



PERFORMANCE WORK STATEMENT (PWS) DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology

Commodities Enterprise Contract (CEC) – Next Generation (NG)

Date: February 22, 2018

TAC- 18-44158

PWS Version Number: 1.5

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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	9
5.0	SPECIFIC TASKS AND DELIVERABLES.....	10
5.1	PROGRAM/PROJECT MANAGEMENT AND REPORTING.....	10
5.1.1	CONTRACT POST AWARD CONFERENCE.....	10
5.1.2	DELIVERY ORDER KICKOFF MEETINGS.....	11
5.1.3	CONTRACT LEVEL PROGRAM REVIEWS.....	11
5.1.4	CONTRACTOR PROJECT MANAGEMENT PLAN.....	12
5.1.5	MONTHLY PROGRESS REPORTS	12
5.1.6	SHIPMENT/DELIVERY WEEKLY PROGRESS REPORT	13
5.1.7	CEC-NG PRODUCT CATALOG.....	13
5.1.7.1	CEC-NG TECHNOLOGY SERVICE MANAGEMENT PORTAL MAINTENANCE	14
5.1.7.2	CONTRACTOR HOSTING PORTAL	15
5.1.8	CHANGE MANAGEMENT PLAN	16
5.1.9	TECHNOLOGY REFRESH	17
5.1.10	TECHNOLOGY INSERTION.....	19
5.1.11	TECHNOLOGY RETIREMENT	20
5.1.12	INCIDENTAL SOFTWARE	21
5.1.13	INCIDENTAL HARDWARE	21
5.1.14	INCIDENTAL SERVICES	21
6.0	TECHNICAL FUNCTIONAL AREAS	21
6.1	END USER DEVICES.....	22
6.2	SERVERS.....	23
6.3	NETWORKING AND SECURITY APPLIANCES	23
6.4	STORAGE ARRAYS/STORAGE APPLIANCES	23
6.5	CONVERGED VIRTUALIZATION INFRASTRUCTURE	23
6.6	SUPPORTING TECHNOLOGIES	24
7.0	SYSTEM ACCEPTANCE (Pre-production) TESTING	24
8.0	STANDARD INSTALLATION	25
9.0	WARRANTY SUPPORT (it HARDWARE AND INCIDENTAL SOFTWARE).....	27
9.1	WARRANTY REPAIR	34
10.0	INCIDENTAL TECHNICAL SUPPORT SERVICES.....	34
10.1	PRE-DEPLOYMENT SUPPORT SERVICES.....	35
10.1.1	SITE SURVEYS	35
10.2	INSTALLATION AND INITIALIZATION SUPPORT.....	35
10.2.1	CUSTOM INSTALLATION, DESIGN AND CONFIGURATION	35
10.3	POST-DEPLOYMENT SUPPORT SERVICES	35

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

10.3.1	TRAINING SUPPORT	35
10.3.2	APPLICATION SUPPORT.....	36
11.0	PACKAGING, HANDLING, STORAGE AND TRANSPORTATION.....	36
12.0	DELIVERY ACCEPTANCE	37
13.0	VA-SPECIFIC GENERAL REQUIREMENTS	38
13.1	ENTERPRISE AND IT FRAMEWORK.....	38
13.2	CONTRACTOR PERSONNEL SECURITY AND PRIVACY REQUIREMENTS	
	40	
13.3	METHOD AND DISTRIBUTION OF DELIVERABLES	45
13.4	PERFORMANCE METRICS	45
13.5	FACILITY/RESOURCE PROVISIONS.....	46
13.6	SHIPMENT OF HARDWARE OR EQUIPMENT	47
	ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED	50
	ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM	
	SECURITY/PRIVACY LANGUAGE.....	57

DRAFT

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T) is to provide benefits and services to Veterans of the United States. In meeting these goals, OI&T strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely, and compassionate manner. A Veteran-focused enterprise, OI&T seeks to provide a seamless, unified Veteran-experience through the deployment of technology and associated services that will enable the VA to provide the services, care, and benefits our Veterans have earned. The requirements described herein shall support the IT needs of VA programs, Initiatives, and other requirements throughout the VA enterprise, while simultaneously supporting other government agencies with their respective IT Hardware Commodity Product needs.

VA maintains a complex IT enterprise architecture. Accordingly, VA is seeking to establish the Commodity Enterprise Contract – Next Generation (CEC-NG) vehicle through which it will acquire and ensure standardization of commercial IT hardware and associated installation, configuration, warranty, maintenance, and technical support services solutions across the VA enterprise. A Multiple Award Indefinite Delivery, Indefinite Quantity (IDIQ) Multi-Agency Contract (MAC), CEC-NG seeks to build-upon the successes and business practices established, and the cost and schedule efficiencies realized, by VA through the use of the existing CEC contract. The product and task requirements for CEC-NG seek to not only ensure standardization, but interoperability with existing hardware infrastructure, while promoting the adoption of open standard products and leveraging the Government's purchasing power as a large enterprise. The IT Hardware Commodity purchases contemplated for this effort are as follows: end user devices (e.g., laptops, desktops, zero clients, and tablets); servers; networking and security appliances (e.g., switches, routers, wireless access points, controllers, and firewalls); storage arrays/storage appliances (e.g., backup tapes); converged virtualization infrastructure; and supporting technologies (e.g., printers, multi-functional devices, telephony, and video teleconference equipment). CEC-NG laptop and desktop procurements will be consistent with Office of Management and Budget (OMB) Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops. Incidental hardware, software, and services required for successful implementation of integrated solutions may also be acquired via the CEC-NG contracts. Finally, as VA's enterprise architecture continues to evolve, changes and/or updates to the products offered may be necessary to ensure compliance with VA Enterprise Architecture approved initiatives in accordance VA Directive 6051 and 6551. These changes and updates will be incorporated into CEC-NG through unique Technology Refresh, Technology Insertion, and/or Technology Retirement provisions used on the current CEC contract.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
3. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
4. 10 U.S.C. § 2224, “Defense Information Assurance Program”
5. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
6. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
7. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, <http://www.va.gov/vapubs/>
8. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
9. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
10. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
11. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
12. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
13. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
14. 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
15. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
16. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
17. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
18. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
19. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” July 28, 2016
20. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
21. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle”, March 22, 2010
22. VA Handbook 6500.6, “Contract Security,” March 12, 2010
23. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

24. OI&T ProPath Process Methodology (Transitioning to Process Asset Library (PAL) (reference process maps at <http://www.va.gov/PROPATH/Maps.asp> and templates at <http://www.va.gov/PROPATH/Templates.asp>
25. One-VA Technical Reference Model (TRM) (reference at <http://www.va.gov/trm/TRMHomePage.aspx>)
26. National Institute Standards and Technology (NIST) Special Publications (SP)
27. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
28. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
29. VA Directive 6300, Records and Information Management, February 26, 2009
30. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
31. OMB Memorandum, "Transition to IPv6", September 28, 2010
32. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
33. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
34. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
35. 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
36. 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
37. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
38. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
39. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
40. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
41. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
42. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
43. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
44. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
45. 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>)

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

46. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
47. 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>)
48. 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
49. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
50. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
51. 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>)
52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
53. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
54. Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015
55. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
56. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
57. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
58. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
59. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
60. 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>
61. 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>
62. 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>
63. "Veteran Focused Integration Process (VIP) Guide 1.0", December, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

64. “VIP Release Process Guide”, Version 1.4, May 2016,
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
65. “POLARIS User Guide”, Version 1.2, February 2016,
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>
66. VA Directive 6051, “VA Enterprise Architecture,” April 8, 2016
67. VA Directive 6551, “VA Enterprise Design Patterns,” March 17, 2016

3.0 SCOPE OF WORK

VA requires commercial IT solutions (comprised of hardware, incidental services, and incidental software) to improve efficiency and productivity. VA seeks to take advantage of technological advances and new business practices that promise to increase productivity and/or reduce costs while ensuring interoperability with VA’s existing hardware infrastructure. The requirements described herein shall support the IT needs of VA programs, Initiatives, and other requirements throughout the VA enterprise, while simultaneously supporting other government agencies with their respective IT Hardware Commodity Product needs. The IT Hardware Commodity Products included in this acquisition consist of end user devices (e.g., desktops, laptops and zero clients, and tablets); servers; networking and security appliances (e.g., switches/routers, wireless access points, controllers, and firewalls); storage arrays/storage appliances (e.g., backup tapes); converged virtualization infrastructure; and supporting technologies (e.g., printers, multi-functional devices, telephony, and video teleconference equipment); all of which are discussed in Section 6.0 and detailed in the applicable technical specifications attached hereto. In addition to these IT hardware commodities, and the incidental services that support them, any resulting contract shall include the ability to provide advance logistics services in order to ensure all commodities are properly delivered and received. Advance logistics services may include temporary storage of hardware for just-in-time implementation, pre-configuration or imaging, advanced delivery notifications, data about assets being procured, and barcoding to automate VA receipt processes. Incidental hardware, software, and services required for successful implementation may be acquired via any resulting Delivery Order (DO) and are detailed in Sections 9.0, and 10.0 of this document. VA and any other governmental agencies may purchase IT Hardware Commodity Products or total IT solutions. As VA’s Enterprise Architecture continues to evolve, changes and/or updates to the products offered may be necessary to ensure compliance with Enterprise Architecture approved initiatives. These changes and updates will be incorporated into CEC-NG through Technology Refresh, Technology Insertion, and/or Technology Retirement which are discussed in paragraphs 5.1.9, 5.1.10, 5.1.11, respectively.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

4.0 PERFORMANCE DETAILS

This is a competitive acquisition for the award of multiple IDIQ MACs from which Firm Fixed Priced (FFP) DOs shall be competed and issued, unless an exception to fair opportunity is otherwise justified. While it is anticipated that DOs will be predominantly FFP, the use of a Time and Materials (T&M) pricing for select DOs or portions of select DOs is explicitly within the scope of this contract. Any T&M requirements will be defined within the individual DO.

4.1 PERFORMANCE PERIOD

The ordering period for the IT Hardware Commodity Products and services described herein shall be for five (5) years from date of award. However, because performance of each DO awarded prior to Contract expiration may require continued warranty and technical support services as described in Section 9.0, warranty technical support services may be performed for a maximum of years after the expiration of the five (5) year ordering period.

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

There are Federal holidays set by law (USC Title 5 Section 6103) that the Government follows. These Congress Declared holidays or Observed days are listed on Office of Personnel Management (OPM) site: <https://www.opm.gov/policy-data-oversight/snow-dismissal-procedures/federal-holidays/>.

