 12, 2010
28. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
29. OI&T Process Asset Library (PAL), <https://www.va.gov/process/> . Reference Process Maps at <https://www.va.gov/process/maps.asp> and Artifact templates at <https://www.va.gov/process/artifacts.asp>
30. One-VA Technical Reference Model (TRM) (reference at <https://www.va.gov/trm/TRMHomePage.aspx>)
31. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
32. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
33. VA Handbook 6510, "VA Identity and Access Management", January 15, 2016
34. VA Directive 6300, Records and Information Management, February 26, 2009
35. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
36. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, June 10, 2014
37. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
38. OMB Memorandum, "Transition to IPv6", September 28, 2010
39. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
40. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
41. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
42. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

43. 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
44. 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
45. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
46. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
47. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
48. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
49. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, Digital Identity Guidelines, June 2017
50. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
51. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
52. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
53. 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>)
54. 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>)
55. VA Memorandum “Mandate to meet PIV Requirements for New and Existing Systems” (VAIQ# 7712300), June 30, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846>
56. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
57. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
58. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
59. 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>)

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

60. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
61. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
62. Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015
63. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
64. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
65. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
66. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014,
<https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
67. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
68. 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>
69. 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>
70. 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>
71. “Veteran Focused Integration Process (VIP) Guide 2.0”, May 2017,
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
72. “VIP Release Process Guide”, Version 1.4, May 2016,
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
73. “POLARIS User Guide”, Version 1.2, February 2016,
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>
74. VA Memorandum “Use of Personal Email (VAIQ #7581492)”, April 24, 2015,
<https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
75. VA Memorandum “Updated VA Information Security Rules of Behavior (VAIQ #7823189)”, September, 15, 2017,
<https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
76. Attachment A- Sample Dashboard Report

3.0 SCOPE OF WORK

The Contractor shall provide all management, staff, and supplies for eCMS Help Desk support. The Contractor shall provide on-site support at each OPAL office referenced in Paragraph 4.2.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) shall be 12 months from date of award, with four (4) 12-month option periods. If exercised, Optional Task One under PWS Section 5.5 shall have a PoP up to 12 months in each period of performance. If exercised, Optional Task Two under PWS Section 5.6 shall have a PoP up to 12 months in each period of performance.

Any work at the Government site shall not take place on Federal holidays or weekends (but may require off-hour work due to network loading or other disruptions that could occur) 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

The Contractor shall provide on-site support during the core hours of 8 AM to 5 PM Local Time.

Tasks under this PWS shall be performed on-site by a Senior Business Analyst listed in Paragraph 5.1.4 in the VA OPAL facility listed below:

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

OPAL Facility	Address	Contact Information (site POCs)
Technology Acquisition Center (TAC-NJ)	23 Christopher Way Eatontown, NJ 07724	Attention: Eric Boorum Phone 732-795-1146 Email: Eric.boorum@va.gov

In support of Optional Tasks One and Two, if exercised, the tasks under this PWS shall be performed by a Senior Business Analyst listed in Paragraph 5.1.4 for the VA OPAL facilities listed below:

On-Site Support

OPAL Facility	Address	Contact Information (site POCs)
Technology Acquisition Center (TAC-A)	1701 Directors Blvd Austin, TX 78744	Attention: Jeffrey Bishop Phone 512-981-4414 Email: Jeffrey.bishop2@va.gov
Strategic Acquisition Center (SAC)	10300 Spotsylvania Avenue, Suite 400 Fredericksburg, VA 22408	Attention: Adam Spacht Phone 202-422-1923 Email: Adam.Spacht@va.gov
Strategic Acquisition Center – Frederick (SAC-F)	321 Ballenger Center Drive, Suite 125 Frederick, MD 21703	Attention: Adam Spacht Phone 202-422-1923 Email: Adam.Spacht@va.gov
National Acquisition Center (NAC)	1st Ave Bldg 37 Hines, IL 60141	Attention: Raymond Schraeder Phone 708-786-5211 Email: Raymond.schraeder@va.gov
National Acquisition Center (NAC) Commodities and Services Acquisition Service and Denver Logistics Center (DLC)	555 Corporate Circle Golden, CO 80401-5621	Attention: Raymond Schraeder Phone 708-786-5211 Email: Raymond.schraeder@va.gov

Remote Support

OPAL Facility	Address	Contact Information (site POCs)
OPAL Front Office and Logistics Support Services (LSS)	810 Vermont Ave, NW Washington, DC 20420	Attention: Kristine Stout Phone 202-382-2734 Email: Kristine.stout@va.gov

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences throughout the PoP. Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government. All travel must be approved prior to the trip by the Contracting Officer's Representative (COR).

