PRODUCT DESCRIPTION

DEPARTMENT OF VETERANS AFFAIRS

Office of Information and Technology
Connectivity & Collaboration Services (CCS)

National Local Exchange Carrier Services for the Enterprise
Next Generation
Service Order XX
Date: June 16, 2026
Force Order: (VA-26-00076053)
PD Version Number: XX

DRAFT

Contents

CONTENTS

1.0 PRODUCT REQUIREMENTS 4
1.1 SERVICE TYPES AND FEATURES, DELIVERY METHODS, AND QUANTITIES 4
This Task Order includes the following service and featured quantities: 4
2.0 Performance Details 6
2.1 PERIOD OF PERFORMANCE 6
2.2 Type of Contract 7
2.3 Place of Performance 7
3.0 SPECIFIC TASKS AND DELIVERABLES 7
3.1 Meeting requirements 8
3.1.1 PROGRAM PROGRESS REVIEWS 8
3.2 Recurring voice services 9
3.2.1 SERVICE TYPES AND FEATURES 9
4.0 PROJECT MANAGEMENT 10
4.1 TASK Order KiCKOFF Meeting 10
5.0 TRANSITION-IN OF SERVICES AND LOCATIONS 10
6.0 SITE INVENTORY OF LINES AND CIRCUITS 11
7.0 TRANSITION-OUT OF SERVICES AND LOCATIONS 11
8.0 SERVICE LEVEL AGREEMENT (SLA) 12
8.1 CONTRACTOR CUSTOMER SUPPORT 12
8.2 MEAN TIME TO REPAIR (MTTR) 13
8.3 PRIORITY 1– SERVICE OUTAGE 13
8.4 PRIORITY 2– SERVICE DEGRADED 14
8.5 EXCLUSIONS 14
8.6 MAINTENANCE PERFORMACE 14
8.7 PERFORMANCE METRICS 15
8.8 TROUBLE ISOLATION CHARGES 16
8.9 Account Records and Reporting 16
9.0 SPECIAL CONSIDERATIONS 16
10.0 Task Order Modifications and Administration 17
11.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) PROCUREMENTS (SECTION 508) 17
11.1 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS 18
11.2 COMPATABILITY WITH ASSISTIVE TECHNOLOGY 18
11.3 ACCEPTANCE AND ACCEPTANCE TESTING 18
12.0 INFORMATION TECHNOLOGY USING SUSTAINABLE PRODUCTS AND SERVICES 18

DRAFT

13.0 SHIPMENT OF HARDWARE OR EQUIPMENT 19
13.1 SPECIAL SHIPPING INSTRUCTIONS 19
13.2 NATIONAL ACQUISITIONS 19
14.0 GENERAL REQUIREMENTS 20
14.1 VA TECHNICAL REFERENCE MODEL 20
14.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS 20
14.3 SOCIAL SECURITY NUMBER (SSN) REDUCTION 20
14.4 INTERNET PROTOCOL VERSION 6 (IPV6) 21
14.5 TRUSTED INTERNET CONNECTION (TIC) 21
ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/ PRIVACY LANGUAGE 22

DRAFT

1.0 PRODUCT REQUIREMENTS

The Contractor is required to deliver Local Exchange Carrier Services and Features as outlined in paragraph 5.4 of the National Local Exchange Carrier Services for the Enterprise Next Generation Attachment B PWS. These services are for the Service Delivery Points (SDPs) specified in the attached workbooks, which encompass various locations throughout the Enterprise.

No changes to services or features may be applied to this requirement except as approved by the Contracting Officer or designated Office of Information & Technology Solution Delivery/Infrastructure Engineering or Provisioning representative.

1.1 SERVICE TYPES AND FEATURES, DELIVERY METHODS, AND QUANTITIES

This Task Order includes the following service and featured quantities:

Service Types and Features	Quantity
5.3 Site Inventory	
5.4.1.1 POTS Line Measured Rate (includes extended calling area)	
5.4.1.1 POTS Line Flat Rate	2645
5.4.1.1 POTS Line Ground Start Flat Rate	
5.4.1.2 Centrex Line	
5.4.1.3 T-1 DSS	
5.4.1.4 PRI (mileage/station link included)	422
5.4.1.5 DID/DOD (Blocks of 20)	1399
5.4.1.6 Session Initiated Protocol Trunking Session	
5.4.1.6 SIP Seat/TN	
5.4.1.7 Metro Ethernet 1.5Mbps	
5.4.1.7 Metro Ethernet 2Mbps	
5.4.1.7 Metro Ethernet 3Mbps	
5.4.1.7 Metro Ethernet 5Mbps	
5.4.1.7 Metro Ethernet 10Mbps	
5.4.1.7 Metro Ethernet 20Mbps	
5.4.1.7 Metro Ethernet 30Mbps	
5.4.1.7 Metro Ethernet 40Mbps	
5.4.1.7 Metro Ethernet 50Mbps	
5.4.1.7 Metro Ethernet 60Mbps	
5.4.1.7 Metro Ethernet 70Mbps	
5.4.1.7 Metro Ethernet 80Mbps	
5.4.1.7 Metro Ethernet 90Mbps	
5.4.1.7 Metro Ethernet 100Mbps	
5.4.1.7 Metro Ethernet 200Mbps	
5.4.1.7 Metro Ethernet 300Mbps	
5.4.1.7 Metro Ethernet 400Mbps	
5.4.1.7 Metro Ethernet 500Mbps	