4.2 PLACE OF PERFORMANCE

The IT Hardware Commodity Products will be delivered to, and used at, Government locations throughout the Continental United States (CONUS), as well as those Outside the Continental United States (OCNUS). Incidental services required under any resulting DOs may be performed at any Government facility throughout these CONUS and OCNUS locations. Although government locations may vary depending upon the requiring agency and its specific IT Hardware Commodity Product requirements, a listing of specific VA locations, for informational purposes, only, may be found at <http://www1.va.gov/directory/guide/home.asp?isFlash=1>.

Delivery locations will be specified in any resulting, individual DO. However, please be advised that delivery locations may be subject to change after award via a modification, as agreed to by the respective parties.

4.3 TRAVEL

The Government anticipates that travel will be required for performance of various task requirements described herein. In general, Program Management (PM) travel for

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

Contract level tasks will not be directly reimbursed by the Government and shall be included in the Contractor's FFP for IT Hardware Commodity Products. If additional travel is required, these requirements and costs shall be specified and the terms negotiated at the DO level. Travel for Standard Installation and Warranty shall be captured in the Contractor's Firm Fixed Prices for Standard Installation and Warranty, respectively.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor, which for purposes of this document shall encompass the prime Contractor and all subcontractors, shall perform the following tasks:

5.1 PROGRAM/PROJECT MANAGEMENT AND REPORTING

The Contractor shall provide program/project management support at both the Contract and DO level. This PM or Program Management Team shall work closely with the Government to manage contractual and programmatic issues that arise during performance of the Contract. The Contractor-PM shall be responsible for the execution of all Contract tasks to include, but shall not be limited to: program reviews; kickoff meetings; status updates; various reporting requirements; and day-to-day concerns.

5.1.1 CONTRACT POST AWARD CONFERENCE

The Contractor shall coordinate and administer a Contract Post Award Conference with key stakeholders and subject matter experts (SMEs), all of whom shall be identified by the VA OI&T Program Manager (PM). At the Government's election, the Contract Post Award Conference may be held on-site at the Contractor's facility, Government facility, or by telephone conference. The Contractor shall schedule the Conference within ten (10) business days after contract award or as agreed upon between the VA Contracting Officer's Representative (COR), the CO, and the Contractor. At the Conference, the Contractor shall present the details of the intended approach for managing the Contract, including an Initial Draft Contract Level Work Plan and Schedule to support the quarterly Contract Level Program Review requirements described in paragraph 5.1.3, below. All the key Contractor personnel shall be present for this initial review. Side meetings shall be held to allow for further in-depth discussion of the various program areas, as necessary. The Contractor shall provide a Post Award Conference Report, to include Meeting Minutes and a Post Award Action Item Summary electronically, to the COR and all meeting participants no later than ten (10) calendar days after conclusion of the Contract Post Award Conference.

Deliverables:

- A. Post Award Conference Report
- B. Initial Draft Contract Level Work Plan and Schedule

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

5.1.2 DELIVERY ORDER KICKOFF MEETINGS

If required by the COR and/or CO, the Contractor shall participate in kickoff meetings to be procured at the DO level. The purpose of these meetings is for the Contractor to brief the Government on how it intends to meet all the requirements of the DO. At the Government's election, the kickoff meetings may be held on-site at the Contractor's facility, Government facility, or by telephone conference. Specific requirements will be detailed in the individual DO. The CO also reserves the right to require ad hoc DO meetings as deemed necessary, and at any time throughout the period of performance, to ensure performance of ongoing tasks which are identified by the Government to require closer coordination between the parties. Upon request for any ad hoc meetings, relevant contractor personnel must be made available within seventy-two (72) business hours. Ad hoc meetings may be held virtually.

5.1.3 CONTRACT LEVEL PROGRAM REVIEWS

The Contractor shall conduct Contract Level Program Reviews on a quarterly basis. At the Government's election, the Program Reviews may be held on-site at the Contractor's facility, Government facility, or by telephone conference. These Program Reviews shall address and provide in-depth information on program progress and all functions summarized by DO(s) to include, but shall not be limited to:

1. Administration
 - Including discussion of any key personnel changes that have or will be occurring
2. Schedule
3. Configuration Management
4. Technology Refresh / Insertion/ Retirement Products
 - Summary of technology insertion/refresh/retirement activities
 - Provide a technology roadmap identifying product lifecycle milestones, new technologies and product End Of Life (EOL) and / or End of Sale (EOS) replacement strategies
5. Logistics
6. Testing
7. Quality Assurance
8. Field Support
9. Customer Issues and Resolutions

The Contractor shall provide a Quarterly Program Review Report, which includes Program Review Minutes and a Program Review Action Item Summary, and an updated Contract Level Work Plan and Schedule, electronically, to the COR and all meeting participants no later than ten (10) calendar days after conclusion of the Contract Level Program Review.

Deliverables:

- A. Quarterly Program Review Report
- B. Updated Contract Level Work Plan and Schedule

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

5.1.4 CONTRACTOR PROJECT MANAGEMENT PLAN

If required by the individual DO, the Contractor shall provide a Contractor Project Management Plan (CPMP) specifying the approach, timeline, and tools to be used in execution of the DO. The CPMP shall include the risk, quality and technical management approach, detailed master schedule and milestones, project change control method, and proposed personnel. The Contractor shall keep the CPMP current throughout the DO period of performance. The CPMP shall take the form of both a narrative and graphic format that addresses the requirements discussed above. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as specified within the DO. The initial CPMP shall be delivered electronically to the designated Government Point of Contact (POC) no later than ten (10) calendar days after award of the DO. Updates are to be provided on a semi-annual basis.

Deliverable:

- A. Contractor Project Management Plan and Updates

5.1.5 MONTHLY PROGRESS REPORTS

If required by the individual DO, the Contractor shall submit a Monthly Progress Report (MPR) via electronic mail. The MPRs shall address project status, including all work completed during the reporting period and work planned for the subsequent reporting period. The MPR shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation and a mitigation plan that addresses the immediate issue as well as steps to be taken to avoid future recurrence of the issue. The Contractor shall monitor performance against the CPMP (if applicable) and report any deviations. It is expected that the Contractor shall maintain communication with VA so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall provide the designated Government point of contact (POC) with MPRs in electronic form in Microsoft Word and Project formats no later than five (5) calendar days after the end of the preceding month. These reports shall reflect data as of the last day of the preceding month.

The MPR shall include, but not be limited to, the following items:

1. Project status and progress summary by DO
2. Summary of equipment delivered and/or installed/de-installed that month
3. Summary of repairs, including date/time/location of repair and whether repair was accomplished on-time
4. Significant open issues, risk and mitigation action
5. Summary of problems resolved

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

6. Subcontractor performance – discuss 1st tier subcontractors and vendor performance
7. Schedule status
8. Status of required background investigations
9. Invoices, by Contract Line Item Number (CLIN), submitted and payments received to date
10. Warranty Information
11. License Information
12. Any other areas as specifically identified by the VA as detailed in the individual DOs

Monthly reports shall not contain security related information.

Deliverable:

- A. Monthly Progress Report

5.1.6 SHIPMENT/DELIVERY WEEKLY PROGRESS REPORT

If required by the individual DO, the Contractor shall provide a Shipment/Delivery Weekly Progress Report which shall identify (if applicable), but shall not be limited to: the items shipped, the serial number service tag, Model, Media Access Controller Address, and Manufacturer associated with each piece of equipment; the date of each shipment; the status of each shipment; tracking information; and information relative to Government-receipt of the equipment items at each delivery site. In addition, the Shipment/Delivery Weekly Progress Report shall identify any problems encountered and provide a description of how the problems were resolved or addressed. If problems have not been completely resolved, the Contractor shall provide an explanation and status of resolution. Shipment/Delivery Weekly Progress Reports shall be submitted to the VA PM in Microsoft Excel Format and shall clearly identify each serial number of the equipment being delivered with one (1) serial number per cell. The Shipment/Delivery Weekly Progress Report shall be provided weekly beginning two (2) weeks after any resulting award of the Order and conclude after the final delivery required under the Order has been accepted by the Government.

Deliverable:

- A. Weekly Progress Report

5.1.7 CEC-NG PRODUCT CATALOG

The Contractor shall create, provide, and maintain a CEC-NG Product Catalog. The CEC-NG Product Catalog shall be provided electronically to the COR and CO, and shall detail all IT Hardware Commodity Products and prices offered by the Contractor under its respective CEC-NG Contract. The catalog shall also include, but not be limited to: IT Hardware Commodity Product Specification Sheets; incidental software and hardware dependencies; Manufacturer; Manufacturer Part Numbers; Unit Prices; and associated prices for all subcomponents/modules that can be applied to the commodity items to

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

customize them to specific implementations. Please note that the CEC-NG Product Catalog shall not include the Contractor's contractually incorporated ceiling prices; instead, the CEC-NG Product Catalog unit price shall be the commercially published list price for each IT Hardware Commodity Product and associated subcomponents/modules, which will be utilized solely for informational purposes. The Government reserves the right to purchase any and/or all subcomponents/modules as specified in the Contractor's catalog. The CEC-NG Product Catalog shall be updated following each Government-approved Technology Refresh, Technology Insertion, and Technology Retirement ECP.

Deliverable:

A. CEC-NG Product Catalog

5.1.7.1 CEC-NG TECHNOLOGY SERVICE MANAGEMENT PORTAL MAINTENANCE

The Government anticipates the formation and maintenance of an Information Technology Service Management (ITSM) portal(s), the primary purpose of which is to store information relative to all IT Hardware Commodity Products available under CEC-NG for the government-wide marketplace. In addition, the ITSM shall also serve as a Delivery Order Tracking System. Upon Government development and issuance of approval from the CO or His / Her Designee, the Contractor shall upload the CEC-NG Product Catalog to the ITSM portal and provide updated information, as necessary, to reflect changes in IT Hardware Commodity Products, as a result of government-approved Engineering Change Proposals.