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

The total number of trips in support of the Data Manager attending the program related meetings referenced in PWS Section 5.1.2 for this effort is estimated to be one (1) trip per year for a duration of two days. The trip destination will be at the following location:

OPAL Facility	Address
Technology Acquisition Center (TAC-NJ)	23 Christopher Way Eatontown, NJ 07724

If Optional Task One is exercised, the total number of trips in support of the Data Manager attending the program related meetings referenced in PWS Section 5.1.2 for this effort is estimated to be one (1) trip per year per site, for a duration of two days. The trip destination will be at the following locations:

OPAL Facility	Address
Technology Acquisition Center (TAC-A)	1701 Directors Blvd Austin, TX 78744
Strategic Acquisition Center (SAC)	10300 Spotsylvania Avenue, Suite 400 Fredericksburg, VA 22408
Strategic Acquisition Center – Frederick (SAC-F)	321 Ballenger Center Drive, Suite 125 Frederick, MD 21703
National Acquisition Center (NAC)	1st Ave Bldg 37 Hines, IL 60141
National Acquisition Center (NAC) Commodities and Services Acquisition Service and Denver Logistics Center (DLC)	555 Corporate Circle Golden, CO 80401-5621
OPAL Front Office and Logistics Support Services (LSS)	810 Vermont Ave, NW Washington, DC 20420

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall sustain VA's eCMS production environment.

There are approximately 460 VA OPAL employees/contractors that currently use eCMS. In FY17 OPAL awarded 17,470 actions. VA is assuming a 10% increase in actions and users per year, and increased use of telework.

Table 1.0 FY17 OPAL Actions

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

Office	Actions	Tickets	Users
TAC-NJ	3074	4098	125
TAC-Austin	1245	3430	25
NAC-IL	8902	6000 (est)	159
NAC-CO	1313	3000 (est)	30
FO/LSS	353	647	25
SAC	1044	1135	52
SAC-F	1539	3011	44
Total	17,470	21,321	460

5.1 PROJECT MANAGEMENT

5.1.1 TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within ten (10) days after TO award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least five (5) calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three (3) calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PM's.

5.1.2 PROGRAM RELATED MEETINGS

Program related meetings shall occur once per year at each site being supported. The Contractor shall coordinate the date of the meeting with the COR. The Contractor's Data Manager and the facility POC shall analyze lessons learned and review training materials. The Contractor shall address any concerns such as reoccurring errors that may require new policies to be put in place to address these concerns.

5.1.3 REPORTING REQUIREMENTS

The Contractor shall include all Help Desk activities in a Help Desk Monthly Summary Log to be reviewable by the COR in real time and submitted monthly in a VA approved electronic format. A monthly, quarterly and yearly roll-up of all help desk activities shall include all issues separated by location to include open, closed, escalated, resolution times, requestor name and contact information, description, priority, and current status. For the resolution times, two times need to be tracked. One is for how long the entire ticket took to be resolved, that would be the total amount of resolution time. The second resolution time would be how long it took this OPAL support group to personally resolve or escalate the ticket to the next support tier.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

Deliverables:

A. Help Desk Monthly Summary Log

5.1.4 KEY PERSONNEL

The Contractor shall provide the following key personnel to perform the tasks in this PWS:

Data Manager –The Data Manager will be responsible for the overall quality of the data and the data-related reports specified in the PWS. The Data Manager will also be primarily responsible for data validation, data reconciliation, and the aggregation of data collected at each support location into a unified system capable of producing consolidated reports and metrics. The Data Manager shall have at least 3 years' experience in eCMS and its supporting systems and an understanding of OPAL business practices to include, reporting, policies, and procedures.