DRAFT

5.4.1.7 Metro Ethernet 1000Mbps	
5.4.1.8 MPLS Metro Ethernet 30Mbps	
5.4.1.8 MPLS Metro Ethernet 40Mbps	
5.4.1.8 MPLS Metro Ethernet 50Mbps	
5.4.1.8 MPLS Metro Ethernet 60Mbps	
5.4.1.8 MPLS Metro Ethernet 70Mbps	
5.4.1.8 MPLS Metro Ethernet 80Mbps	
5.4.1.8 MPLS Metro Ethernet 90Mbps	
5.4.1.8 MPLS Metro Ethernet 100Mbps	
5.4.1.8 MPLS Metro Ethernet 200Mbps	
5.4.1.8 MPLS Metro Ethernet 300Mbps	
5.4.1.8 MPLS Metro Ethernet 400Mbps	
5.4.1.8 MPLS Metro Ethernet 500Mbps	
5.4.1.8 MPLS Metro Ethernet 600Mbps	
5.4.1.8 MPLS Metro Ethernet 700Mbps	
5.4.1.8 MPLS Metro Ethernet 800Mbps	
5.4.1.8 MPLS Metro Ethernet 900Mbps	
5.4.1.8 MPLS Metro Ethernet 1000Mbps	
5.4.1.9 Circuit Mileage	
5.4.1.10 Caller ID feature POTS Line	389
5.4.1.10 Caller ID feature PRI Circuit (23B+D)	96
5.4.1.11 Three Way Calling feature (POTS Line)	76
5.4.1.12 Call Forward feature (POTS Line)	124
5.4.1.12 Call Forward Busy feature (POTS Line)	5
5.4.1.12 Call Forward No Answer feature (POTS Line)	4
5.4.1.13 Call Wait feature (POTS Line)	
5.4.1.14 Voicemail feature (POTS Line)	19
5.4.1.15 Call Block feature (POTS Line)	714
5.4.1.16 Call Hunting/Roll over feature (POTS Line)	279
5.1.4.17 Call Redirect feature (POTS Line)	2
5.4.1.18 Third Party Billing Block feature (POTS Line)	
5.4.1.19 PIC/LPIC provisioning charge by LEC (per telephone number)	
5.4.1.20 TSP installation (per location)	
5.4.1.20 TSP (provisioning service)	
5.4.1.20 TSP (restoral service)	
5.4.1.21 PS/ALI service installation (per location)	
5.4.1.21 PS/ALI service (MRC)	17
5.4.1.22 HSI/DSL 1.5Mbps (standalone)	
5.4.1.22 HSI/DSL 3-7Mbps (standalone)	
5.4.1.22 HSI/DSL 12-40Mbps (standalone)	
5.4.1.22 HSI/DSL up to (1000Mbps) (standalone)	
5.4.1.22 HSI/DSL (1.5Mbps)	
5.4.1.22 HSI/DSL (3- 7Mbps)	
5.4.1.22 HSI/DSL (12-40Mbps)	
5.4.1.22 HSI/DSL Static IP address	

DRAFT

5.4.1.23 Additional Directory Listing	
5.4.1.24 Non-Published Number	268
5.4.1.25 Emergency Call Routing	
5.4.1.25 Emergency Call Routing (additional Number)	
5.4.1.26 Remote Call Forward (No physical connection)	
5.4.1.27 Remote Access to Call Forward	
5.4.1.27 Remote Access to Call Forward (additional paths)	
5.4.1.28 Call Redirect (must include Screening Removal for VCL)	1
5.4.1.29 Call Screening Removal (must include Call Redirect for VCL)	1
5.4.1.30 Anonymous Call Reject	
5.4.1.31 Long Distance Service Switched Access (Annual approx.)	
5.4.1.31 Long Distance Service Dedicated Access (Annual approx.)	
5.4.1.32 Long Distance Service International Access (Annual approx.)	
5.4.1.33 Toll Free Service - Dedicated (TFS)	
5.4.1.33 Toll Free Service - Switched (TFS)	

Please be advised that each quantity identified in the Table above represents the total quantity required for each of the corresponding LEC services required herein, across the enterprise, during the base period of performance. Attachment 1 details how the above-identified total quantities are comprised; and specifies the exact quantity, for each LEC service, required at each SDP. Any option period exercised will be for a continuation of the same services, in the same quantities, and to the same SDPs, as provided within the base period of performance.

2.0 PERFORMANCE DETAILS

2.1 PERIOD OF PERFORMANCE

The period of performance for this task order shall be as follows:

Transition-In	TBD
Base Period	TBD
Option Period One	
Option Period Two	
Option Period Three	
Option Period Four	

DRAFT

2.2 TYPE OF CONTRACT

2.3 PLACE OF PERFORMANCE

3.0 SPECIFIC TASKS AND DELIVERABLES

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 workday after the weekend or holiday.

Attch B PWS Tasks	Deliverable ID	Deliverable Description
5.1.1	A	**Quarterly Task Order Status Report** Due 5 days after Task Order award and updated Quarterly Inspection: destination Acceptance: destination
5.1.2	A	**Implementation Report** Weekly Status. Inspection: destination Acceptance: destination
5.2.1	A	**Kickoff minutes** Due 5 days after Kickoff meeting Inspection: destination Acceptance: destination
5.2.1	A	**Work Plan** 10 days after award Inspection: destination Acceptance: destination
5.2.1	A	**Transition In Plan** 10 days after award Inspection: destination Acceptance: destination
5.2.1	A	**Notification of Successful Transition-In Completion** 90 Days after Contract Award Inspection: destination Acceptance: destination
5.2.1	A	**Inventory of Lines and Circuits** 90 Days after Contract award Inspection: destination Acceptance: destination

DRAFT

Attch B PWS Tasks	Deliverable ID	Deliverable Description
5.2.1	A	**Monthly Cutover Report** Inspection: destination Acceptance: destination
5.2.2	A	**Program Progress Review** Due 90 Days after Contract award Inspection: destination Acceptance: destination
5.3	A	**Task Order Site Inventory Report** Due 5 Days after Site Visit Inspection: destination Acceptance: destination
5.6.1	A, B, C	**CONTRACTOR CUSTOMER SUPPORT** Due 14 Days after Contract award Inspection: destination Acceptance: destination

3.1 MEETING REQUIREMENTS

For successful management and contract surveillance, the following reviews are required.