The ITSM Portal site(s) will also be used as a DO Tracking System up to the point of, and including, delivery and maintenance of the IT Commodity Products. Therefore, the Contractor shall also provide up-to-date ITSM Portal Information as necessary on the ITSM Portal site(s) including, but not limited to:

1. Product Description
 - a. Bill of Material (BOM)
 - b. Serial Number / Service Tag (if applicable)
 - c. Model Number
 - d. The Contractor shall provide all commercially available hardware documentation to include specifications, installation guides, user's manuals and/or any additional standard hardware documentation electronically
2. Procurement / Delivery Date / Tracking and Delivery Information
3. Government contract number / Order number (VA uses Electronic Contract Management System (eCMS) Contract. Other agencies may have different system.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

4. Government Purchase Order (PO) Number (VA uses Integrated Funds Distribution Control Point Activity Accounting & Procurement (IFCAP). Other agencies may have different system
5. Government Delivery Site Code (if applicable)
6. Government Delivery Site Mailing Address
7. Equipment Status up to and including delivery confirmation
8. Warranty Information
9. Incidental Software License Information
10. Toll Free Phone Number for warranty support

The ITSM Portal will be used to present all IT Hardware Commodity Products and incidental services offered by the CEC-NG contract to government customers as well as up-to-date status and tracking information. The ITSM portal may change throughout the contract's period of performance; therefore, the Government unilaterally reserves the right to modify the form, format, and information to be provided.

Where possible, the Contractor shall use electronic means to collect data to populate the portals and reduce paper (for example Electronic Packing Slips or Advanced Ship Notification (ASN) 856, etc.) to validate delivery.

Upon Contracting Officer notification, the Contractor shall provide the Government with a list of Contractor personnel that require access to the Government ITSM Portal to maintain information on those sites so processes can be initiated for proper security and remote access vetting. The Contractor shall immediately notify the Government if any planned and/or actual personnel changes occur to the staff that will be maintaining information on the ITSM portals.

5.1.7.2 CONTRACTOR HOSTING PORTAL

The Contractor shall create, provide, and host an on-line portal to which the CEC-NG Product Catalog will be uploaded and provide updated information, as necessary, to reflect changes in IT Hardware Commodity Products, as a result of government-approved Engineering Change Proposals.

The Contractor-Hosted Portal site will also be used as a DO Tracking System up to the point of, and including, delivery and maintenance of the IT Commodity Products. Therefore, the Contractor shall also provide up-to-date information including, but not limited to:

1. Product Description
 - a. Bill of Material (BOM)
 - b. Serial Number / Service Tag (if applicable)
 - c. Model Number
 - d. The Contractor shall provide all commercially available hardware documentation to include specifications, installation guides, user's manuals and/or any additional standard hardware documentation electronically

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

2. Procurement / Delivery Date / Tracking and Delivery Information
3. Government contract number / Order number (VA uses Electronic Contract Management System (eCMS) Contract. Other agencies may have different system.
4. Government Purchase Order (PO) Number (VA uses Integrated Funds Distribution Control Point Activity Accounting & Procurement (IFCAP). Other agencies may have different system
5. Government Delivery Site Code (if applicable)
6. Government Delivery Site Mailing Address
7. Equipment Status up to and including delivery confirmation
8. Warranty Information
9. Incidental Software License Information
10. Toll Free Phone Number for warranty support

The Contractor-Hosted Portal will be used to present all IT Hardware Commodity Products and incidental services offered by the CEC-NG contract to government customers as well as up-to-date status and tracking information.

The Contractor-Hosted Portal site shall have capability to sort or filter information to the individual Government agency level. Since the Contractor-Hosted Portal site may contain proprietary or otherwise sensitive information, it shall be the Contractor's responsibility to ensure that the portal is adequately secured and implements role-based access so that only Government personnel with a valid need to know have the ability to access the site. In the event the Contractor is unable to ascertain whether an individual should be granted access to the site, the Contractor shall consult with the VA PM, COR, and/or CO.

Deliverable:

- A. Contractor-Hosted Portal Information

5.1.8 CHANGE MANAGEMENT PLAN

The Contractor shall submit a Change Management Plan that details its process to manage changes to the IT Hardware Commodity Products delivered under any resulting Contract. This Plan must include all changes as described in PWS Attachment A ("Engineering Change Proposals") and describe the methods by which the Contractor validates that the IT Hardware Commodity Product delivered to the Government meets the requirements of the Government's detailed specifications. These methods shall include, but shall not be limited to, necessary performance testing procedures performed by the Contractor and/or necessary VA System Acceptance Testing described in paragraph 7.0, and/or any other non-VA acceptance testing procedures identified within an individual DO. The Plan shall also include the methods by which the Contractor ensures all necessary IT Hardware Commodity Product documentation is updated to adequately reflect these changes. The Change Management Plan shall be delivered electronically to the COR, CO, and VA PM no later than thirty (30) calendar days after contract award. The Contractor is hereby advised that it shall not substitute

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

components of a IT Hardware Commodity Product, or make any modifications thereto, which would result in any change to the vendor/ OEM model or part number proposed, unless authorized, in writing, by the CO through the Engineering Change Proposal (ECP) process.

The Government also recognizes that OEMs often make internal subcomponent changes within specific IT Hardware Commodity Products that do not change the high-level model numbers of the components. The parties recognize that subcomponent changes often can have material effects on the compatibility of specific products with other IT assets or systems. If after any award, the Contractor independently determines that an OEM subcomponent change has negatively affected the ability of an IT Hardware Commodity Product to interoperate with other Government IT assets or systems, the Contractor shall notify the Contracting Officer immediately and rectify the situation within ten (10) calendar days of a request by the Contracting Officer. In the event that the Government determines that an OEM component change has negatively affected the ability of an IT Hardware Commodity Product to interoperate with other Government IT assets or systems, the Contractor shall rectify the situation within ten (10) calendar days of receipt of the Contracting Officer's notification. If the OEM is unable to correct the interoperability problem within ten (10) calendar days, the Contractor may propose an alternate, interoperable product to be substituted in the original component's place, via an Emergency ECP. All Emergency ECPs must be submitted for Government approval within two (2) calendar days of Contractor and/or Government determination that the inoperability problem is not correctable. The Contractor shall deliver substitute components within thirty (30) calendar days of approval of the Emergency ECP at no additional cost and no additional schedule impact to the DO. The IT Hardware Commodity Product prices proposed, and incorporated into any resulting contract, are binding and thereby establish the Government's maximum liability for said IT Hardware Commodity Product over the life of the Contract. Therefore, the price of the IT Hardware Commodity Product(s) substituted due to inoperability shall not exceed the price proposed and incorporated into the basic Contract, for the IT Hardware Commodity Product being substituted.

Deliverables:

- A. Change Management Plan
- B. Emergency Engineering Change Proposals

5.1.9 TECHNOLOGY REFRESH

The Contractor shall monitor all IT Hardware Commodity Products provided under any resulting CEC-NG Contract and notify the CO if any IT Hardware Commodity Products are required to be changed or updated to accommodate the latest technology. If any IT Hardware Commodity Products are approaching the EOL and/or EOS (e.g., if a vendor/ OEM will no longer be marketing, selling, or promoting a particular product, or limiting or ending support for said product) within the next twelve (12) months the Contractor shall provide notification and a Technology Refresh ECP, as defined in PWS Attachment A,

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

to the COR and CO no less than twelve (12) months prior to the EOL and/or EOS date. Notification shall be either via email or other electronic means, as stipulated by the CO. The Contractor shall update the ITSM Portal with product refresh information within ten (10) calendar days (as defined in Section 5.1.7) from receipt of Government approval. The Government reserves the right to reject any Contractor-proposed ECP, for any reason, at no cost to the Government.

The following conditions shall be met in performing a technology refresh:

- a. The product(s) refreshed shall be fully compatible/backwards compatible with the originally provided product.
- b. The product(s) refreshed shall meet or exceed the mandatory technical requirements as stated in the Government's applicable product specifications.

NOTE: The Government recognizes that over time IT Hardware Commodity Products experience subcomponent specification changes that do not substantially change the fundamental characteristics of the original product proposed. For example, ports and interface cabling methods of products may substantially change, but these interface changes are easily overcome by adapter cables. If a replacement product cannot meet any product characteristic, the Contractor may propose a replacement product; however, when proposing a product with changes via the ECP process, the Contractor shall document the subcomponent characteristics the replacement product does not meet with respect to the original specification and why it believes not meeting these characteristics is immaterial to the successful ability for the replacement product proposed to meet the original intent of the IT Hardware Commodity Product. The Government shall take the Contractor's and OEM's recommendation into account when determining acceptability of the replacement product. If a specification variance is allowed, the Government will notify all Contract holders of the updated allowance so other Contract holders may take this allowance into account with respect to future ECPs it may propose. .

- c. The IT Hardware Commodity Product(s) refreshed shall be off-the-shelf configurations, i.e. the refreshed IT Hardware Commodity Products proposed by the Contractor shall be available for purchase across industry segments and should minimize any custom hardware or custom software unique to the Government's needs.
- d. The product prices proposed, and incorporated into any resulting contract, are binding and thereby establish the Government's maximum liability for said product over the life of the Contract. Therefore, the price of the product(s) refreshed, including support services, shall not exceed the price proposed and incorporated into the basic Contract, for the product being refreshed.
- e. On a quarterly basis the Contractor shall review all IT Hardware Commodity Products on contract to ensure that the products are meeting contract requirements and leveraging technology advancement, including the ability to be purchased with the maximum warranty term, as defined in Section 9.0. If after

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

1 this review the Contractor determines that no changes are required for any
2 specific IT Hardware Commodity Product, then the Contractor shall notify the
3 Government of its intent to not make any change to that commodity. If the
4 Contractor determines that a commodity change is required, then the Contractor
5 shall notify the Government of the results of its review as part of its engagement
6 of the ECP process. The Contractor shall develop CEC-NG Products Review
7 Report to detail the status of CEC-NG products.

- 8 f. All refreshed products shall comply with the Acceptance testing defined in
9 Section 7.0 of this PWS.
- 10 g. The Government may request one (1) or more ECP test unit(s) for an
11 approximate duration of six (6) months for the Acceptance testing and baseline
12 configuration development. The ECP test unit shall be provided at no additional
13 cost to the Government. The Contractor shall be responsible for the
14 configuration reset, shipping, packaging and return of the ECP test unit at no
15 additional cost to the Government. The Government will make every effort to not
16 put protected information onto the storage media of any ECP test unit, however,
17 if it does, at the Governments discretion, and with no additional cost to the
18 Government, the storage media may be retained by the Government after the
19 testing period has completed. As removal of storage media in some products
20 can pose significant difficulty and/or repackaging and return shipping may pose
21 an expense greater than the cost of the ECP test unit, the Contractor may simply
22 elect to abandon the ECP test unit in place. If the Contractor elects
23 abandonment it shall notify the Government in writing anytime during the test
24 period. If the ECP test unit is abandoned the Government may elect to retain the
25 hardware or dispose of the hardware as the Government sees fit at no expense
26 to the Contractor.