Senior Business Analyst - The Senior Business Analyst will be responsible for supporting an end-user community, training, identifying business needs and determining solutions to business problems. Solutions often include a systems development component, but may also consist of process improvement or organizational change. The Senior Business Analyst shall have at least 2 years' experience in eCMS and its supporting systems and an understanding of OPAL business practices and data. Advanced knowledge in Micro Strategy, MS SQL, Microsoft Access, Microsoft Excel, and Microsoft SharePoint is required.

Tasks under this PWS shall be performed by the personnel listed above, only one Data Manager is required to support all locations, if exercised, and one Senior Business Analyst is required for each location, if exercised.

5.2 SUPPORT TO OPAL CONTRACTING TEAMS

5.2.1 OPAL eCMS HELP DESK SUPPORT

The Contractor shall provide eCMS Help Desk support for all OPAL users via on-site desk-side, telephone, email and/or web cast. On-site support shall be available 80% of the time, off-site support through any medium 100% of the time. OPAL normal business hours are defined as 8:00 am to 5:00 pm for the time zone that the offices are operating under. The Contractor shall provide eCMS support for links to all systems referenced in PWS Section 1.0. The Contractor shall report irregularities to the COR and reconcile data between eCMS and other IAE systems as requested. The Contractor shall provide a response within 30 minutes from receipt of the notification. The Contractor shall provide resolution to the problem within 2 hours. Any issue that the Contractor cannot resolve within 2 hours shall be escalated to an OPAL eCMS Application Coordinator,

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

VA eCMS Help Desk Support Team, or an OPAL Integrated Funds Control, Accounting and Procurements (IFCAP) Point of Contact.

5.2.2 ENTERPRISE ACQUISITION SYSTEM (EAS) REFERRALS

The Contractor shall escalate any identified issue that cannot be resolved, to the EAS Help Desk within 1 hour of receipt of Help Desk ticket. The Contractor shall ensure that the end user is copied on all correspondence between the eCMS Help Desk and EAS Help Desk. The Contractor shall be responsible for tracking, coordinating and reporting of all escalated issues until resolved. Upon escalation of trouble tickets to the EAS Help Desk, the Contractor is not responsible for the resolution of the identified issue, however, shall be responsible for reporting until resolution is achieved. Typically 99% of issues are resolved prior to escalation to the eCMS Help Desk.

5.2.3 OPAL eCMS CONTRACTING SYSTEM SUPPORT

The Contractor shall provide the following OPAL eCMS contracting support:

1. Work with VA staff to support IFCAP which includes such activities as assisting in resolving obligation problems, training staff in information to be transferred for obligation. The Contractor shall assist OPAL staff with retrieval of 2237s from IFCAP into eCMS.
2. The Contractor shall perform problem resolution and training when contracting staff are having issues with completion of eCMS tasks, to train users to create and manage actions/documents in eCMS.
3. Provide problem resolution and one-on-one training when contracting staff are having issues with reporting of contracting actions from eCMS to Federal Procurement Data System – New Generation (FPDS-NG). The Contractor shall validate FPDS-NG data migration from eCMS to FPDS-NG.
4. Train and conduct problem resolution and one-on-one training when contracting staff are having issues in reporting of solicitation and solicitation amendment actions to FBO, including verifying solicitation data and documents are properly loaded into FBO and that users follow proper FBO upload procedures.
5. Train and conduct problem resolution and one-on-one training when contracting staff are having issues with the communication of solicitation and solicitation amendment actions from eCMS to GSA's e-Buy system, utilizing e-Buy Connect.

5.2.4 OPAL eCMS APPLICATION SUPPORT

The Contractor shall provide the following OPAL eCMS application support:

1. Based upon direction by the OPAL Government eCMS Application Coordinator the Contractor shall perform configuration of user accounts, assignment of roles

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

and permissions, specification of site data, identity register information, standard address data, monitor, and edit warrant information, and desktop access.

2. Collect contracting data artifacts and materials that may potentially be suitable for reuse by other VA eCMS users, these may be in the context of Best Practices/Standard Operating Procedures (SOP), and providing those artifacts to the COR and Contracting Officer prior to submitting to the eCMS Core Team for review and possible posting on the Center for Acquisition Resource Excellence (CARE) portal.