3.1.1 PROGRAM PROGRESS REVIEWS

The Contractor shall conduct Program Progress Reviews (PPR) for Government personnel at a mutually agreeable facility (meeting can be virtual). The Contracting Officer (CO)/Contract Specialist (CS) or the Contracting Officer Representative (COR) will schedule the initial PPR. It is anticipated the first PPR will occur no later than 90 calendar days after the date of contract award. Thereafter, PPRs shall occur quarterly, for the life of the contract. During each PPR, the Contractor shall present material that addresses:

1. Status of current services
2. Activities determined to be of importance to VA, such as unanticipated problems
3. Status of significant issues
4. How issues are to be resolved by VA or Contractor

The Contractor shall produce and distribute the PPR meeting minutes identifying the key discussion points and action items. The Contractor shall deliver the PPR meeting minutes to the COR within five business days after the PPR.

DRAFT

3.2 RECURRING VOICE SERVICES

The Contractor shall provide LEC telecommunication voice services as listed in section 1.1. This is based on services currently in place and where commercially available.

3.2.1 SERVICE TYPES AND FEATURES

The Contractor shall provide the service types required as listed on the SDP.

3.2.1.1 SERVICE TYPES

3.2.1.2 SERVICE FEATURES

3.2.2 LOCAL TELECOMMUNICATIONS FEATURES

Features that are not commercially available must be noted in the response. This may include call forwarding, call waiting, voice mail, conference calling, and call blocking as examples.

3.2.3 TELECOMMUNICATION AVAILABILITY

The Contractor shall provide telecommunication services 24 hours per day, seven days per week, 365 days per annum. The Contractor shall adhere to all Public Utilities Commission (PUC) Agreements that regulate the area of service. The PUC shall be the primary ombudsman for regulated services. Government LEC services requirements and conditions may be more stringent than PUC regulations and both may apply. All Contractors and their subcontractors must be recognized and regulated by the PUC in the area that the Contractor offers service. Rate and service schedules must comply with both Federal Communications Commission (FCC) and PUC rules. LEC service providers must have their own facilities in the network fully or in part. Best effort service shall not be accepted. The Government requires telephone service portability and that established telephone numbers be retained.

3.2.4 TELECOMMUNICATIONS SERVICE PRIORITY

The Contractor shall comply with the assignment of a Telecommunications Service Priority (TSP) to all circuits ordered. TSP is a program that authorizes National Security and Emergency Preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits or other telecommunications services as a result of hurricanes, floods, earthquakes, and other natural or man-made disasters (see http://tsp.ncs.gov). The TSP Program requires service vendors to prioritize requests by identifying those services critical to NS/EP based on the Federal Communications Commission (FCC) mandate (REF: 88-341). A TSP assignment ensures that it shall receive priority attention by the service vendor before any and all non-TSP service. The Contractor shall ensure that the Department of Veterans Affairs is the customer of record.

3.2.5 E-911 PS/ALI AVAILABILITY

The Contractor shall comply with all applicable local and FCC regulatory requirements including Local Number Portability (LNP), directory assistance, and emergency services

DRAFT

(911 or E911) requirements to identify the location of an originating station and route them to the appropriate Public Safety Answering Point (PSAP).

4.0 PROJECT MANAGEMENT

The Contractor shall provide project management as follows:

4.1 TASK ORDER KICKOFF MEETING

The Contractor shall hold a Task Order Kickoff Meeting within ten (10) business days after any award. At a minimum, the Contractor shall present, for review and approval by the Government, a Work Plan that details the intended approach and project schedule for the installation of all services required in Section 1.1 (Service Types and Features, Delivery Methods, and Quantities), within the designated Transition-In Period. A copy of the Work Plan shall be provided to the Government one (1) calendar day before the Kickoff Meeting. Dates, locations (can be virtual), and agenda for the Task Order Kickoff Meeting shall be provided to, and confirmed by, the Government at least five (5) calendar days prior to the Task Order Kickoff Meeting. At a minimum, the Contracting Officer (CO), Contract Specialist (CS), Contracting Officer's Representative (COR), and VA Program Manager (PM) shall be invited. The Contractor shall produce and distribute the Task Order Kickoff Meeting Minutes, identifying the key discussion points and action items, to the Government within five (5) business days after the conclusion of the Task Order Kickoff Meeting. The Contractor is hereby advised and understands that any Work Plan approved by the Government shall be incorporated into the Contract and thereby serve as the firm delivery schedule for service installation during the Transition-In Period.