27
28 In performing Technology Refresh of a given IT Hardware Commodity Product, the
29 Contractor shall maintain the same brand name item as identified in the original
30 Contract to the maximum extent practicable. However, the Government also recognizes
31 that this is not always feasible or in the best interest of the parties. Accordingly, any and
32 all requests for a change to OEM shall include a justification for said change with its
33 ECP. Final determination relative to the OEM request is solely within the Government's
34 discretion.

35 36 37 Deliverables:

- 38 A. Technology Refresh Engineering Change Proposals
39 B. CEC-NG Products Review Report
40

41 5.1.10 TECHNOLOGY INSERTION

42 As new IT Hardware Commodity Product technologies are developed and/or used by
43 the commercial industry or the Government, the Government and/or Contractor may
44 identify these technologies, and propose within-scope additions, modifications,
45 upgrades, enhancements, and/or improvements to the contract's IT Hardware

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

Commodity Products. The Contractor shall translate the technology insertion recommendation into a formal Technology Insertion ECP for the CO's approval. The Government reserves the right to reject any Contractor-proposed ECP, for any reason, at no cost to the Government.

All inserted products shall undergo Acceptance testing as defined in Section 7.0 of this PWS.

The Government may request one (1) or more ECP test unit(s) for an approximate duration of six (6) months for the Acceptance testing and baseline configuration development. The ECP test unit shall be provided at no additional cost to the Government. The Contractor shall be responsible for the configuration reset, shipping, packaging and return of the ECP test unit at no additional cost to the Government. The Government will make every effort to not put protected information onto the storage media of any ECP test unit, however, if it does, at the Government's discretion, and with no additional cost to the Government, the storage media may be retained by the Government after the testing period has completed. As removal of storage media in some products can pose significant difficulty and/or repackaging and return shipping may pose an expense greater than the cost of the ECP test unit, the Contractor may simply elect to abandon the ECP test unit in place. If the Contractor elects abandonment it shall notify the Government in writing anytime during the test period. If the ECP test unit is abandoned the Government may elect to retain the hardware or dispose of the hardware as the Government sees fit at no expense to the Contractor.

Please be advised that final determination as to what constitutes a Technology Refresh versus a Technology Insertion rests solely with the Government.

Deliverable:

A. Technology Insertion Engineering Change Proposals

5.1.11 TECHNOLOGY RETIREMENT

Occasionally OEM's cease producing certain commodity products or the Government changes Information Technology strategy affecting the likelihood of a commodity product ever being purchased again. If the Government determines that these changes dramatically reduce the likelihood of a commodity product being purchased, the Government will notify the Contractor that an IT Hardware Commodity Product specification is being retired. If the Government declares a specification retired, the Contractor can cease efforts to find commodity items to remain on contract that meet the Government's specification for that item.

If the Contractor receives notification from its OEM that a commodity product is being permanently retired and the Contractor is unable to find suitable replacement devices from any OEM that can meet the intent of the original Government specification, the Contractor shall recommend that the Government retire that particular specification/product. Included with the Contractor's recommendation shall be OEM

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

documentation pertaining to the retirement of that particular technology and results of its industry search for replacement items which meet the Government's specification. Upon receipt of this notification the Government, at its discretion, may retire the product, or may determine that retirement is not warranted, in which case the Contractor shall propose a new product(s) that meets the Government's requirements. The Government is not obligated to change its specifications to ensure that every Contractor can find products that meet the Governments specification.

5.1.12 INCIDENTAL SOFTWARE

Stand-alone purchasing of software licenses is not within the scope of this Contract. However, software licenses incidental to, and necessary for, the successful operation of IT Hardware Commodity Products that are not a part of the Government Baseline (as defined in Section 7.0) may be included in any resulting DOs. Any incidental software shall go through Pre-Certification and Acceptance testing and/or shall be allowed by the TRM (www.va.gov/trm).

Incidental software may be purchased at time of DO award or as part of a future DO citing the need for incidental software related to IT Hardware Commodity items purchased under a prior CEC-NG DO award. Contractors are hereby advised that in the event of conflict between the TRM and the requirements set forth in an individual DO, the DO requirements take precedence.

5.1.13 INCIDENTAL HARDWARE

In order for proper installation and/or integration of IT Hardware Commodity Products, incidental hardware may be required. These incidental hardware items may consist of, but are not limited to: subcomponents (e.g. Random-Access Memory (RAM), hard drives, and expansion cards); expansion modules; cables; cords; racks; wires; hot swappable components, peripherals, and removable storage media. These items will be identified in individual DOs. In addition, incidental hardware may be purchased as part of any DO solicitation citing the need for incidental hardware related to IT Hardware Commodity items purchased under a prior CEC-NG DO award.

5.1.14 INCIDENTAL SERVICES

Services that are required for successful implementation of, and/or migration of workloads and data off previously acquired IT systems to, the IT Hardware Commodity items purchased may be acquired under the CEC-NG Contract. These services shall be directly related to hardware purchased under the CEC-NG contract vehicle. The services listed within Section 10.0 are within the scope of the Contract and services requirement will be detailed in the individual DO.

6.0 TECHNICAL FUNCTIONAL AREAS

The Contractor shall provide the following IT Hardware Commodity Products and all incidental hardware, software, and services render the hardware operational. Incidental

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

software required shall be specified in individual DOs. The Contractor shall provide all commercially available hardware documentation to include specifications, installation guides, user's manuals and/or any additional standard hardware documentation, electronically. Specific details and quantities shall be described in the individual DOs.

The Contractor shall provide only new equipment and new parts for the required IT Hardware Commodity Products described herein, as well as any other subcomponents and/or incidental hardware. **ABSOLUTELY NO "GRAY MARKET GOODS" shall be provided under any DO, to include any subcomponents and/or incidental hardware.** Gray Market Goods are defined as genuine branded goods sold outside of an authorized sales-territory (or by non-authorized dealers in an authorized territory) at prices lower than being charged in authorized sales territories (or by authorized dealers).

All subcomponents and incidental hardware provided under a DO must be appropriate for use by a federal agency, not invalidate any OEM coverage for the IT Hardware Commodity Product, and be fully compatible and interoperable with the associated IT Hardware Commodity Product.

If software is required under a DO, the Contractor shall only provide the latest commercially available version unless authorized, in writing, by the CO.

The six (6) CEC-NG Technical Functional Areas are detailed below.

6.1 END USER DEVICES

The Contractor shall provide End User Devices (e.g., laptops, desktops, zero clients, and tablets) to facilitate information and data processing and computing mobility across the Government. Detailed specifications for each configuration tier are provided in PWS Attachment B, entitled "End User Devices Specifications."

The Contractor shall provide one (1) OEM for each End User Device Product required in this Technical Functional Area; however, multiple OEMs may be provided across the Technical Functional Area.

The Contractor shall ensure that all end user devices are delivered pre-installed with the operating system (OS) required by the applicable DO, unless otherwise stipulated in the individual DOs. If any DO fails to specify which OS to provide, the Contractor shall ask the Government to confirm the specific OS required so the proper OS can be provided.

If any End User Device DO includes a requirement for cellular functionality for a device, the cellular service contract required to enable the cellular functionality is not in scope of CEC-NG.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

6.2 SERVERS

The Contractor shall provide Servers to facilitate information/data processing, network services, database management and warehousing, community collaboration, training, web services, and/or resource distribution (e.g., cloud computing) across the Government. Servers shall include, but are not limited to, rack and blade devices. Detailed specifications for each product are provided in PWS Attachment C, entitled “Server Specifications.”

The Contractor shall provide one (1) OEM for each Server Product in this Technical Functional Area; however, multiple OEMs may be provided across the Technical Functional Area.

6.3 NETWORKING AND SECURITY APPLIANCES

The Contractor shall provide Networking and Security Appliances to facilitate network connectivity with security capability and communication across the Government. Networking Appliances shall include, but are not limited to Switches, Routers, Wide Area Network (WAN) Acceleration, Security Appliances, Wireless Access Points, Wireless Controllers, and Load Balancers. Detailed specifications for each product are provided in PWS Attachment D, entitled “Networking Appliances Specification.”

The Contractor shall provide one (1) OEM for each Networking and Security Appliance Product in this Technical Functional Area; however, multiple OEMs may be provided across the Technical Functional Area.

6.4 STORAGE ARRAYS/STORAGE APPLIANCES

The Contractor shall provide Storage Arrays/Storage Appliances to facilitate data warehousing, management, sharing, and streaming across the Government. The Storage Appliance category shall also include items such as discrete hard drives, memory components, and storage media. Detailed specifications for each product are provided in PWS Attachment E, entitled “Storage Arrays/Storage Appliances”. The Contractor shall provide one (1) OEM for each Storage Product in this Technical Functional Area; however, multiple OEMs may be provided across the Technical Functional Area.

6.5 CONVERGED VIRTUALIZATION INFRASTRUCTURE

The Contractor shall provide Converged Virtualization Infrastructures (CVI) to facilitate information/data processing, network services, database management and warehousing, community collaboration, training, web services, and/or resource distribution (e.g., cloud computing) across the Government. CVI configurations shall include, but are not limited to, both traditional converged and hyperconfigured

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

1 configurations. Detailed specifications for each product are provided in PWS
2 Attachment F, entitled “CVI Specifications.” The Contractor shall provide one (1) OEM
3 for each CVI Product in this Technical Functional Area; however, multiple OEMs may be
4 provided across the Technical Functional Area.
5
6

6.6 SUPPORTING TECHNOLOGIES

7
8 The Contractor shall provide Supporting Technologies including, but not limited to:
9 Printers, Multi-Functional Devices (MFD), telephony and video teleconference
10 equipment, scanners, and ancillary components. All OEM software required for the
11 successful operation of all Supporting Technology Devices shall be included in the
12 delivery. All Supporting Technology Devices shall be provided ready to use (e.g.,
13 requisite starter ink cartridges, power supplies). Detailed specifications for each product
14 are provided in PWS Attachment G, entitled “Supporting Technologies.” The Contractor
15 shall provide one (1) OEM for each Supporting Technology Product in this Technical
16 Functional Area; however, multiple OEMs may be provided across the Technical
17 Functional Area.
18

7.0 SYSTEM ACCEPTANCE (PRE-PRODUCTION) TESTING

19
20
21 It is the Government’s desire that all End User Devices be delivered to the Government
22 without an Operating System (OS) installed thereon. Contractors will be required to
23 provide each End User Device (including docking stations and monitors) initially, and
24 one (1) End User Device with each Government-approved technical refresh and
25 technical insertion, for Pre-Production testing. The Pre-Production test units shall be
26 provided at no additional cost to the Government. Following successful Pre-Production
27 Testing, the Contractor will not be required to install the Government Baseline; instead,
28 the Government Baseline will be installed by the Government at the field sites.
29

30 Within ten (10) business days after contract award and as part of every approved
31 engineering change proposal (e.g., a new make/model/devices within a model due to
32 technology refresh or insertion), the Contractors shall furnish, at no cost to the
33 Government, the proposed end user device (one (1) of each configuration), to the
34 Government-designated Pre-Production Test facilities.
35

36 The Government Pre-Production Test Facilities will test the end user device to ensure
37 that it functions correctly within the current Government infrastructure; regression
38 testing must take place involving Government application software to ensure that the
39 Government-specific Baseline is functioning correctly. The Government will complete
40 product testing as soon as practicable, however, this regression testing requires a
41 minimum of thirty (30) calendar days for completion. Upon successful regression
42 testing, Government will notify the Contractor that the end user device has passed
43 testing. If the proposed equipment fails to pass the Pre-Production testing, Government
44 will return the failed devices to the Contractor or designated OEM point of contact (at

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

the Contractor's cost), and the Contractor shall provide new devices to the government-designated Pre-Production Test Facility. If the test unit passes, the accepted test unit will not be returned to the Contractor. Government reserves the right to reject any engineering change proposal at no cost to the Government. Any approved engineering change proposal for an item requiring Pre-Production Testing shall be considered conditional until Pre-Production Testing is successfully completed.