5.2.5 BEST PRACTICES AND STANDARD OPERATING PROCEDURES (SOPs)

The Contractor shall recommend Best Practices and SOPs for OPAL eCMS. These shall each be comprised of OPAL specific:

1. eCMS data value guidance;
2. Procedures for milestones of various eCMS action types;
3. Procedures for standard filing of eCMS actions;
4. Procedures on organizing and uploading action briefcase files; and
5. Process to ensure proper adherence to the weekly pipeline and workload reports that are reviewed by OPAL leadership

5.3 REPORTING SUPPORT

The Contractor shall utilize the Procurement Data Warehouse using Microstrategy for generation of Standard Reports, detailed below, and Customized Reports. It is expected that in addition to the Standard Reports listed below, 2 additional Standard Reports will be added per year.

In the case the eCMS and VOA Ad Hoc Reporting Tool fail to function or are not capable of creating the Standard Reports, the Contractor shall generate the reports utilizing Microsoft Access or Microsoft Excel.

The Contractor shall develop and provide the following Standard Reports:

1. Weekly and Monthly Award Reports – The Contractor shall develop Weekly and Monthly Award Reports to track all awards made within OPAL. One of these reports shall contain all award action fields from eCMS with the filter being Action State of awarded in the current fiscal year.
2. VOA Award Report – This Report shall track all awarded actions within VOA in the current fiscal year.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

3. Monthly FPDS-NG Year to Date Report – This Report shall be pulled from www.fpds.gov to report on all awards reported to FPDS in the current fiscal year.
4. Monthly Adhoc Reconciliation of Virtual Office of Acquisition (VOA) to eCMS Reports– The Contractor shall develop this report with 25 columns to compare fields in the VOA with data values in eCMS to compare the data within eCMS and VOA and to locate deltas and inconsistencies. Both awarded and not awarded actions need to be reconciled in the current fiscal year and past fiscal years.
5. Daily eCMS Pipeline Reports – The Contractor shall utilize and maintain the Adobe PDF version of the eCMS Pipeline report located in Microstrategy to provide this report. The Contractor shall be responsible for all formatting including advanced and conditional formatting. The Contractor is also responsible for the creation and maintenance of all logic built into the report.
6. Daily FORCE Pipeline Reports – The Contractor shall utilize and maintain the Microsoft Excel version of the FORCE Pipeline report located in Microstrategy to provide this Report. The Contractor shall be responsible for all formatting including advanced and conditional formatting. The Contractor is also responsible for the creation and maintenance of all logic and filters built into the report.
7. Daily Adhoc Data Integrity Reports – The Contractor shall review on a daily basis all Pipeline reports and Award Report to identify data anomalies to provide this Report. Based upon their review, the Contractor shall report their findings to the eCMS Application Coordinator at their respective site. The Contractor shall create reports in Microstrategy to easily locate these data anomalies and work with contracting staff to resolve the data errors. The Contractor shall follow up to make sure that all errors have been corrected.
8. Biweekly Closeout Reports – The Contractor shall utilize and maintain the Microsoft Excel Closeout Report created from the Microsoft Access Closeout database tool to generate this Report. For the excel report, the Contractor shall be responsible for all formatting including advanced and conditional formatting. For the access database, the Contractor is responsible for the creation and maintenance of all tables, queries and logic built into the Closeout database tool.

The Customized Reports are any other reports that are not listed above and require the Contractor to generate them manually utilizing eCMS, VOA, VOA Ad Hoc Reporting Tool and Microstrategy. These reports are estimated at 20 per month for the life of the effort.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

The Contractor shall ensure proper email subscriptions are set up and maintained for each report within VOA and Microstrategy based on the requirements specified by OPAL government eCMS Application Coordinator.

Deliverables:

- A. Standard Reports
- B. Customized Reports

5.4 TRAINING SUPPORT

The Contractor shall conduct training sessions for new eCMS features, new eCMS users and eCMS refresher training. Training shall be performed in the eCMS Training environment. VA OPAL will provide the training facilities and equipment required to accomplish each session. The training sessions shall be conducted as classroom base, with the capability to allow access from remote participants.

The Contractor shall provide and update Training Materials and instructional information to reflect new and modified features introduced for each eCMS release. The training requirements are listed below:

1. eCMS New Releases Training

The Contractor shall provide information and guidance to support eCMS New Releases to adhere to existing OPAL standard procedures and best practices. The Contractor shall update end-user of all new features implemented in new eCMS releases. The Contractor shall provide electronic only eCMS New Release Training Material detailing the training content that they are going to cover in each New Releases Training Session.