Deliverable:

A. Task Order Kickoff Meeting Minutes
B. Work Plan

5.0 TRANSITION-IN OF SERVICES AND LOCATIONS

The Contractor shall ensure the successful transition (i.e., installation and a cutover) of all services required in Section 1.1 (Service Types and Features, Delivery Methods, and Quantities) within the designated Transition-In Period. During the Transition-In Period, the Contractor shall take all necessary steps to assume full responsibility of all required services at each SDP by the end of the Transition-In Period; this includes, taking all actions necessary to transition the services required hereunder from the current service provider identified in Attachment 2, Tab "SDP," Column "Current Provider." The Contractor shall have thirty (30) calendar days from date of any award to develop and deliver to the Government a Transition-In Plan that describes both an installation and a cutover plan, for Government approval. The Transition-In Plan shall include a listing of

DRAFT

tasks the Contractor must execute for the successful transition-in of all SDPs identified within Attachment 2, to include identifying the Contractor's installation and cutover approaches. The Contractor shall not commence installation and cutover until the

Contractor receives acceptance of the Transition-In Plan, in writing, from the Government. Deviations from the Transition-In Plan shall be coordinated and approved by the Government prior to any work being accomplished in/at the affected area. The Contractor shall coordinate with the Government to ensure all circuits and services are transitioned. Upon successful installation and cutover of all services at each SDP, notification of transition-in completion shall be provided, in writing, to the Government within the Transition-In Period. The Contractor is hereby advised and understands that any Transition-In Plan approved by the Government shall be incorporated into the Contract and thereby serve as the Contractor's firm methodology and delivery schedule relative to the installation and cutover of all services for all SDPs during the Transition-In Period.

Deliverables:

A. Transition-In Plan
B. Notification of successful transition-in completion

6.0 SITE INVENTORY OF LINES AND CIRCUITS

In accordance with NLEC-NG PWS Section 5.3 (Site Inventory), the Contractor shall complete an inventory of all lines and circuits provided by the Contractor upon successful transition-in of services. The inventory shall include the demarcation binding post assignments, the local and long-haul circuit identification, and the Network Interface (NI) location for each of the SDPs specified in Attachment 2. The Contractor shall submit the baseline inventory data to the Government no later than 15 business days after notification of successful transition-in completion.

Deliverables:

A. Site Inventory of Lines and Circuits

7.0 TRANSITION-OUT OF SERVICES AND LOCATIONS

In the event that a new and subsequent contract for like-kind services is not awarded to the Contractor, the Contractor shall not only ensure continuity of all required services and deliverables through the end of the performance period, but simultaneously work with the Government and the successful awardee of any subsequent action so to guarantee a successful transition of services at each SDP. Upon notification from the Government to execute transition-out services, the Contractor shall coordinate with the Government to ensure all circuits and services provided by the Contractor in

DRAFT

accordance with this PD successfully cutover (i.e., are disconnected/discontinued) at the conclusion of performance. The Contractor shall also coordinate with the Government to provide account information for the SDPs and ensure that all circuits and services provided are transitioned-out to any successful awardee of any subsequent action for like-kind services. If transition-out services are required, the Government will notify the Contractor of the time period (phase) for which transition-out services will be conducted (e.g., during the last three (3) months of performance/service). The Contractor shall provide the Government with a monthly report that lists the status of all cutovers. The Monthly Cutover Report shall be provided five (5) calendar days after the conclusion of each month. No physical transition of services may be affected without written government approval.

If a new and subsequent contract for like-kind services is, in fact, awarded to the Contractor, transition-out services and its associated deliverables, will not be required.

Deliverables:

A. Monthly Cutover Report

8.0 SERVICE LEVEL AGREEMENT (SLA)

The Contractor services shall conform to SLA parameters as defined in the following subtasks. This SLA shall apply from the Government Acceptance Date for the Service to the duration of the Service Term. Satellite, cellular, or other radio services shall not be an acceptable solution.

8.1 CONTRACTOR CUSTOMER SUPPORT

The Contractor shall use an escalation process to resolve customer service issues and provide a single POC for each issue or dispute. The Contractor shall provide the COR an Escalation Process Plan within 14 calendar days after base contract award outlining the specific steps taken to resolve customer service issues. The Escalation Process Plan shall be updated within 30 calendar days after any change of contractor key personnel.

The Contractor shall provide the COR a Customer Support Organization Chart containing employee names, email addresses, and direct phone numbers.

The Contractor shall provide technical Help Desk support. Technical Help Desk support is required 24 hours a day, 7 days a week, and 365 days year. A manned toll-free number shall be designated as the primary help number for VA to call to report a problem and have a Trouble Ticket assigned. Automated answering or ticket automation service shall not be an acceptable solution. The Contractor's customer service representative shall be in the Continental United States (CONUS) and be fluent in

DRAFT

spoken and written English. A Trouble Ticket is the method used by the Government to advise the Help Desk of a perceived fault, including a service outage or a failure to meet an SLA. A unique Trouble Ticket reference number shall be given to the Government representative and used each time the Government calls in to the Help Desk for any fault update or, if appropriate, to inform the Contractor of restoration of the service.

The Contractor shall provide the COR a Monthly Help Desk Report at the completion of each billing cycle. The Help Desk Report shall contain all tickets opened during the billing cycle and shall include a list of trouble ticket numbers and the circuits effected, reporting location, time of trouble ticket report, time of service restoration, and description of fault and resolution of fault.

Deliverable:

A. Escalation Process Plan
B. Customer Support Organization Chart
C. Monthly Help Desk Report

8.2 MEAN TIME TO REPAIR (MTTR)

MTTR is the average time for the Contractor to restore the service during a service outage in a billing month. The SLA for MTTR shall be four (4) hours for outage and 72 hours for service degraded. The Contractor shall provide technical support/resolution during established business hours to assist VA with issues pertaining to the LEC Services in Section 5.4.1. MTTR times begin when the Contractor receives a support request from VA. The Contractor shall respond to VA's support requests according to the following fault classifications.