8.0 STANDARD INSTALLATION

The Contractor may be required to provide installation support for all IT Hardware Commodity Products listed in the Technical Function Areas, Section 6.0, and as detailed in the attached specifications, as specified in individual DOs. Contractor shall validate successful operation of any installed products prior to acceptance the installation services. Details of the installation tasks to be completed before Government acceptance is granted shall be detailed in the DO.

For all DOs, the Contractor shall provide standard component documentation (e.g., User Manual, Operators Manual, Installation Guide, etc.) to support Government installation and ongoing operation of the hardware. At a minimum, component documentation must be provided in electronic PDF format.

The Contractor shall develop a master delivery schedule of equipment to all sites receiving delivery of equipment as specified in each DO. This schedule shall include, at a minimum, current status of site delivery. Schedules shall be coordinated with the local designated POC for installation requirements for each site identified in the DO.

The Contractor shall install new equipment as indicated in each DO which may require installation of equipment after normal business hours. After-hours installation requirements will be defined in each DO and determined by each site on an installation-by-installation basis.

The Contractor shall abide by all local Government site policies and requirements regarding equipment delivery, installation, and associated personnel. The Contractor shall be responsible for coordinating all deliveries by contacting the site prior to delivery to obtain knowledge of local constraints and policies, including security requirements both for equipment and personnel.

If the new equipment replaces an existing system, the DO may require the Contractor to migrate workload from the existing system to the replacement system. Once the existing system no longer supports production workload the DO may require the Contractor to disconnect the existing hardware and turn it over to local Government IT Operations staff for further disposition. The Contractor shall remove all storage devices (e.g., hard drives, flash memory) from replaced systems, annotate the Government identification number and/or serial number of the new storage device and the Government identification number and/or serial number of the replaced storage device,

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

1 create a cross reference list for signature by the Information Security Officer (ISO), and
2 turn the storage device over to the local Government IT Operations staff.

3
4 When DOs include Standard Installation requirements and do not detail any specific
5 installation requirements, the Contractor shall perform the following installation services:

- 6 1. The Contractor shall remove all packaging and waste associated with new
7 equipment installations and dispose of accordingly. The Government encourages
8 the Contractor to use multipacks, if available.
9
- 10 2. The Contractor shall provide any necessary racks, mounts, brackets, installation
11 kits, and/or interconnection cables necessary to install the required hardware to
12 an operational state. An interconnection cable is defined as a cable between
13 components and subcomponents of an assembly purchased together as part of a
14 single DO, and not cables required to interface the item to the larger IT network (e.g.,
15 uplinks). Any incidental hardware beyond what is described above shall be
16 identified in the individual DOs. Once the new hardware is installed and
17 connected, the hardware shall be powered on, logged onto, and tested for
18 network connectivity. Staging areas for IT Hardware commodities to be installed
19 are usually available at most Government sites (availability and size will vary by
20 site). The Contractor shall coordinate site staging areas with the site delivery
21 POC as identified in the individual DO.
22
- 23 3. The Contractor shall prepare an Installation Certification Sheet and have the
24 installation certified by the designated Government site installation POC. The
25 Contractor shall ensure the Government POC certifies the installation on the
26 same day of installation, and the Contractor must deliver the Installation
27 Certification Sheet to the Government IT Operations POC as specified in the DO.
28
- 29 4. If applicable, and as defined in the individual DO, the Contractor shall input
30 Government asset identification information into the Basic Input / Output System
31 (BIOS) of each Desktop and/or Laptop. The method shall include both a central
32 factory level assignment and a local Government site assignment capability.
33
- 34 5. The Contractor shall apply the Contractor service tag and serial number at the
35 factory on the exterior of the equipment. The Contractor shall provide the serial
36 numbers for each piece of equipment to the VA site installation POC and/or COR
37 no later than five (5) calendar days prior to shipment to the site. Any further
38 requirements for the service tag will be defined at the DO level. The Contractor
39 shall provide a label or tag that can be affixed to each component or assembly
40 purchased that indicates how to engage warranty service on the component or
41 assembly.
42
- 43 6. The Contractor shall provide the necessary knowledge and support for
44 installation of the IT Hardware Commodity Products across the Local Area
45 Network (LAN), virtual private network (VPN), and/or Wide Area Network (WAN)
46 environments.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

7. The Contractor shall provide support for IT hardware installation including applicable operating systems; installation of software; monitoring and adjusting system performance; application of latest hardware/software patches, security updates and service packs; and repairs and upgrades as necessary for installation of the IT Hardware Commodity Product.

All standard installation performed OCONUS will be deemed a custom installation in accordance with PWS paragraph 10.2.1.

9.0 WARRANTY SUPPORT (IT HARDWARE AND INCIDENTAL SOFTWARE)

The Contractor is responsible for warranty and warranty support. The Contractor shall provide, maintain, and administer warranty support agreements for use on all IT Hardware Commodity Products and incidental software, and shall provide extended warranty technical support at the level required in individual DOs. The Contractor shall be the primary/initial interface between the Government and the OEMs regarding all technical support issues as well as the primary interface for all warranty information.

Upon delivery of each IT Hardware Commodity Product, the Contractor shall pass through the applicable OEM warranty to the Government, at no additional cost to the Government. In addition, for all IT Hardware Commodity Products, the Contractor shall provide the Government with the Standard or Premium Warranty, as defined below, as part of the purchase price. This Warranty shall run concurrently with any applicable pass through OEM warranty provided. The Government reserves the right to purchase additional one (1) year increments of either the Standard or Premium Warranty Support, as an Extended Warranty, for any IT Hardware Commodity Product. The Government can purchase an Extended Warranty, be it Standard or Premium Warranty Support, for a Product, as outlined in the table below, at any time prior to the expiration of the then in-effect Warranty coverage period, for that product. However, if the then in-effect Warranty expires, it cannot be renewed via this contract. In no instance, however, shall Warranty Coverage and/or Support exceed seven (7) years from the date a product is purchased.

Product Group	Standard Warranty	Premium Warranty
Group 1 – End User Devices		
Group A – Windows OS-compatible End Point*	Unit price without Warranty	Not Applicable
	Unit price with 1 Year Warranty	Not Applicable
	Unit price with 2 Year Warranty	Not Applicable
	Unit price with 3 Year Warranty	Not Applicable
	Unit price with 4 Year	Not Applicable

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

	Warranty	
Group B – MAC OS-compatible End Point*	Unit price without Warranty	Not Applicable
	Unit price with 1 Year Warranty	Not Applicable
	Unit price with 2 Year Warranty	Not Applicable
	Unit price with 3 Year Warranty	Not Applicable
	Unit price with 4 Year Warranty	Not Applicable
Group C – Zero Clients	Unit price without Warranty	Not Applicable
	Unit price with 1 Year Warranty	Not Applicable
	Unit price with 2 Year Warranty	Not Applicable
	Unit price with 3 Year Warranty	Not Applicable
Groups D - Mobile Tablets	Unit price without Warranty	Not Applicable
	Unit price with 1 Year Warranty	Not Applicable
	Unit price with 2 Year Warranty	Not Applicable
Group 2 – All Servers		
	Unit price without Warranty	
	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
	Unit price with 6 Year Warranty	Unit price with 6 Year Warranty
	Unit price with 7 Year Warranty	Unit price with 7 Year Warranty

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

Group 3 – Networking and Security Appliances		
	Unit price without Warranty	
	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
	Unit price with 6 Year Warranty	Unit price with 6 Year Warranty
	Unit price with 7 Year Warranty	Unit price with 7 Year Warranty
Group 4 – All Storage Arrays/Storage Appliances		
	Unit price without Warranty	
	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
	Unit price with 6 Year Warranty	Unit price with 6 Year Warranty
	Unit price with 7 Year Warranty	Unit price with 7 Year Warranty
Group 5 – All CVI		
	Unit price without Warranty	
	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty

Commodities Enterprise Contract (CEC) – Next Generation (NG)TAC Number: **TAC-18-44158**

	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
	Unit price with 6 Year Warranty	Unit price with 6 Year Warranty
	Unit price with 7 Year Warranty	Unit price with 7 Year Warranty
Group 6 – Supporting Technologies		
	Unit price without Warranty	
	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty

*Note: Standard and Premium Warranty requirements do not apply to Docking Stations. Accordingly, Contractors are not required to provide these warranties with its proposed docking stations; Contractors shall only pass-through the applicable OEM warranty.

For all IT Hardware Commodities, the Warranty shall begin on the first day following the date the equipment is accepted by the Government in accordance with Paragraph 12.0.