2. eCMS Refresher Training

The Contractor shall provide eCMS Refresher Training as required at each facility to ensure VA OPAL staffs obtain the latest knowledge of procedures and processes to operate eCMS. The sessions shall be coordinated directly with the VA OPAL supervisory staff of each location and the COR of the eCMS contract. The Contractor shall provide electronic eCMS Refresher Training Material detailing the training content that they are going to cover in each Refresher Training Sessions.

The Contractor shall develop and provide Training Material to include training agenda and training presentation slides for each training session. The Contractor shall create a list of completed training and attendees.

3. eCMS New User Training

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

The Contractor shall provide eCMS New User Training as required at each facility to ensure VA OPAL staffs obtain knowledge of the procedures and processes to operate eCMS. The sessions shall be coordinated directly with the VA OPAL supervisory staff of each location and the COR of the eCMS contract. The Contractor shall use the eCMS New User Training Material developed by the VA Acquisition Academy (VAAA).

The Contractor shall generate and provide an eCMS Training Material and Attendees List Report. This Report shall contain the final training material for each new eCMS features, new eCMS users and eCMS refresher training and a list of attendees for each training session conducted.

Deliverables

- A. eCMS New Release Training Materials
- B. eCMS Refresher Training Materials

5.5 ADDITIONAL LOCATIONS TIER 1 ECMS SUPPORT SERVICES (OPTIONAL TASK ONE)

If exercised by VA, the Contractor shall perform the work required under PWS Sections 5.1 through 5.4 to provide eCMS Tier 1 support services for one additional VA facility, up to a total of 6 additional sites. This Optional Task may be exercised up to 6 times in each period of performance, once for each facility listed in PWS Section 4.2.

5.6 DASHBOARD REPORTS (OPTIONAL TASK TWO)

If exercised by VA, the Contractor shall develop a Dashboard Report that will pull data from eCMS, VOA, and FPDS to provide OPAL leadership with the statistics included in Attachment A - "Sample Dashboard Report". The Contractor shall include five (5) minor revisions (determined by the COR), per year. The distribution of these reports shall be weekly in October through August and daily in September. This Optional Task may be exercised up to 7 times in each period of performance, once for each facility listed in PWS Section 4.2.

Deliverable

- A. Dashboard Report

5.7 OPTION PERIODS ONE - FOUR

If the Option Period is exercised by VA, all tasks in the following sections shall apply: 5.1 through 5.4, and all subsections (except 5.1.1 which pertains to the base period only) and, if exercised, 5.5 and 5.6.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 ONE-VA TECHNICAL REFERENCE MODEL

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.

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), 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 comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in the VA Handbook 6510 and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

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

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-04-04, M-05-24, M-11-11, and NIST

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at:

<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf>,

<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf>, and

<https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf> respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

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

1. Automated provisioning and are able to use enterprise provisioning service.
2. Interfacing with VA's Master Veteran Index (MVI) to provision identity attributes, if the solution relies on VA user identities. MVI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VAIQ# 7712300 Mandate to meet PIV requirements for new and existing systems.

<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846>

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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

6.1.3 INTERNET PROTOCOL VERSION 6 (IPv6)

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005

(<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/y2005/m05-22.pdf>) and September 28, 2010 (<https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf>). IPv6 technology, in accordance with the USGv6 Profile, NIST Special Publication (SP) 500-267 (<https://www.nist.gov/programs-projects/usgv6-technical-basis-next-generation-internet>), the Technical Infrastructure for USGv6 Adoption (<http://www-x.antd.nist.gov/usgv6/index.html>), 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. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack (IPv6/IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack (IPv6/ IPv4) operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282>.