8.3 PRIORITY 1– SERVICE OUTAGE

A service outage is defined as an unscheduled period in which the service is interrupted and unavailable for use by Customer for 60 or more Unavailable Seconds within a 15-minute period. This includes a business impacting function or service is not available such as loss of dial tone, inability to dial 911, or inability to receive a call on the circuit due to service outages. This shall include total loss of service, or the service is degraded to the extent where the Government is unable to use it. This shall include the inability to receive or transmit data or access critical medical systems due to circuit impairment. The Contractor shall respond to all service outages within four hours. Notifications shall be provided to VA local POC as identified by TO, every business day via telephone until restored. The fault shall not return for seven calendar days, or it shall be considered a continuation of the original service impact.

DRAFT

8.4 PRIORITY 2– SERVICE DEGRADED

Service Degraded means VA's workflow is not seriously affected or limited. The Contractor repair technician shall respond to all Service Degraded reports within four hours. Status notifications shall be provided to VA local POC as identified by TO, every business day via telephone until restored. The fault shall not return for 30 calendar days, or it shall be considered a continuation of the original fault.

8.5 EXCLUSIONS

During scheduled maintenance of the LEC Service, the Contractor shall notify VA COR/PM within three business days of the maintenance window and describe in detail how long and to what level degraded service is to be expected. The Contractor shall obtain approval in advance from the appropriate VA POC as identified by TO before scheduled maintenance occurs. The voice service shall not be unavailable for any outage that results from any maintenance performed by the Contractor as defined by the following three exceptions:

1. VA is notified at least three business days in advance of outage or service degradation;
2. During the installation period; or
3. Trouble beyond the demarcation point or Network Interface (NI) not caused by the Contractor.

8.6 MAINTENANCE PERFORMACE

The Contractor shall obtain the approval of the VA Facility Telecommunications Manager (TM) prior to starting any work that will cause a service outage (refer to PWS Section 5.4.2.1). The Contractor shall notify the COR and VA Facility TM, if work needs to be performed outside of normal business hours, a minimum of three business days before the work is to begin (except in the case of Trouble Ticket repair). The Contractor shall receive approval from the VA Facility TM prior to commencement of either intrusive testing or contractor actions which may affect service quality.

Service charges for trouble beyond the demarcation point not caused by the Contractor (refer to PWS Section 5.4.2.1) shall be charged to the Government at the rates established by the State PUC. These charges may include a Trouble Isolation Charge (TIC) as well as charges for time or materials for the purpose of reestablishing the service or clearing the fault.

The Contractor shall clean up all work areas immediately after completing work in VA facilities, including removal and disposal of defective equipment. The Contractor shall place fire-stop materials in conduits and pathways during an installation. Fire-Stop materials must be previously approved by local electrical and building codes. The Contractor shall notify VA when any service request, repair, or maintenance is completed. Notification shall be by telephone call or email to the VA local technical

DRAFT

contact. The service request, repair, or maintenance is not considered complete until a VA Facility Chief Information Officer (CIO) or designee confirms that the completion of service is acceptable.

8.7 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Performance Levels
Transition	No Loss of service.	100% of the time
Account Management	Complete visibility and access to all accounts provided to VA-only, password protected, web-based management portal	100% of the time
Telecommunication Services Restoration	Service restorations are done within 24 hours.	100% of the time
Voice and Data Services and Customer Support	Customer service representative available 24 hours/day, 7 days a week, 365 days a year.	100% of the time
Major Failure Response Time	Contractor responds to major system failures within one hour of notification.	100% of the time
Minor Failure Response Time	Contractor responds to minor system failures within four hours of notification, Monday through Friday, from 8 a.m. to 5 p.m. ET.	99.9% of the time
Service Request Response Time	Qualified technician calls requestor within one hour of a service request.	99.9% of the time
Telecommunication Availability (Uptime)	Telecommunication services are available 24 hours per day, 7 days per week.	99.9% of the time
VA Directive 710 (6.1.1)	The Contractor(s) shall comply with all personnel security requirements included in this contract and local level organization security requirements described in each individual task order. Contractor Technicians will require escorts in VA facilities in accordance with Section 2.h (6) of VA Directive 0710	100% of the time

DRAFT

8.8 TROUBLE ISOLATION CHARGES

When contractor intervention is required to diagnose a fault in service to an SDP covered under any resulting contract, Trouble Isolation Charges (TIC) will apply depending upon where the trouble is isolated. If the trouble condition has been diagnosed to be before the demarcation point, as defined in 47 CFR § 68.3, the Contractor shall assume all costs associated with diagnosing and remedying the issue. However, the Government shall be responsible for TIC when the trouble has been diagnosed to be beyond the demarcation point. Reporting of trouble beyond the demarcation point shall be captured within the "Monthly Help Desk Report" deliverable required by Section 5.6.1 (Contractor Customer Support) of the NLEC-NG PWS. All TIC charges associated with trouble beyond the demarcation point shall be invoiced to the applicable "Trouble Beyond Demarcation" Not to Exceed (NTE) Contract Line Item Number (CLIN) for the applicable period of service.

8.9 ACCOUNT RECORDS AND REPORTING

The Contractor shall provide VA access to customer support and service records. The Contractor shall maintain accurate customer service records. Customer Service Records shall be aggregated by service delivery point with an itemized list of service types provided. Customer Service Records (CSR), the price associated with each service, shall be organized by VA parent facility. All data must have the ability for Electronic Data Interchange (EDI) in a variety of formats, i.e., MS Word, MS Excel, extensible markup language (XML), or other standard formats such as flat-files or text files. The report shall be delivered to the COR or designee by email on or about the same time every month.