To ensure end users can quickly and easily identify the process for warranty support, the Contractor shall apply a label or tag containing pertinent warranty support information, identified below, to each end user device prior to shipping to the Government. These labels or tags shall be in a location that is easily accessible, can withstand normal wear and tear, and shall not interfere with the normal operation and use of the device. Prior to placement of label or tag and shipment of devices, the Contractor shall identify proposed locations and obtain concurrence from the Government Program Manager or COR, as identified within each DO. All costs associated with the inclusion of these labels or tags shall be included in the unit price of the end user device. The labels or tags shall state the following: "This (INSERT TYPE OF DEVICE) was purchased with (INSERT LENGTH OF WARRANTY) warranty. To initiate the warranty support, contact (INSERT CONTRACTOR NAME) at the following phone number (INSERT WARRANTY PHONE NUMBER)." To meet evolving needs, the Government retains the right to alter the language to be included on the labels/tags. This may be done via a no-cost modification to the contract, or identified within the requirements of the individual DO. If the OEM of the item is providing the warranty, then the Contractor may request that the Government waive the requirement to apply the

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

label or tag. If the Government denies the waiver then the label or tag must be provided even for components covered by an OEM warranty.

Warranty Technical Support Levels

The following defines the Standard Warranty Technical Support, and where applicable, the Premium Warranty Technical Support, required for each IT Hardware Commodity Group, which the Contractor shall provide when specified in individual DO requirements. The Contractor shall serve as a single point of interface for all Support and Technical Issues.

If a zero-day security vulnerability (zero day is defined as a security issue or software bug which industry has found to be actively being exploited by hackers) is identified by an OEM with respect to any component of the installed equipment or software during the warranty period, the Contractor shall support all Government efforts to remediate including supporting the installation of patches or other security remediation as soon as they are released by the OEM of the component exhibiting the security vulnerability. Zero-day patching may include implementation of OEM recommended workarounds or other manual remediation steps. The Contractor shall troubleshoot and assist with identifying remediation efforts and helping Government create release management documentation with respect to how to remediate the security vulnerability identified.

During the warranty period, the Contractor shall ensure all components within the solution maintain compatibility with OEM feature updates within thirty (30) calendar days of release to general availability (e.g. new OS shall be supported thirty (30) calendar days following release).

For OEM major software upgrades, the Contractor shall ensure all components within the solution maintain compatibility within ninety (90) calendar days of release to general availability during the warranty period (e.g. when new OS is released it shall be supported by the solution within ninety (90) calendar days following release).

The Contractor shall provide the following with both Standard and Premium Warranties:

1. Software / Firmware / BIOS updates
2. Fault troubleshooting to determine part replacement is necessary

Standard Warranty Requirements

1. Technical telephone and email support shall be available Monday – Friday (i.e., standard five (5) day business week) from 6:00 am to 9:00 pm eastern time. The Contractor shall provide a dedicated toll-free line and technical support email address that will route directly to a Contractor Tier 2 (End User Device Specialist) or 3 (Back Office Device Specialist) customer service/technical support representative, and not a Tier 1 help desk/support technician. The Contractor's dedicated toll-free line and technical support email address shall remain the same throughout the length of the contract and any resulting delivery orders.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

2. The Contractor shall acknowledge the Governments' request for warranty support, via email or call-back, within two (2) business hours of receipt, in accordance with the days and times specified above.
3. Contractor's initial on-site or remote diagnosis shall be completed within one (1) business day from Government's initial request for warranty support.
4. Following diagnosis, on-site labor/repair and/or part/product replacement shall be completed by the Contractor within the same or next business day after Contractor's initial diagnosis. Contractor shall provide steady efforts to ensure that the product is restored to fully operational status.
5. The Contractor shall repair or replace all failing equipment, to fully operational status, by Close of Business (COB) on the second business day after diagnosis. The Contractor shall bear all shipping costs for replacement subcomponents and/or replacement chassis, as well as the return of the failed subcomponents and/or chassis to the Contractor. In the event the Contractor requests that the Government keep the failed subcomponent and/or chassis, and the Government agrees, the Government will bear the disposal costs associated with the failed subcomponent and/or chassis.
6. Each additional business day that the issue is unresolved shall result in the issue continuously being escalated to the next support level, until top level support is reached. The Contractor shall provide the Government with a clear escalation time-line from the Contractor's help desk support technician to the Chief Executive Officer (CEO), or otherwise equivalent highest level Officer.
7. Twenty-four (24) hour access to Contractor or OEM provided web support/knowledge base.
8. Access to all product/firmware microcode patches, updates, and upgrades.

Premium Warranty Requirements

1. Technical telephone and email support shall be available twenty-four (24) hours a day, seven (7) days a week, 365/366 days a year. The Contractor shall provide a dedicated toll-free line and technical support email address that will route directly to Contractor personnel that ensure Premium Warranty requirement can be met. The Contractor's dedicated toll-free line and technical support email address shall remain the same throughout the length of the contract and any resulting delivery order.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

2. Contractor response to Government's request for warranty support shall be made within fifteen (15) minutes of Government's initial contact.
3. Contractor's initial on-site or remote diagnosis shall be completed within four (4) hours from Government's initial request for warranty support.
4. Contractor's initial attempt to repair shall be completed within four (4) hours following the Contractor's initial on-site or remote diagnosis. Contractor shall provide commercially reasonable efforts to ensure that the product is restored to fully operational status.
5. Each four (4)-hour period that the issue is unresolved shall result in the issue continuously being escalated to the next support level, until top level support is reached. The Contractor shall provide the VA with a clear escalation time-line from the Contractor's help desk support technician to the Chief Executive Officer (CEO), or otherwise equivalent highest level Officer.
6. Twenty-Four (24) hour access to Contractor or OEM web support/knowledge base.
7. Access to all product/firmware/ microcode patches, updates and upgrades.

Regardless of whether the Contractor is providing Standard or Premium Warranty Technical Support, the Government will provide internal Tier 1 help desk support for the IT Hardware Commodity Products purchased under any resulting contract. The process flow is defined in PWS Attachment I, entitled "CEC Call Flow." The Contractor shall provide a dedicated toll-free line and technical support email address that will route directly to a Tier 2 (End User Device Specialist) or Tier 3 (Back Office Device Specialist) customer service/technical support representative versus a Tier 1 Government help desk/support technician. If the OEM and the Contractor are not the same, the Contractor is responsible to work through the escalation process. The Contractor shall provide a clear escalation time line and process through all levels of technical support.

Under both Standard and Premium Warranty Technical Support, the Contractor shall provide asset tracking information to the Government's Tier 1 Help Desk for all IT Hardware Commodity Products. Data to be provided shall include, at a minimum:

- 1 Government Contract/order number (e.g., eCMS Contract/order number for VA)
- 2 Purchase Order Number, if applicable (e.g., IFCAP PO for VA)
- 3 Government Delivery Site Code, if applicable
- 4 Government Delivery Site Mailing Address
- 5 Equipment Model
- 6 Equipment Serial Number
- 7 Warranty Information
- 8 Hardware / Software License Information

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

9.1 WARRANTY REPAIR

The Contractor shall provide on-site warranty repair services in accordance with the timeframes set forth in the applicable technical support level specified in an individual DO. The Contractor shall repair or replace all failing equipment covered under the warranty. In the event that failing/defective equipment capable of storing VA data (e.g., hard drives, storage devices, mobile tablets, laptops) is replaced pursuant to the Warranty, the Contractor shall disconnect and/or remove the failing/defective equipment and turn said equipment over to local Government IT Operations Staff for disposition, and/or removal of VA data where possible. If authorized by the Government, failing/defective equipment that is replaced pursuant to the Warranty and is not capable of storing VA data, or from which all VA data has successfully been removed, shall be returned to the Contractor. All replacement items shall, at a minimum, assume the remaining warranty period of the original item replaced. The Contractor shall use OEM original and refurbished parts along with OEM certified technicians to perform any warranty repair. The Contractor shall bear all shipping costs for replacement parts. The Contractor shall only maintain spare parts inventories at Government locations when explicitly approved by the Government.

If the Contractor is not the manufacturer, the Contractor shall manage the service/support function. Additionally, the Contractor is responsible for ensuring that its own or any subcontractor-provided technical support does not void a pass through OEM warranty. If Contractor/Subcontractor provided technical support results in a warranty being voided, the Contractor will still be responsible for providing warranty support with no degradation in system operational status or availability to the Government. Government IT Operations staff shall be authorized to repair faulty equipment on-site without voiding warranties purchased if this is deemed most expeditious to returning the unit to service. These repair services may be conducted by Government or Government contracted staff.

As stated previously, the Contractor shall make available Standard and Premium Extended Warranty coverage for the specified IT Hardware commodities in increments of one (1) year, where applicable, but in no event shall extended warranty coverage exceed the maximum warranty periods identified in Section 9.0, beginning on the first day following Government acceptance of the hardware.

The Contractor shall provide a report of all warranties to the Government as detailed in the individual DOs and provide a listing of any warranties within 180 days of expiration as an attachment to the Monthly Progress Report.

10.0 INCIDENTAL TECHNICAL SUPPORT SERVICES

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

The following services shall be provided by the Contractor for required support above and beyond standard installation and warranty requirements identified in Sections 8.0 and 9.0 and as more specifically identified in individual DOs.

10.1 PRE-DEPLOYMENT SUPPORT SERVICES

10.1.1 SITE SURVEYS

When required, the Government will provide the Contractor access to Government sites to perform site surveys necessary to develop plans for the installation/initialization of the newly acquired hardware and associated incidental software. The Contractor shall take into account floor plans and layouts, existing IT systems, existing software systems and interfaces, existing cabling, power distribution, grounding, Heating, Ventilating, and Air Conditioning (HVAC) systems, access floor systems, lighting, backboards, and any other required Government Furnished Equipment (GFE) and materials.

If facility/structural alterations are required to support installation, all such alterations must be authorized and performed by the Government.

10.2 INSTALLATION AND INITIALIZATION SUPPORT

10.2.1 CUSTOM INSTALLATION, DESIGN AND CONFIGURATION

The Contractor shall provide custom installation, design, and configuration support above and beyond standard installation requirements identified in Section 8.0 and as identified in the individual DOs. These services shall include but are not limited to technical areas such as system design, de-installation, data migration, and OCONUS installations.

10.3 POST-DEPLOYMENT SUPPORT SERVICES

10.3.1 TRAINING SUPPORT

The Contractor shall provide standard commercial training and other services related to installation, set-up, configuration, and use of purchased equipment.

Training requirements shall be specified in individual DOs.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

10.3.2 APPLICATION SUPPORT

Application support shall include support for installation, configuration, upgrading, patching, and/or debugging of all incidental software. If the Contractor is not the software developer, the Contractor shall manage the service/support function.

If a software failure is suspected, the Contractor shall attempt to resolve the issue remotely in accordance with Government security standards and policies. If the software cannot be resolved remotely, the Contractor shall arrange for an on-site technician to be dispatched to resolve the issue. The Contractor shall repair or replace all failing incidental software as required by the terms of the applicable warranty unless otherwise specified in the individual DO. The Contractor shall bear all costs associated with remote and/or on-site technician diagnosis and remediation assistance in repairing the root cause of the software failure.