6.1.4 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/y2008/m08-05.pdf>), M08-23 mandating Domain Name System Security (NSSEC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/y2008/m08-23.pdf>), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

6.1.5 STANDARD COMPUTER CONFIGURATION

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 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 365 ProPlus and Windows 10. However, Office 365 ProPlus and Windows 10 are not the VA standard yet and are currently approved for

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

limited use during their rollout, we are in-process of this rollout and making them the standard by OI&T. Upon the release approval of Office 365 ProPlus and Windows 10 individually as the VA standard, Office 365 ProPlus and Windows 10 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 with switches for silent and unattended installation 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) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP)

The Contractor shall support VA efforts IAW the Veteran Focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP Guide can be found at <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>. 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 now the single authoritative process that IT projects must follow to ensure development and delivery of IT products

6.1.7 PROCESS ASSETT LIBRARY (PAL)

The Contractor shall utilize PAL, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to VIP standards). PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards or guides to assist project teams in facilitating their VIP compliant work.

6.2 SECURITY AND PRIVACY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

- 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.
- c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
 - d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
 - 1) Optional Form 306
 - 2) Self-Certification of Continuous Service
 - 3) VA Form 0710
 - 4) Completed SIC Fingerprint Request Form
 - e. 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).
 - f. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
 - g. 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.
 - h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

- i. 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.
- j. 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.
- k. 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 Performance Levels
-----------------------	----------------------	-------------------------------

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

<p>5.1.3 Reporting Requirements</p>	<p>Help Desk Monthly Summary Log</p> <p>Help Desk Log of monthly, quarterly and yearly roll-up of help desk activities and all issues separated by location.</p>	<p>COR review of Monthly report, Call log, complaints and observance of performance.</p>
<p>5.2.1 OPAL eCMS Help Desk Support</p>	<p>On-Site Support - Provide desk-side support for all OPAL users, resolving issues on an ad hoc basis. 80% of problem resolution within two hours of help desk request. 100% Problem resolution within two business day of receipt of help desk request.</p> <p>Off-Site Support. Contractor support staff shall provide telephone, e-mail, and web cast support to users 90% within one business day, 100% of time in 3 business days.</p>	<p>COR review of contractor log, complaints, and observance of performance</p>
<p>5.2.2 EAS Referrals</p>	<p>Escalate the identified issue, if cannot be resolved, to the EAS help desk within 1 hour of receipt of help desk ticket.</p>	<p>COR review of Monthly report, Call log, complaints and observance of performance.</p>

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

<p>5.2.3 OPAL eCMS Contracting System Support</p>	<p>1. Support IFCAP activities.</p> <p>2. Problem resolution issues with completion of contract administration tasks</p> <p>3. Problem resolution from eCMS to FPDS-NG. Validate FPDS-NG data migration from eCMS to FPDS-NG.</p> <p>4. Problem resolution from eCMS to FBO</p> <p>5. Problem resolution from eCMS to GSA's e-Buy system, utilizing e-Buy Connect.</p>	<p>80% IN 1 HOUR 20% IN 2 HOURS</p>
<p>5.2.4 OPAL eCMS APPLICATION SUPPORT</p>	<p>1. Perform configuration of user accounts, assignment of roles and permissions, specification of site data, identity register information, standard address data, monitor, and edit warrant information, and desktop access.</p> <p>1. 2. Collection of data artifacts suitable for reuse by other VA eCMS users</p>	<p>1 day 3 days to draft 3 days for final after Government review and approval</p>
<p>5.3 REPORTING SUPPORT</p>	<p>Standard Reports Weekly and Monthly Award Reports – develop reports to track all awards made within OPAL. <u>Monthly FPDS Year to Date Reports</u> – generate report using FPDS to display the number of actions and dollars obligated year to date. <u>Monthly Reconciliation of Virtual Office of Acquisition (VOA) to eCMS Reports</u> –develop a report with 25 columns to compare fields in the VOA with data values in eCMS. <u>Daily eCMS Pipeline Reports</u> - utilize and maintain the Adobe PDF version of the eCMS Pipeline report located in Microstrategy. <u>Daily FORCE Pipeline Reports</u> - utilize and maintain the Microsoft Excel version of the FORCE Pipeline report located in Microstrategy.</p>	<p>1 day to draft reports 1 day for final report after government review and approval</p> <p>.5 day to draft</p>