9.0 SPECIAL CONSIDERATIONS

As defined in the NLEC-NG PWS at Section 6.1 (POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS), the Contractor shall comply with all personnel security requirements included in the basic contract and local level organization security requirements described below:

The position sensitivity of contractor work to be performed hereunder is designated as low risk and the level of background investigation will be commensurate with the required level of access.

a. All Contractor personnel shall always be escorted by facility Office of Information and Technology (OIT) staff while on station. Contractor staff

will not require PIV badges due to being escorted, however all Contractor-staff will be badged by the facility as a visitor. Contractor staff must check in with the facility OIT Area Manager or LCON as identified in any TO contract resulting from the requirements established herein prior to performing any work or installations.

b. The Contractor shall be responsible for the actions of all personnel provided to work for VA under any resulting contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of any TO contract resulting from this PD, the Contractor shall be responsible for all resources necessary to remedy the incident.

10.0 TASK ORDER MODIFICATIONS AND ADMINISTRATION

Close adherence to specific contract terms is required, and invoices shall only include services clearly captured in any Task Order award resulting from this PD. Invoices shall be submitted in accordance with the requirements established in the NLEC-NG Basic Contract. Separate invoicing of taxes, fees, tariffs and/or other miscellaneous charges is strictly prohibited. All contract-holders are bound by the maximum unit pricing captured in their respective NLEC-NG Basic Contract and all unit prices captured in any award resulting from this PD shall be inclusive of all taxes, fees, tariffs, and/or miscellaneous charges. The Contractor understands and acknowledges that no modifications of any kind to the requirements established herein, to include any and all attachments hereto, shall be made without the express authorization of the cognizant Contracting Officer and formal modification to any resulting contract. The Government shall not be liable, and the Contractor shall bear the sole risk and responsibility, for any work conducted by the Contractor without the express authorization of the cognizant Contracting Officer and formal modification to any resulting contract.

11.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) PROCUREMENTS (SECTION 508)

On January 18, 2017, the Access Board issued a final rule that updated accessibility requirements covered by Section 508 and refreshed guidelines for telecommunications equipment subject to Section 255 of the Communications Act. The final rule went into effect on January 18, 2018. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

DRAFT

11.1 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: Revised 508 Standards and 255 Guidelines (access-board.gov). A single PDF file version of the Revised Section 508 Standards and 255 Guidelines will be supplied upon request or can be obtained from the Access Board website. Federal agencies must comply with the Rehabilitation Act of 1973, as amended.

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

- ☒ E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)
- ☒ E204 Functional Performance Criteria
- ☒ E206 Hardware Requirements
- ☒ E207 Software Requirements
- ☒ E208 Support Documentation and Services Requirements

11.2 COMPATABILITY WITH ASSISTIVE TECHNOLOGY

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

11.3 ACCEPTANCE AND ACCEPTANCE TESTING

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

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

12.0 INFORMATION TECHNOLOGY USING SUSTAINABLE PRODUCTS AND SERVICES

N/A

DRAFT

13.0 SHIPMENT OF HARDWARE OR EQUIPMENT

13.1 SPECIAL SHIPPING INSTRUCTIONS

13.2 NATIONAL ACQUISITIONS

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

Shipment/Delivery Kick-off Meeting

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

Shipment/Delivery Weekly Progress Report

The Contractor shall provide a Shipment/Delivery Weekly Progress Report which shall identify the items shipped, the serial number 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 and provide a description of how the problems were resolved/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 in Microsoft Excel Format and shall clearly identify each serial number of the equipment being delivered with one (1) serial number per cell.

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

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

Task Order #: _____ (e.g., 36C10A25NXXXX (the Task Order number is in block #20 of the SF 1449))
Project Description: (e.g. Service Order XX)

DRAFT

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

Deliverables:

A. Master Delivery Schedule
B. Shipment/Delivery Weekly Progress Report

14.0 GENERAL REQUIREMENTS

14.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall comply with the VA OIT Technical Reference Model (VA TRM). Compliance with the VA TRM is achieved by using only technologies and standards that are listed as approved for use in the VA TRM. The Contractor shall provide all necessary information requested by VA to ensure TRM approval is obtained prior to use on VA's network.

14.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS

VA has established minimum mandatory security requirements and requires that any network connected software system or service must meet the VA Critical Security Controls as outlined in the VA Memorandum, "VA Security Controls", https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010. VA Critical Security Controls identify the minimum mandatory requirements that must be implemented across all VA enterprise infrastructure, cloud computing environments, information systems, networks, and specialized devices (medical devices/systems, special-purpose systems, and research scientific computing devices) that process, store, and/or transmit VA data. Effective July 1, 2025, the Contractor shall implement these VA Critical Security Controls, within any network connected software system or service prior to being authorized for use in the VA. This functional requirement is not negotiable, and Plan of Action & Milestones (POAM) will not be accepted in the event these controls cannot be implemented for new systems. Critical Security Controls are intended to increase VA's security posture and provide security and privacy risk visibility into the VA network and is not a new requirement. The Contractor's failure to maintain these VA Critical Controls after implementation will result in VA discontinuing the use of the system.