Application Support requirements shall be specified in individual DOs. The incidental software, as defined within the individual DOs, shall inherit the same warranty support as stipulated for the corresponding IT Hardware Commodity Product.

11.0 PACKAGING, HANDLING, STORAGE AND TRANSPORTATION

The Contractor shall establish packaging, handling, storage and transportation processes and procedures to prevent damage and mishandling of the hardware, incidental software and other incidental items from acquisition through installation. The Contractor shall be liable for all damage, deterioration, and/or losses incurred during shipment, handling, storage and transportation unless the damage, deterioration, and/or losses are due solely to the fault of the Government.

The Contractor shall identify and report to the Government any unique or special packaging, handling, storage or transportation requirements.

The Contractor shall be responsible for transporting equipment to the installation site and for the personnel required for installing the equipment at the installation site. Movement of equipment from the delivery site to the staging and installation locations may require vehicles with lift capability or machine transport carts. The Contractor shall provide its personnel with vehicles, carts, trash, receptacles, and any other equipment or supplies necessary to carry out the requirements of each DO. VA anticipates, at a minimum, that carts will be required at all sites. Additional site requirements will be provided during pre-installation coordination with the sites and as specified in the individual DOs.

Unless otherwise specified, all items shall be preserved, packaged, and packed in accordance with standard commercial practices and in a manner that will afford protection against corrosion, deterioration and physical damage during shipment. The items shall be packed in a manner which conforms to the requirements of Uniform

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

Freight Classification for rail shipment, National Motor Freight Classification for truck shipment, Parcel Post Regulations, and the regulations of other carriers as applicable to the mode of transportation employed.

Exterior shipping containers and items not shipped in containers shall be clearly marked on an external surface as follows:

- a) Delivery POC name & Phone number
- b) Contract Number
- c) DO Number
- d) IFCAP Purchase Order Number (for VA orders)
- e) Itemized list of contents including quantity and Contract Line Item Number (CLIN)

12.0 DELIVERY ACCEPTANCE

Each DO issued will have its own Acceptance Official, who will be identified in the individual DO. Unless otherwise specified within a DO, acceptance of all items delivered under the CEC-NG Contract will take place at the Government site specified on each individual DO. The Contractor shall only tender for acceptance those items that conform to the requirements of the CEC-NG Contract and DO under which delivery of IT Hardware Commodities is required. Government may request equipment be delivered to an individual facility without having the Contractor install the equipment. In these instances, Government will take responsibility for the equipment at the delivery location and free the Contractor from all responsibilities associated with initial equipment installation. In these instances only, the date of acceptance shall be considered to be the date of equipment delivery.

To ensure an orderly delivery and acceptance process, the Contractor shall perform the following:

- Conduct Kick-off Call for the program and additional Kick-off Calls as defined in specific DOs.
- Contact Government POC to verify shipping address and availability to receive shipment, via email. (For VA orders, Carbon Copy (cc) VAITAAGRILLOS@va.gov on all VA orders).
- Once shipment begins to a site, send email to Government POC (for all VA orders, cc vaitaagrilos@va.gov), containing the following:
 - Subject line shall include: Purchase Order Number, project description, and site
 - Shipping date and estimated delivery date
 - Tracking number and details
 - Attach listing of equipment serial numbers
 - Attach copy of Government award document
 - Any agency-specific details shall be identified as a requirement in the individual DOs.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

- Weekly follow-up calls with the designated Government points of contact, if required by the specific DO

13.0 VA-SPECIFIC GENERAL REQUIREMENTS

13.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T One-VA TRM. One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, "VA System Security Controls," and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements set forth in OMB Memoranda M-04-04, M-05-24, M-11-11, as well as the NIST FIPS 201-2, and supporting NIST SP. 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

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

<https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf> respectively. The identity authentication Level of Assurance (LOA) requirement for this specific effort is LOA-4.

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/fy2005/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 (<http://www-x.antd.nist.gov/usgv6/index.html>), the Technical Infrastructure for USGv6 Adoption (<http://www.nist.gov/itl/antd/usgv6.cfm>), and the NIST SP 800 series applicable compliance (<http://csrc.nist.gov/publications/PubsSPs.html>) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native Internet Protocol Version 6 (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, Domain Name Service (DNS), Internet Service Provider (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>.

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/fy2008/m08-05.pdf>), M08-23 mandating Domain Name System Security (NSSEC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf>), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall support VA efforts 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

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.

13.2 CONTRACTOR PERSONNEL SECURITY AND PRIVACY REQUIREMENTS

The following security requirement must be adhered to regarding Contractor owned equipment used to support the VA. PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to 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 the VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the ISO must be notified and verify all security requirements have been adhered to.

1. Information made available to the Contractor/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 the VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, Federal Acquisition Regulation (FAR) 52.227-14(d) (1).

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

2. VA information should not be co-mingled, if possible, with any other data on the Contractor/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 shall ensure that VA's information is returned to the 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 shall not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the 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 shall be sent to the VA CO within thirty (30) days of termination of the Contract.
4. The Contractor/Subcontractor shall receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or 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 for cause under Federal Acquisition Regulation (FAR) Part 12.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

7. The Contractor/Subcontractor shall 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.
8. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.
9. 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's prior written approval. The Contractor/Subcontractor shall refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.
10. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.
11. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Certification and Accreditation (C&A) or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.
12. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access is:

- ☐ Tier 1 / Low Risk
- ☐ Tier 2 / Moderate Risk
- ☐ Tier 4 / High Risk

The Position Sensitivity and Background Investigation will be defined within each individual DO.

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
Tier 1 / Low	National Agency Check with Written Inquiries (NACI) A NACI is conducted by OPM and covers a 5-year period. It consists of a review of

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, “Personnel Security Suitability Program,” Appendix A)
	records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Tier 2 / Moderate	Minimum Background Investigation (MBI) A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.
Tier 3 / High	Background Investigation (BI) A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

Contractor Responsibilities (as required within each individual DO based on Position Sensitivity and Background Investigation):

- 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. The Contractor shall provide the name, address, date of birth, Social Security Number and any other pertinent and relevant information of the Contractor personnel assigned to this project to the COR (or, in the absence of a COR, the Government designated Program Manager), as requested, and prior to the DO Level Kickoff Meetings.
- b. Within three (3) business days after DO 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. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon the designations identified within the DO), 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 Government within one (1) business day of

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

- 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 five (5) business days after DO 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 three (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 three (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

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.

- 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.

Deliverables:

- A. Contractor Staff Roster
- B. Optional Form 306
- C. Self-Certification of Continuous Service
- D. VA Form 0710
- E. Completed SIC Fingerprint Request Form

13.3 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).

13.4 PERFORMANCE METRICS

The Contractor shall monitor performance against the established schedule, milestones, risks, and resource support outlined in the approved CPMP. The Contractor shall report any deviations in the Monthly Progress Report. As a minimum, the following metrics shall be included:

Performance Objective	Performance Standard	Acceptable Performance Levels	Surveillance Method
1. Technical	Shows understanding of requirements	Achieve 3.0 or higher	Performance Assessment

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

Needs	Efficient and effective in meeting requirements Meets technical needs and mission requirements Offers quality services/products		
2. Project Milestones and Schedule	Quick response capability Products completed, reviewed, delivered in timely manner Notifies customer in advance of potential problems	Achieve 3.0 or higher	Performance Assessment
3. Project Staffing	Currency of expertise Personnel possess necessary knowledge, skills and abilities to perform tasks	Achieve 3.0 or higher	Performance Assessment
4. Value Added	Provided valuable service to Government Services/products delivered were of desired quality	Achieve 3.0 or higher	Performance Assessment

The COR may 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.

Detailed Performance Metrics shall be identified in the individual DOs.

The Contractor shall comply with IEEE 1680 "Standard for Environmental Assessment of Personal Computer Products"—also known as the EPEAT—the first U.S. standard that provides guidelines for identifying environmentally friendly desktop and laptop computers and monitors. For more detailed information on the EPEAT criteria, visit <http://www.epeat.net/>. All End-User Devices (PWS section 6.1) provided under this contract, with the exception of docking stations, shall be rated EPEAT "Silver" or higher. Equipment provided on this contract is required to comply with EPA disposal standards.

13.5 FACILITY/RESOURCE PROVISIONS

The Government may provide system access when authorized contract staff work at a Government location as required according to individual DOs 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.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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 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 ISO and Privacy Officer.

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath (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 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.

13.6 SHIPMENT OF HARDWARE OR EQUIPMENT

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

Inspection: Destination

Acceptance: Destination

Free on Board (FOB): Destination

Ship To and Mark For: To Be Determined Per each DO

	Primary		Alternate
Name:	_____	Name:	_____
Address:	_____	Address:	_____
Voice:	_____	Voice:	_____
Email:	_____	Email:	_____

Special Shipping Instructions:

Prior to shipping, Contractor shall notify and obtain concurrence from the Site POCs, by phone followed by email, of all incoming deliveries including line-by-line details for review of requirements. The subject of the notification email(s) shall include the IFCAP Purchase Order (PO) number and project title. The following email address shall be carbon copied on the notification email(s): VAITAAGRILOS@va.gov. Contractor cannot make any changes to the delivery schedule at the request of Site POC; any and all changes shall only be authorized by the Contracting Officer identified within the DO. Following shipment, the Contractor shall provide tracking information to the site POCs, VA Program Manager, CO, and Contract Specialist identified therein.

All VA shipments, either single or multiple container deliveries, shall bear the VA IFCAP Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA IFCAP PO number shall indicate total number of containers for the complete shipment (e.g. "Package 1 of 2"), clearly readable on manifests and external shipping labels. The pallets / containers shall be packaged or shipped in a manner easiest for receiving personnel to read the package labels without having to break the pallet(s) down to gain access to scan the labels. A copy of the master shipping manifest shall be attached to the first package or pallet in the series of the shipment (for example: "box 1 of 5" or "pallet 1 of 5").