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

	<p><u>Daily Adhoc Data Integrity Reports</u> - review on a daily basis all Pipeline reports and Award Report to identify data anomalies. Biweekly Closeout Reports - utilize and maintain the Microsoft Excel Closeout Report created from the Microsoft Access Closeout database tool.</p> <p>Custom Reports</p> <p><u>The Customized Reports</u> – develop Customized reports manually utilizing eCMS, VOA, VOA Ad Hoc Reporting Tool, FPDS and Microstrategy. These reports are estimated at 20 per month.</p> <p>Ensure proper email subscriptions are set up and maintained for each report within VOA and Microstrategy.</p>	<p>reports .5 day for final report after government review and approval</p>
5.4 Training Support	<p>eCMS New Release Training Material - provide information and guidance to support eCMS New Releases to adhere to existing OPAL standard procedures and best practices. eCMS Refresher Training Material - provide eCMS Refresher Training to ensure VA OPAL staffs obtain latest knowledge of procedure and process to operate eCMS. New User Training - provide eCMS New User Training to ensure VA OPAL staffs obtain knowledge of procedure and process to operate eCMS. Conduct ad hoc training sessions as required by the contracting office.</p>	<p>60% of training within three business days of the requested training date. 100% within 10 days of requested training date.</p>

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.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

6.5 FACILITY/RESOURCE PROVISIONS

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

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

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

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, PAL, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, 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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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.

6.6 GOVERNMENT FURNISHED PROPERTY

For on-site support the Government will provide the following:

1. Network connectivity
2. Work space
3. Furniture
4. Computer Equipment
5. Office supplies
6. System Admin access level in eCMS

For off-site help desk support the Government will NOT provide any of the above furnished property except network connectivity.

The Government has determined that remote access solutions involving Citrix Access Gateway (CAG) have proven to be an unsatisfactory access method to complete the tasks on this specific contract. The Government also understands that GFE is limited to Contractors requiring direct access to the network to: access development environments; install, configure and run TRM-approved software and tools (e.g., Oracle, Fortify, Eclipse, SoapUI, WebLogic, LoadRunner, etc.); upload/download/ manipulate code, run scripts, apply patches, etc.; configure and change system settings; check logs, troubleshoot/debug, and test/QA.

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

1. **6** of standard laptops

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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

6.7 ORGANIZATIONAL CONFLICT OF INTEREST

Please be advised that since the awardee of this contract will have access to Acquisition sensitive information contained in eCMS it may preclude them from future efforts and some restrictions on future activities of the awardee may be required in accordance with FAR 9.5. The Contractor and its employees, as appropriate, shall be required to sign Non-Disclosure Agreements (Appendix A).

DRAFT

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

APPENDIX A

CONTRACTOR NON-DISCLOSURE AGREEMENT

This Agreement refers to Contract/Order _____ entered into between the Department of Veterans Affairs and _____ (Contractor).

As an officer of **<fill in name of Contractor>**, authorized to bind the company, I understand that in connection with our participation in the **<fill in program>** acquisition under the subject Contract/Order, Contractor's employees may acquire or have access to procurement sensitive or source selection information relating to any aspect of **<fill in program>** acquisition. Company **<fill in name>** hereby agrees that it will obtain Contractor - Employee Personal Financial Interest/Protection of Sensitive Information Agreements from any and all employees who will be tasked to perform work under the subject Contract/Order prior to their assignment to that Contract/Order. The Company shall provide a copy of each signed agreement to the Contracting Officer. Company **<fill in name>** acknowledges that the Contractor - Employee Personal Financial Interest/Protection of Sensitive Information Agreements require Contractor's employee(s) to promptly notify Company management in the event that the employee releases any of the information covered by that agreement and/or whether during the course of their participation, the employee, his or her spouse, minor children or any member of the employee's immediate family/household has/or acquires any holdings or interest whatsoever in any other private organization (e.g., contractors, offerors, their subcontractors, joint venture partners, or team members), identified to the employee during the course of the employee's participation, which may have an interest in the matter the Company is supporting pursuant to the above stated Contract/Order. The Company agrees to educate its employees in regard to their conflict of interest responsibilities.

Company **<fill in name>** further agrees that it will notify the Contracting Officer within 24 hours, or the next working day, whichever is later, of any employee violation. The notification will identify the business organization or other entity, or individual person, to whom the information in question was divulged and the content of that information. Company **<fill in name>** agrees, in the event of such notification, that, unless authorized otherwise by the Contracting Officer, it will immediately withdraw that employee from further participation in the acquisition until the Organizational Conflict of Interest issue is resolved.

This agreement shall be interpreted under and in conformance with the laws of the United States.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

Signature and Date

Company

Printed Name

Phone Number

DRAFT

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

**CONTRACTOR EMPLOYEE
PERSONAL FINANCIAL INTEREST/PROTECTION OF SENSITIVE INFORMATION
AGREEMENT**

This Agreement refers to Contract/Order _____ entered into between the Department of Veterans Affairs and _____ (Contractor).

As an employee of the aforementioned Contractor, I understand that in connection with my involvement in the support of the above-referenced Contract/Order, I may receive or have access to certain "sensitive information" relating to said Contract/Order, and/or may be called upon to perform services which could have a potential impact on the financial interests of other companies, businesses or corporate entities. I hereby agree that I will not discuss or otherwise disclose (except as may be legally or contractually required) any such "sensitive information" maintained by the Department of Veterans Affairs or by others on behalf of the Department of Veterans Affairs, to any person, including personnel in my own organization, not authorized to receive such information.

"Sensitive information" includes:

- (a) Information provided to the Contractor or the Government that would be competitively useful on current or future related procurements; or
- (b) Is considered source selection information or bid and proposal information as defined in FAR 2.101, and FAR 3.104-4; or
- (c) Contains (1) information about a Contractor's pricing, rates, costs, schedule, or contract performance; or (2) the Government's analysis of that information; or
- (d) Program information relating to current or estimated budgets, schedules or other financial information relating to the program office; or
- (e) Is properly marked as source selection information or any similar markings.

Should "sensitive information" be provided to me under this Contract/Order, I agree not to discuss or disclose such information with/to any individual not authorized to receive such information. If there is any uncertainty as to whether the disclosed information comprises "sensitive information", I will request my employer to request a determination in writing from the Department of Veterans Affairs Contracting Officer as to the need to protect this information from disclosure.

I will promptly notify my employer if, during my participation in the subject Contract/Order, I am assigned any duties that could affect the interests of a company, business or corporate entity in which either I, my spouse or minor children, or any member of my immediate family/household has a personal financial interest. "Financial interest" is defined as compensation for employment in the form of wages, salaries, commissions, professional fees, or fees for business referrals, or any financial

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

investments in the business in the form of direct stocks or bond ownership, or partnership interest (excluding non-directed retirement or other mutual fund investments). In the event that, at a later date, I acquire actual knowledge of such an interest or my employer becomes involved in proposing for a solicitation resulting from the work under this Contract/Order, as either an offeror, an advisor to an offeror, or as a Subcontractor to an offeror, I will promptly notify my employer. I understand this may disqualify me from any further involvement with this Contract/Order, as agreed upon between the Department of Veterans Affairs and my company.

Among the possible consequences, I understand that violation of any of the above conditions/requirements may result in my immediate disqualification or termination from working on this Contract/Order pending legal and contractual review.

I further understand and agree that all Confidential, Proprietary and/or Sensitive Information shall be retained, disseminated, released, and destroyed in accordance with the requirements of law and applicable Federal or Department of Veterans Affairs directives, regulations, instructions, policies and guidance.

This Agreement shall be interpreted under and in conformance with the laws of the United States.

I agree to the Terms of this Agreement and certify that I have read and understand the above Agreement. I further certify that the statements made herein are true and correct.

Signature and Date Company

Printed Name Phone Number

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

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

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), 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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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:

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

<https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-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.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

- 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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

**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,

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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 Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*.

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 7 and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk*

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

Management Framework for VA Information Systems – Tier 3: VA Information Security Program and VA Handbook 6500.5, Incorporating Security and Privacy in System Development Lifecycle.

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

c. Include this Privacy Act clause, including this subparagraph (c), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

b. "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

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

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires A&A of the Contractor's systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection security agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

- 1) Vendor must accept the system without the drive;
- 2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

- 3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
- 4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;
 - a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
 - b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
 - c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

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.

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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;

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

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) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Information Security Rules of Behavior, updated version located at <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4848>, relating to access to VA information and information systems;
 - 2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS #10176) and complete this required privacy and information security training annually;
 - 3) 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 2 days 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

**OPAL Tier 1 Electronic Contract Management
System (eCMS) Support Services
TAC-18-50524**

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.

DRAFT