14.3 SOCIAL SECURITY NUMBER (SSN) REDUCTION

The Contractor solution shall support the Social Security Number (SSN) Fraud Prevention Act (FPA) of 2017 which prohibits the inclusion of SSNs on any document sent by mail. The Contractor support shall also be performed in accordance with Section 240 of the Consolidated Appropriations Act (CAA) 2018, enacted March 23, 2018, which mandates VA to discontinue using SSNs to identify individuals in all VA information systems as the Primary Identifier. The Contractor shall ensure that any new IT solution discontinues the use of SSN as the Primary Identifier to replace the SSN with the Integrated Control Number (ICN) in all VA information systems for all

DRAFT

individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA Master Person Index (MPI) for identity traits to include the use of the ICN as the Primary Identifier. The Contractor solution may only use a Social Security Number to identify an individual in an information system if and only if the use of such number is required to obtain information VA requires from an information system that is not under the jurisdiction of VA.

14.4 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support IPv6-Only based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020 (https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf). Which defines IPv6-only as the state of an operational system or service when IPv4 protocol functions (addressing, packet forwarding) are not in use. The NIST USGv6 profile defines technical requirements for a product to be capable of operating in IPv6-Only environments. IPv6-Only technology, in accordance with the USGv6 Program ((https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1), NIST Special Publication (SP) 500-267B Revision 1 "USGv6 Profile" (https://doi.org/10.6028/NIST.SP.500-267Br1), and NIST SP 800-119 "Guidelines for the Secure Deployment of IPv6" (https://doi.org/10.6028/NIST.SP.800-119), compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices, applications, and systems shall support all applicable functionality on native IPv6-Only as well as dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g., web, email, DNS, ISP services, etc.) shall support native IPv6-Only and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall support using native IPv6-Only and dual stack (IPv6 / IPv4) for all functionality and operations.

14.5 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M-19-26, "Update to the Trusted Internet Connections (TIC) Initiative" (https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf), VA Directive 6513 "Secure External Connections", and shall comply with the TIC 3.0 Core Guidance Documents, including all Volumes and TIC Use Cases, found at the Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/publication/tic-30-core-guidance-documents.)

1. VA is notified at least three business days in advance of outage or service degradation.

2. During the installation period; or
3. Trouble beyond the demarcation point or Network Interface (NI) not caused by the Contractor.

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

NOTE: In the event of a conflict, VAAR Security Clauses take precedence over the language in this Addendum B.

APPLICABLE SECTIONS FROM: *VA NOTICE 24-12, APRIL 22, 2024, UPDATE TO VA HANDBOOK 6500.6, CONTRACT SECURITY, APPENDIX C VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE*

B1. GENERAL

This entire section applies to all acquisitions requiring any Information Security and Privacy language. Contractors, contractor personnel, Subcontractors and subcontractor personnel will be subject to the same federal laws, regulations, standards, VA directives and handbooks, as VA personnel regarding information and information system security and privacy.

B2. VA INFORMATION CUSTODIAL LANGUAGE

a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter “contract”) unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General. The primary clause used to define computer software license (not data/intellectual property first produced under this Contractor or order) is FAR 52.227-19, Commercial Computer Software License.

b. Information made available to the Contractor by VA for the performance or administration of this contract will be used only for the purposes specified in the service agreement, SOW, PWS, PD, and/or contract. The Contractor shall not use VA information in any other manner without prior written approval from a VA Contracting Officer (CO). The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General.

DRAFT

c. VA information will not be co-mingled with any other data on the Contractor's information systems or media storage systems. The Contractor shall ensure compliance with Federal and VA requirements related to data protection, data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.

d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of Contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The Contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to Contractor and Subcontractor staff associated with the contract) to VA, VA's Office Inspector General (OIG), and/or Government Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.

e. The Contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.

f. The Contractor shall not make copies of VA information except as specifically authorized and necessary to perform the terms of the contract. If copies are made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.

g. If a Veterans Health Administration (VHA) contract is terminated for default or cause with a business associate, the related local Business Associate Agreement (BAA) shall also be terminated and actions taken in accordance with VHA Directive 1605.05, Business Associate Agreements. If there is an executed national BAA associated with the contract, VA will determine what actions are appropriate and notify the contractor.

h. The Contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance with VA Information Security Knowledge Service requirements. The Contractor shall transmit VA sensitive information using VA approved Transport Layer Security (TLS) configured with FIPS based cipher suites in conformance with National Institute of Standards and Technology (NIST) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.

DRAFT

i. The Contractor's firewall and web services security controls, as applicable, shall meet or exceed VA's minimum requirements.

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

k. Notwithstanding the provision above, the Contractor 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 medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the Contractor is in receipt of a court order or other requests for the above-mentioned information, the Contractor shall immediately refer such court order or other requests to the VA CO for response.

l. Information made available to the Contractor by VA for the performance or administration of this contract or information developed by the Contractor in performance or administration of the contract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (IAM) Security processes specified in the VA Information Security Knowledge Service.

m. Any data destruction done on behalf of VA by a Contractor shall be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.

n. The Contractor shall provide its plan for destruction of all VA data in its possession according to VA Directive 6500 and NIST 800-88, Guidelines for Media Sanitization prior to termination or completion of this contract. If directed by the COR/CO, the Contractor shall return all Federal Records to VA for disposition.

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is used to store, process, or access VA information that cannot be destroyed shall be returned to VA. The Contractor shall hold the appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the Contractor shall send via a trackable method (USPS, UPS, FedEx, etc.) and immediately provide the COR/CO with the tracking information. Self-

DRAFT

certification by the Contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.

p. All electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) used to store, process or access VA information will not be returned to the Contractor at the end of lease, loan, or trade-in. Exceptions to this paragraph will only be granted with the written approval of the VA CO.

B3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. *N/A*

B4. TRAINING

a. *N/A*

B5. SECURITY INCIDENT INVESTIGATION

a. The Contractor, Subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711). The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the Contractor, Subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO the incident number received from the ESD.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following:

(1) The date and time (or approximation of) the Security Incident occurred.

(2) The names of individuals involved (when applicable).

(3) The physical and logical (if applicable) location of the incident.

(4) Why the Security Incident took place (i.e., catalyst for the failure).

(5) The amount of data belonging to VA believed to have been compromised.

(6) The remediation measures the Contractor is taking to ensure no future incidents of a similar nature.

c. After the Contractor has provided the initial detailed incident summary to VA, they will continue to provide written updates on any new and relevant

DRAFT

circumstances or facts they discover. The Contractor, Subcontractor, and their employes shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

d. VA IT Contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.

e. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG, and the VA Office of Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

f. The Contractor shall comply with VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.

g. With respect to unsecured Protected Health Information (PHI), the Contractor is deemed to have discovered a data breach when the Contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.

h. If the Contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the Contractor/Subcontractor processes or maintains under the contract; the Contractor shall pay liquidated damages to the VA as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

B6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. *N/A*

B7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE

DRAFT

a. *N/A*

B8. SECURITY AND PRIVACY CONTROLS COMPLIANCE TESTING, ASSESSMENT AND AUDITING

a. *N/A*

B9. PRODUCT INTEGRITY, AUTHENTICITY, PROVENANCE, ANTI-COUNTERFEIT AND ANTI-TAMPERING

a. The Contractor shall comply with Code of Federal Regulations (CFR) Title 15 Part 7, “Securing the Information and Communications Technology and Services (ICTS) Supply Chain”, which prohibits ICTS Transactions from foreign adversaries. ICTS Transactions are defined as any acquisition, importation, transfer, installation, dealing in or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs or the platforming or data hosting of applications for consumer download.

b. When contracting terms require the Contractor to procure equipment, the Contractor shall purchase or acquire the equipment from an Original Equipment Manufacturer (OEM) or an authorized reseller of the OEM. The Contractor shall attest that equipment procured from an OEM or authorized reseller or distributor are authentic. If procurement is unavailable from an OEM or authorized reseller, the Contractor shall submit in writing, details of the circumstances prohibiting this from happening and procure a product waiver from the VA COR/CO.

c. All Contractors shall establish, implement, and provide documentation for risk management practices for supply chain delivery of hardware, software (to include patches) and firmware provided under this agreement. Documentation will include chain of custody practices, inventory management program, information protection practices, integrity management program for sub-supplier provided components, and replacement parts requests. The Contractor shall make spare parts available. All Contractor(s) shall specify how digital delivery for procured products, including patches, will be validated and monitored to ensure consistent delivery. The Contractor shall apply encryption technology to protect procured products throughout the delivery process.

d. If a Contractor provides software or patches to VA, the Contractor shall publish or provide a hash conforming to the FIPS Security Requirements for Cryptographic Modules (FIPS 140-2 or successor).

e. The Contractor shall provide a software bill of materials (SBOM) for procured (to include licensed products) and consist of a list of components and associated metadata which make up the product. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information

DRAFT

Administration (NTIA) report "The Minimum Elements for a Software Bill of Materials (SBOM)."

f. Contractors shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.

g. Throughout the delivery process, the Contractor shall demonstrate a capability for detecting unauthorized access (tampering).

h. The Contractor shall demonstrate chain-of-custody documentation for procured products and require tamper-evident packaging for the delivery of this hardware.

B10. VIRUSES, FIRMWARE, AND MALWARE

a. The Contractor shall execute due diligence to ensure all provided software and patches, including third-party patches, are free of viruses and/or malware before releasing them to or installing them on VA information systems.

b. The Contractor warrants it has no knowledge of and did not insert, any malicious virus and/or malware code into any software or patches provided to VA which could potentially harm or disrupt VA information systems. The Contractor shall use due diligence, if supplying third-party software or patches, to ensure the third-party has not inserted any malicious code and/or virus which could damage or disrupt VA information systems.

c. The Contractor shall provide or arrange for the provision of technical justification as to why any "false positive" hit has taken place to ensure their code's supply chain has not been compromised. Justification may be required, but is not limited to, when install files, scripts, firmware, or other Contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor.

d. The Contractor shall not upload (intentionally or negligently) any virus, worm, malware or any harmful or malicious content, component and/or corrupted data/source code (hereinafter "virus or other malware") onto VA computer and information systems and/or networks. If introduced (and this clause is violated), upon written request from the VA CO, the Contractor shall:

(1) Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware throughout VA's information networks, computer systems and information systems; and
(2) Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

DRAFT

B11. CRYPTOGRAPHIC REQUIREMENT

a. *N/A*

B12. PATCHING GOVERNANCE

N/A

B13. SPECIALIZED DEVICES/SYSTEMS (MEDICAL DEVICES, SPECIAL PURPOSE SYSTEMS, RESEARCH SCIENTIFIC COMPUTING)

N/A

B14. DATA CENTER PROVISIONS

N/A

DRAFT

POINTS OF CONTACT

VA Program Manager:
Name:
Address:
Voice:
Email:
Contracting Officer's Representative:
Name:
Address:
Voice:
Email:
Contracting Officer:
Name: Claudetta Smith
Address: Remote
Voice: 512-981-4135
Email: claudetta.smith@va.gov
Contract Specialist:
Name:
Address:
Voice:
Email:

Facility CIO
Name:TBD
Address:
Voice:
Email:
Implementation Manager
Name:TBD
Address:
Voice:
Email:
Delivery Date Coordinator
Name:TBD
Address:
Voice:
Email:

DRAFT