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

IFCAP PO #: _____ (to be completed at time of DO award)

Project Description: (e.g. Tier I Lifecycle Refresh)

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

Special Shipping Instructions for National Acquisitions:

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

1 Master Delivery Schedule

2
3 The Contractor shall complete the Master Delivery Schedule in accordance with the
4 Instructions, and shall coordinate with the COR for specifics. The Master Delivery
5 Schedule shall be provided after award and updated prior to and after each delivery
6 timeframe.
7

8 Shipment/Delivery Kick-off Meeting

9
10 The Contractor shall conduct a Shipment/Delivery Kick-off Meeting with the Government
11 PM, COR, Delivery Date Coordinator, Implementation Manager, and Facility Chief
12 Information Officers (CIOs) (or designee) to discuss delivery schedule requirements and
13 facilitate delivery of equipment. This meeting may be held in conjunction with the post
14 award conference or identified technical kickoff meeting. The Contractor shall also
15 present the Shipment/Delivery Weekly Progress Report format for review and approval
16 by the Government. This meeting, if held independently, shall be conducted
17 telephonically within ten days after award and shall incorporate any delivery schedule
18 changes to the draft Delivery Schedule identified by the Government.
19

20 Deliverables:

- 21
22 A. Master Delivery Schedule
23 B. Shipment/Delivery Weekly Progress Report
24

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate Local Area Network (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 GFE and 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 ISO must be notified and verify all security requirements have been adhered to.

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

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at <https://www.tms.va.gov>. If you do not have a TMS profile, go to <https://www.tms.va.gov> and click on the "Create New User" link on the TMS to gain access.

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

A2.0 VA Enterprise Architecture Compliance

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

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

A2.1. VA Internet and Intranet Standards

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

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

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

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

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

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

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

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

- ☒ § 1194.21 Software applications and operating systems
- ☒ § 1194.22 Web-based intranet and internet information and applications
- ☒ § 1194.23 Telecommunications products
- ☒ § 1194.24 Video and multimedia products
- ☒ § 1194.25 Self contained, closed products
- ☒ § 1194.26 Desktop and portable computers
- ☒ § 1194.31 Functional Performance Criteria
- ☒ § 1194.41 Information, Documentation, and Support

A3.2. Equivalent Facilitation

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

A3.3. Compatibility with Assistive Technology

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

A3.4. Acceptance and Acceptance Testing

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

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

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

Deliverable:

- A. Final Section 508 Compliance Test Results

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

A4.0 Physical Security & Safety Requirements:

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

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

A5.0 Confidentiality and Non-Disclosure

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

- request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
 4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
 5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
 6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
 7. Contractor must adhere to the following:
 - a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
 - b. Controlled access to system and security software and documentation.
 - c. Recording, monitoring, and control of passwords and privileges.
 - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
 - e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
 - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
 - g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

- 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. Base on Individual DO VA Form 0752 may be required by the 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 EPEAT registered products in providing information technology products and/or services.

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

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements. The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.
3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Silver registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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. If products not included on this list become subject to EPEAT, the Contractor shall submit an ECP for an EPEAT compliant product if the existing product on contract does not meet the established EPEAT standards.

The Contractor shall provide the Government a monthly EPEAT report which details the products delivered and the corresponding EPEAT rating of those products. The Government will provide the template for the EPEAT report at the Contractor Post Award Conference.

Deliverable:

- A. EPEAT Report

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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 Contractor/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 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.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

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

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

MOU-ISA for system interconnection, the Contractor/Subcontractor must complete a 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 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,

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

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.

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.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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 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 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

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

1 of the information system, or systems by or on behalf of VA. These security controls are
2 to be assessed and stated within the PIA and if these controls are determined not to be
3 in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted
4 and approved prior to the collection of PII.

5
6 c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of
7 systems or network operations, telecommunications services, or other managed
8 services requires A&A of the Contractor's systems in accordance with VA Handbook
9 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information*
10 *Systems* and/or the VA OCS Certification Program Office. Government-owned
11 (Government facility or Government equipment) Contractor-operated systems, third
12 party or business partner networks require MOU-ISA which detail what data types are
13 shared, who has access, and the appropriate level of security controls for all systems
14 connected to VA networks.

15
16 d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and
17 NIST standards related to the annual FISMA security controls assessment and review
18 and update the PIA. Any deficiencies noted during this assessment must be provided to
19 the VA CO and the ISO for entry into the VA POA&M management process. The
20 Contractor/Subcontractor must use the VA POA&M process to document planned
21 remedial actions to address any deficiencies in information security policies,
22 procedures, and practices, and the completion of those activities. Security deficiencies
23 must be corrected within the timeframes approved by the Government.
24 Contractor/Subcontractor procedures are subject to periodic, unannounced
25 assessments by VA officials, including the VA Office of Inspector General. The physical
26 security aspects associated with Contractor/Subcontractor activities must also be
27 subject to such assessments. If major changes to the system occur that may affect the
28 privacy or security of the data or the system, the A&A of the system may need to be
29 reviewed, retested and re-authorized per VA Handbook 6500.3. This may require
30 reviewing and updating all of the documentation (PIA, System Security Plan, and
31 Contingency Plan). The Certification Program Office can provide guidance on whether a
32 new A&A would be necessary.

33
34 e. The Contractor/Subcontractor must conduct an annual self-assessment on all
35 systems and outsourced services as required. Both hard copy and electronic copies of
36 the assessment must be provided to the COR. The Government reserves the right to
37 conduct such an assessment using Government personnel or another
38 Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and
39 timely action (this can be specified in the contract) to correct or mitigate any
40 weaknesses discovered during such testing, generally at no additional cost.

41
42 f. VA prohibits the installation and use of personally-owned or
43 Contractor/Subcontractor owned equipment or software on the VA network. If non-VA
44 owned equipment must be used to fulfill the requirements of a contract, it must be
45 stated in the service agreement, SOW or contract. All of the security controls required
46 for GFE must be utilized in approved OE and must be funded by the owner of the

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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
- 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.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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.

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.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

- 1) Nature of the event (loss, theft, unauthorized access);
- 2) Description of the event, including:
 - a) date of occurrence;
 - b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- 3) Number of individuals affected or potentially affected;
- 4) Names of individuals or groups affected or potentially affected;
- 5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- 6) Amount of time the data has been out of VA control;
- 7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
- 8) Known misuses of data containing sensitive personal information, if any;
- 9) Assessment of the potential harm to the affected individuals;
- 10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
- 11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

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 (1) year of credit monitoring services consisting of automatic daily monitoring of at least three (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 (1) 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

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-days' notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

- a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

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

TAC Number: **TAC-18-44158**

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 two (2) calendar days of the initiation of the contract and annually thereafter, as required.

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

SCHEDULE FOR DELIVERABLES

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

Task	Deliverable ID	Deliverable Description
5.1.1	A	Post Award Conference Report Due ten (10) days after conclusion of the Contract Post Award Conference Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.1	B	Initial Draft Contract Level Work Plan and Schedule Due within ten (10) business days after contract award or at the Contract Post Award Conference Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.3	A	Quarterly Program Review Reports Due ten (10) days after conclusion of the Program Review Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.3	B	Updated Contract Level Work Plan and Schedule Due ten (10) days after conclusion of the Program Review Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.4	A	Contractor Project Management Plan and Updates Due ten (10) days after award of DO and updated semi-annually thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.5	A	Monthly Progress Report Due the fifth (5th) day of each month throughout the period of performance (PoP). Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination
5.1.6	A	Weekly Progress Report Due two (2) weeks after award of the DO and updated weekly until final delivery Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination
5.1.7		CEC-NG Product Catalog Due within ten (10) business days after contract award Electronic submission to: VA PM, COR, CO and uploaded to the ITSM Portal and Contractor-hosted Portal. To be updated following each Government-approved Technology Refresh, Technology Insertion, and Technology Retirement ECP. Inspection: destination Acceptance: destination

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: **TAC-18-44158**

Task	Deliverable ID	Deliverable Description
5.1.7.1	A	ITSM Portal Information Updated information due within twenty-four (24) hours of any change to the tracking information including delivery and maintenance of the products. Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination
5.1.8	A	Change Management Plan Due thirty (30) days after contract (DAC) and updated monthly thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.8	B	Emergency Engineering Change Proposals Due two (2) days after discovery of uncorrectable interoperability problem for a product Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.9	A	Technology Refresh Engineering Change Proposals Due no less than ninety (90) days prior to the EOL and/or EOS date of a product. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.19	B	CEC-NG Products Review Report Due ninety (90) days after DAC and updated quarterly throughout the PoP Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.10	A	Technology Insertion Engineering Change Proposals Due anytime throughout the PoP Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
13.2	A	Contractor Staff Roster Due three (3) business days after contract award and updated quarterly throughout the PoP. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
13.2	B	Optional Form 306 Due five (5) business days after contract award and updated quarterly throughout the PoP. Electronic submission to: COR Inspection: destination Acceptance: destination
13.2	C	Self-Certification of Continuous Service Due five (5) business days after contract award and updated quarterly throughout the PoP. Electronic submission to: COR Inspection: destination Acceptance: destination

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

Task	Deliverable ID	Deliverable Description
13.2	D	VA Form 0710 Due five (5) business days after contract award and updated quarterly throughout the PoP. Electronic submission to: COR Inspection: destination Acceptance: destination
13.2	E	Completed SIC Fingerprint Request Form Due five (5) business days after contract award and updated quarterly throughout the PoP. Electronic submission to: COR Inspection: destination Acceptance: destination
13.6	A	Master Delivery Schedule Initial due at Shipment/Delivery Kickoff Meeting, Updates due five (5) days after Shipment/Delivery Kickoff Meeting and updated at each delivery Electronic submission to: VA PM, COR, CO, Facility CIO, Implementation Manager, Delivery Date Coordinator. Inspection: destination Acceptance: destination
13.6	B	Shipment/Delivery Weekly Progress Report Due five (5) days after Shipment/Delivery Kickoff Meeting and updated Weekly Electronic submission to: VA PM, COR, CO, Facility CIO, Implementation Manager, Delivery Date Coordinator. Inspection: destination Acceptance: destination
A3.4	A	Final Section 508 Compliance Test Results Due upon delivery of each deliverable Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

POINTS OF CONTACT:

VA Program Manager:

Name: TBD

Address: TBD

Voice: TBD

Email: TBD

Contracting Officer's Representative:

Name: TBD

Address: TBD

Voice: TBD

Email: TBD

Contracting Officer:

Name: Robert Kirzow

Address: 23 Christopher Way, Eatontown NJ 07724

Voice: 732-795-1017

Commodities Enterprise Contract (CEC) – Next Generation (NG)

TAC Number: TAC-18-44158

Email: Robert.Kirzow@va.gov

Additional POCs related to the Master Delivery Schedule for National Acquisitions will be based on individual DOs

Facility CIO

Name:

Address:

Voice:

Email:

Implementation Manager

Name:

Address:

Voice:

Email:

Delivery Date Coordinator

Name:

Address:

Voice:

Email: