

**Naval Enterprise Networks (NEN)**

**Solicitation: N00039-18-R-0004**

**End User Hardware (EUHW)**

**Attachment 1, Performance Work Statement (PWS)**

**Final v 1.0**

DATE: 17 September 2018

Program Executive Office Enterprise Information Systems

Program Manager, Naval Enterprise Networks

1325 10th Street, SE, Suite 301

Washington, DC 20374

**UNCLASSIFIED**

Table of Contents

[1. INTRODUCTION 1](#_Toc522712671)

[1.1 DoD Management Domains 1](#_Toc522712672)

[2. SCOPE 2](#_Toc522712673)

[3. REQUIREMENTS 3](#_Toc522712674)

[3.1 Program Management 3](#_Toc522712675)

[3.1.1 Key Personnel 3](#_Toc522712676)

[3.1.2 Risk, Issue, and Opportunity Management 4](#_Toc522712677)

[3.1.3 Governance 5](#_Toc522712678)

[3.1.3.1 NEN Governance Boards 5](#_Toc522712679)

[3.1.3.1.1 Program Management Reviews (PMR) 6](#_Toc522712680)

[3.1.4 Contractor Performance Assessment Reporting System (CPARS) 6](#_Toc522712681)

[3.1.5 Enterprise-Wide Contractor Manpower Reporting Application (ECMRA 6](#_Toc522712682)

[3.2 Service Order Provisioning and Delivery 7](#_Toc522712683)

[3.2.1 Core Build Imaging 7](#_Toc522712684)

[3.2.2 Hardware Peripherals 7](#_Toc522712685)

[3.2.2.1 End User Hardware As-a-Service (EUHWaaS) 8](#_Toc522712686)

[3.2.2.2 Purchased End User Hardware 8](#_Toc522712687)

[3.2.3 Technical Requirements 9](#_Toc522712688)

[3.2.3.1 End User Hardware Device Categorization 9](#_Toc522712689)

[3.2.3.1.1 General Purpose (GP) Desktop/Laptop/Tablet 10](#_Toc522712690)

[3.2.3.1.2 Mid-Range Desktop/Laptop 10](#_Toc522712691)

[3.2.3.1.3 High Performance Desktop/Laptop 10](#_Toc522712692)

[3.2.3.1.4 Rugged Laptop 11](#_Toc522712693)

[3.2.3.1.5 Rugged Tablet 11](#_Toc522712694)

[3.2.3.1.6 2-in-1 Detachable 11](#_Toc522712695)

[3.2.3.1.7 Zero Client or Thin Client 11](#_Toc522712696)

[3.2.3.1.8 Ultra-Small Desktop 12](#_Toc522712697)

[3.2.4 State of the Shelf (SOTS) 12](#_Toc522712698)

[3.2.4.1 EUHW SOTS Definition and Methodology 12](#_Toc522712699)

[3.2.4.2 EUHW SOTS Implementation 13](#_Toc522712700)

[3.2.5 EUHWaaS Device Refresh 14](#_Toc522712701)

[3.2.6 EUHWaaS Deployable Computing 14](#_Toc522712702)

[3.2.7 Service Management of EUHWaaS Devices 15](#_Toc522712703)

[3.2.8 EUHW Service Desk Functionality 16](#_Toc522712704)

[3.2.9 Legacy EUHWaaS Support Services 16](#_Toc522712705)

[3.2.10 EUHWaaS Buy-Back 17](#_Toc522712706)

[3.3 Service Order Management 17](#_Toc522712707)

[3.3.1 Contractor Ordering Application Integration 17](#_Toc522712708)

[3.4 Logistics Management 18](#_Toc522712709)

[3.4.1 Supply Chain Risk Management 18](#_Toc522712710)

[3.4.2 Equipment Recall 19](#_Toc522712711)

[3.4.3 Purchased EUHW Warranty Management 19](#_Toc522712712)

[3.4.4 Asset Management 22](#_Toc522712713)

[3.4.4.1 EUHWaaS Asset Management 23](#_Toc522712714)

[3.4.4.2 Purchased EUHW Asset Management 23](#_Toc522712715)

[3.4.5 Shipping, Packing, Tracking, Handling, Storage, and Transportation Requirements 24](#_Toc522712716)

[3.4.5.1 USMC Purchased EUHW Shipping Requirements 25](#_Toc522712717)

[3.4.6 Hardware Device Return & Disposal 25](#_Toc522712718)

[3.5 Transition Services 25](#_Toc522712719)

[3.6 Program Security 26](#_Toc522712720)

[3.7 Service Level Management 27](#_Toc522712721)

[Appendix A Reference Documents 29](#_Toc522712722)

[Appendix B CDRLs…. 32](#_Toc522712723)

[Appendix C Acronyms 33](#_Toc522712724)

**Tables and Figures**

[Table 3.1.3.1: NEN Governance Entities 5](#_Toc521587963)

[Table 3.2.2: Hardware Peripherals 7](#_Toc521587964)

[Table 3.2.3.1: EUHW Category Matrix 9](#_Toc521587965)

[Figure 3.2.4.1: EUHW State of the Shelf (SOTS) Concept 12](#_Toc521587966)

# INTRODUCTION

The Department of the Navy (DON) operates one of the largest combined networks in the world, comprised of the Navy Marine Corps Intranet (NMCI), the Outside Continental United States (OCONUS) Navy Enterprise Network (ONE-Net), the Marine Corps Enterprise Network (MCEN), and other legacy networks. The NMCI, Government Owned/Contractor Operated (GO/CO) and the MCEN, Government Owned/Government Operated (GO/GO) together provide secure end-to-end Information Technology (IT) services to more than 400,000 hardware devices and 600,000+ users at over 1,600 Continental United States (CONUS) sites and Hawaii, Alaska, and Puerto Rico, as well as the MCEN OCONUS sites, including Germany, Japan, Korea, Guam, Australia, and Bahrain, varying from installations to single user locations. For the Navy, ONE-Net provides equivalent secure end-to-end IT services to nearly 30,000 hardware devices and 45,000+ users across 82 locations within three (3) OCONUS regions based out of Yokosuka, Japan; Manama, Bahrain; and Naples, Italy. ONE-Net is currently managed and operated as a hybrid of GO/CO and GO/GO methodology. See End User Hardware (EUHW) Navy Site Listing (Attachment 6) for more information on locations.

The Naval Networking Environment (NNE) will comprise the NMCI, MCEN, ONE-Net as well as other networks across the DON. Naval Enterprise Networks (NEN) is the DON Program Office that procures services and solutions to satisfy requirements for the NMCI, ONE-Net, and the MCEN. Services provided will be interoperable with, and leverage, other Department of Defense (DoD) net-centric enterprise services.

DoD agencies and other military departments (MILDEPs) may use this contract for EUHW services as described herein.

## DoD Management Domains

DoD agencies/MILDEPs may function within single or multiple management domains separate from DON domains. Specific Government transition plans will be in place prior to work commencing under this contract.

DoD agency/MILDEP management domains will be GO/CO, similar to the Navy Management Domain consuming services as described for the Navy as well as leveraging the same CDRLs and CLIN structure.

# SCOPE

This Contract provides End User Hardware (EUHW) to the Government for the use of unclassified Non-secured Internet Protocol Network Router (NIPRNet) and classified Secret Internet Protocol Network Router (SIPRNet) networks. Legacy EUHW are those end user devices provided as a service under the previous/incumbent Contractor. Legacy EUHW shall be provided and managed by the vendor in an uninterrupted capacity until Phase-in of the new EUHW. All requirements for EUHW also apply to Legacy EUHW, and differ only by listed exceptions in section 3.2.6.1. New EUHW will be either acquired as a service (aaS) or purchased, as described in sections 3.2.2.1 and 3.2.2.2. EUHW includes the following: laptop, desktop, tablet, 2-in-1 detachable, ultra-small desktop, and thin/zero client device. A single EUHW device may support multiple users and their associated accounts. The Contractor shall install the Government-provided core build software image on designated EUHW. Images will include the Marine Corps Enterprise Desktop Standard (MCEDS), NMCI, and ONE-Net images, and any future images provided by other DOD Agency/MILDEPs as Government Furnished Information (GFI).

Service management, integration and transport services will be provided by the Network Manager except for those EUHWaaS services defined herein. The Network Manager will be the Service Management, Integration and Transport (SMIT) contractor for NMCI and ONE-Net; the Network Manager for the MCEN will be defined as either the Government or a contractor in individual task orders.

# REQUIREMENTS

## Program Management

### Key Personnel

The Contractor shall provide, as key personnel, a dedicated Program Manager (PM) and a Contracts Manager for the duration of the Contract. Both key personnel must be approved by the Government’s Procuring Contracting Officer (PCO) and shall meet minimum qualifications as stipulated below. Regarding all key personnel, the Contractor shall coordinate the replacement of such personnel with the Government at least thirty (30) days in advance of turnover.

1. Program Manager shall:
2. Maintain overall programmatic (cost, schedule, performance) responsibility for the execution of the contract and the delivery of EUHW and associated services. Serve as the single point of contact for EUHW-related program and multi-provider coordination-related issues and incidents issues. Communicate critical and time sensitive program-related information directly to the NEN Program Manager, Deputy Program Manager, and other designated Government personnel. Represent the Contractor at program-related meetings attended by, or at the request of, the NEN Program Manager or Deputy Program Manager.
3. Meet the following qualifications:
   1. Ten (10) years of combined experience managing and/or executing the planning, provisioning, and/or delivery of EUHW to organizations with at least 100,000 users across multiple locations. This experience includes managing or executing efforts involving replacement of either end-of-life (EOL) or technically obsolete hardware.
   2. SECRET Department of Defense (DoD) Clearance.
   3. Program Management Professional Certification, Defense Acquisition Workforce Improvement Act (DAWIA) Level III Program Management Certification, or equivalent.
   4. Information Assurance Level III Certifications in accordance with DoDD 8140.01 and DoDD 8570.01-M (Appendix A).
4. Contracts Manager shall:
5. Maintain overall responsibility for contracts management, including providing formal contractual information and notifications, as well as representing the Contractor in any negotiations or modifications to the EUHW Contract, and is the single point of contact for the PCO for all contract-related matters. Represent the Contractor at all contract-related meetings attended by, or at the request of, the PCO or his/her delegates.
6. Meet the following qualifications:
   1. Bachelor's degree from an accredited college or university.
   2. Five (5) years of contract management experience with the Department of Defense. At least three (3) years of experience managing information technology contracts with a total value of $75M (million) annually. This experience includes managing contracting efforts involving replacement of either end-of-life or technically obsolete hardware.
   3. SECRET Department of Defense DoD Clearance.

### Risk, Issue, and Opportunity Management

Risk Management for EUHW provides an organized means of identifying, measuring, and ranking risks and developing, selecting, and managing options for resolving or mitigating those risks. Risk, issue, and opportunity management should be forward-looking, structured, continuous, and informative.

The Contractor shall:

1. Develop, submit, and execute a risk, issue and opportunity management implementation methodology in accordance with the Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, January 2017 (Appendix A). The Contractor shall include this methodology in a Program Management Plan (PMP) (CDRL A201).
2. Document and update the status of Contractor risks, issues and opportunities for inclusion in the Monthly Status Report (MSR) (CDRL A202).

### Governance

NEN has established an Enterprise Governance Model for CONUS/OCONUS incorporated within the NEN Operating Model (Appendix A) Environment. This governance uses decision-making boards/bodies, controls and/or metrics, and standards to ensure the performance of the Service Lifecycle is in compliance with DON requirements. Governance efforts will render decisions to manage risks and ensure service levels and performance measures are met. The NEN Enterprise Governance Model will support a multi-vendor/multi-contract environment. The Contractor shall participate and recommend improvements which align with industry and Government standard frameworks.

#### NEN Governance Boards

NEN has various Program Management Office (PMO) Governance Boards, also referred to as “Governance Entities”, to support the management and delivery of services. The NEN Governance entities which involve the Contractor and the anticipated frequency of convening with those entities are provided in Table 3.1.3.1.

Table 3.1.3.1: NEN Governance Entities

|  |  |  |  |
| --- | --- | --- | --- |
| **NEN GOVERNANCE ENTITY** | **FUNCTION** | **FREQUENCY** | **EUHW PWS Section Reference** |
| Program Management Review (PMR) | Program Review  Decision Making | Semi-Annual | 3.1.3.1.1 |
| Schedule Change Control Board (SCCB) | Decision Making | Monthly | 3.2.5 |

For each NEN Governance Board/ Entity cited in Table 3.1.3.1, the Contractor shall:

1. Prepare for and participate in designated meetings at Government request.
2. Identify and designate the appropriate Subject Matter Experts (SMEs) to attend the meeting(s) and address required agenda items.
3. Follow up on issues with designated Governance POCs and complete action items identified by respective Governance Boards.

##### Program Management Reviews (PMR)

The Contractor shall:

1. Participate in semi-annual PMRs in the Washington, D.C. area, unless otherwise directed by the Government. PMRs will be held jointly with the Network Manager when requested by the Government, to include: an overview of enterprise operations, schedule performance, contract status (including a discussion of open issues and negotiations in process), status of operations, operational metrics and trending, metrics for key projects, and an overall assessment of program risk.
2. Coordinate the Meeting Agenda, Meeting Presentation Material, and Meeting Minutes with the Network Manager.

### Contractor Performance Assessment Reporting System (CPARS)

The Contractor Performance Assessment Reporting System (CPARS) has been established to collect Past Performance information on defense contractors as required by FAR 42.1502 (Class Deviation 2013-O0018).

The Contractor shall submit CPARS reports (initial, intermediate, final, out-of-cycle, and addendum) as required in the CPARS Policy Guide that is available at: <https://www.cpars.gov/pdfs/CPARS-Guidance.pdf>. For orders placed against contracts and agreements the contractor’s performance shall be assessed on a total contract basis.

### Enterprise-Wide Contractor Manpower Reporting Application (ECMRA

The Contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Department of the Navy via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address https://www.ecmra.mil/.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at <https://www.ecmra.mil/>.

### Associate Contractor Agreements (ACA)

The Contractor shall enter into Associate Contractor Agreements (ACAs) for any portion of the contract requiring cooperation and coordination (with Contractors under other DON contracts) in the accomplishment of the Government’s requirement. The agreements shall include the basis for sharing information, data, technical knowledge, expertise, and resources essential to the implementation of services which shall ensure the greatest degree of cooperation to meet the terms of the contract. The Contractor will not be relieved of any contract requirements or entitled to any adjustments to the contract terms because of a

The following are “Associate Contractors” with whom ACAs are required:

|  |  |  |
| --- | --- | --- |
| CONTRACT | SERVICES | CONTRACTOR |
| NGEN Contract Number N00039-13-D-0013 | EUHW replacement equipment/Image Development/Maintenance | ES LLC “DXC”. (formerly Hewlett Packard Enterprise Services (HPES) |
| SMIT Contract Number TBD | Software/Network Infrastructure/ Helpdesk Support/Image Development/Maintenance | TBD |

The Contractor shall:

1. Provide the following general information in all ACAs:
   1. Identification of the program(s) involved and relevant Government contracts of the Associate Contractors.
   2. Identification of the Associate Contractors and their relationships.
   3. Description of the Associate Contractor interfaces by general subject matter.
   4. Specific categories of information to be exchanged or support to be provided.
   5. Potential conflicts between relevant Goverenment contracts and the ACA, and include agreements on protection of proprietary data and restrictions on employees
   6. Expiration date or event of the ACA
2. Provide a copy of all ACAs to the PCO for review before executions of the ACA documents by the cooperating Associate Contractor. The PCO has the right to ask questions and receive answers from each party, make comments and suggestions, and provide edits prior to execution by the parties.
3. Ensure ACAs are in place three (3) months after contract award. Subsequent ACAs required during contract performance shall be accomplished within three (3) months of written notice from the PCO to the Contractor.
4. Responsible for resolving any Associate Contractor disagreements. The Contractor is not relieved of any contract requirements or entitled to any adjustments to the contract terms because of a failure to resolve a disagreement with an Associate Contractor.
5. Be responsible of proprietary data contained in or referenced by any ACA. Liability for the improper disclosure of any any proprietary data contained in or referenced by any agreement shall rest with the parties of the agreement, and not the Government.
6. Allow for amendments to ACAs as required by the Government during contract performance.

## Service Order Provisioning and Delivery

### Core Build Imaging

The Contractor shall:

1. Configure EUHW devices, including the Basic Input Output System (BIOS), in accordance with model-specific Cyber Security guidance. Personnel who conduct imaging work will be cleared contractors, at Secret level, and meet Cybersecurity Workforce (CSWF) requirements.
2. Image EUHW devices with the requested Government-provided image when specified in the task order.
3. Provide EUHW device identifiers to the appropriate Network Manager no less than two (2) days prior to delivery to align device with the Machine Name from the task order being fulfilled.
   1. Device identifier shall be in accordance with Microsoft’s “Hardware IDs for a Computer,” as documented in the “ComputerHardwareIDs” tool found in the Windows 10 Software Development Kit.
   2. The identifier, along with the associated Machine Name, shall be supplied in an electronically readable format as defined by the Network Manager.

### Hardware Peripherals

EUHW device peripherals may be ordered as depicted in Table 3.2.2.

Table 3.2.2: Hardware Peripherals

| **Sample Peripherals and Specs** | | **Availability** | |
| --- | --- | --- | --- |
| **Peripheral** | **Threshold Spec** | **Full**  **Bundle** | **Separately**  **Ordered** |
| Monitor | 22” inch | X |  |
| Keyboard | SmartCard enabled | X |  |
| Mouse | USB 3 Button optical w/ scroll | X |  |
| Docking Station | Device Specific |  | X |
| Network Cable | 14’ CAT 7/7a | X |  |

The Contractor shall:

1. Deliver each end user device with peripherals as ordered.
2. Be responsible for all costs associated with Cybersecurity Authorization, interoperability, compatibility, security, and testing of new peripherals.
3. Provide peripheral ordered by the Government within five (5) days of order receipt when ordered separately from end user devices.

#### End User Hardware As-a-Service (EUHWaaS)

In acquiring EUHWaaS, the Government is only acquiring the service of using an EUHW device. This is not a purchase, and titles for all EUHWaaS devices remain with the Contractor. EUHWaaS includes the provisioning, storage of spares, configuration, testing, integration, installation, operation, maintenance, EOL disposal of NIPRNet and SIPRNet EUHW, and internal storage device removal and destruction requirements identified in Hardware Device Return & Disposal (Section 3.4.6 ).

#### Purchased End User Hardware

In purchasing EUHW devices, the Government is acquiring the EUHW devices with full title transfer to the Government. Purchased EUHW includes the provisioning, storage, and configuration of NIPRNet and SIPRNet EUHW, except for internal storage device removal and destruction requirements identified in Hardware Device Return & Disposal (Section 3.4.6).

### Technical Requirements

#### End User Hardware Device Categorization

The DON requires multiple EUHW categories, and in some cases differing levels of performance characteristics within a specific category of EUHW. Table 3.2.3.1 specifies those platforms which represent the EUHW to be acquired.

The Contractor shall:

1. Provide one (1) offering per hardware category and performance level listed in Table 3.2.3.1 and EUHW Device Specifications (Attachment 10).
2. Meet the Microsoft Windows Hardware Certification Program Requirements for the accredited Microsoft Windows Operating System version at time of delivery.
3. Utilize systems which meet Federal Information Processing Standard (FIPS) 140-2 (Appendix A) and are validated by National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) as applies to the Trusted Platform Module (TPM) chip in accordance with Committee on National Security Systems (CNSS), Policy No. 11 (Appendix A).
4. Ensure all EUHW devices, peripherals, and supporting equipment shall comply with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d).
5. Ensure EUHW can be deployed on either NIPRNet or SIPRNet Networks. Devices deployed on the SIPRNet may require a Carriage Assembly as defined in the Task Order.
6. Complete configuration alteration(s) to ordered End User Hardware as specified in the Task Order.
7. Ensure all hardware is supported by a Management Instrumentation interface allowing management of the hardware/BIOS configuration via Windows Management Instrumentation (WMI).

Table 3.2.3.1: EUHW Category Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| **EUHW Category** | **General Purpose** | **Mid-Range** | **High Performance** |
| Desktop | X | X | X |
| Laptop | X | X | X |
| Rugged Laptop | X |  |  |
| Rugged Tablet | X |  |  |
| 2-in-1 Detachable | X |  |  |
| Zero/Thin Client | X |  |  |
| Ultra-Small Desktop | X |  |  |

##### General Purpose (GP) Desktop/Laptop/Tablet

The Contractor shall provide a General Purpose (GP) desktop/laptop/tablet which will:

1. Be able to process core build security applications and group policy objects (GPOs), as well as other business applications included in the core build, allowing for user multi-tasking.
2. Have enough memory and processor speed, in accordance with Section 3.2.4 State of The Shelf (SOTS) process, to allow the user to open multiple applications and allow the user to multi-task between those open applications, while using multiple display outputs to display on multiple screens or monitors at the same time.
3. Be new and not be previously used or part of any refurbished or grey market goods.

##### Mid-Range Desktop/Laptop

The Mid-Range desktop or laptop is an upgrade to the GP desktop and laptop. In addition to the requirements for General Purpose (GP) Desktop/Laptop/Tablet (Section 3.2.3.1.1), the Contractor shall provide a Mid-Range desktop and laptop which is capable of creating, processing, and displaying high resolution graphics while simultaneously running other applications.

##### High Performance Desktop/Laptop

The High Performance desktop or laptops are for specialized users who require top-of-the-line performance. In addition to those requirements of section for Mid-Range Desktop/Laptop (Section 3.2.3.1.2), the Contractor shall provide a High Performance desktop/laptop which will:

1. Be capable of displaying high resolution graphics and handling resource-intensive applications, such as graphic or engineering design (AutoCAD or similar), geospatial processing, modeling and simulation, gaming, video editing, and music development and editing in addition to applications included in the core build.
2. Be capable of customization and utilization of EUHW multiple PCI-e slots with adapter (desktop devices only). This modular capability will allow for optional builds which are custom-tailored to ultra-specific DON Operations.

##### Rugged Laptop

In addition to the requirements for General Purpose (GP) Desktop/Laptop/Tablet (Section 3.2.3.1.1), the Contractor shall provide a Rugged Laptop which will be capable of operating in hazardous environments in compliance with MIL-STD-810G Series (Appendix A) outlined in Rugged Laptops/Tablets – Test Conditions and Threshold Compliance (Attachment 17).

##### Rugged Tablet

Rugged tablets are for specialized users, and the Contractor shall provide a Rugged Tablet which will:

1. Be capable of operating in hazardous harsh environments in accordance with testing performed via Attachment 17 (Rugged Laptops/Tablets – Test Conditions and Threshold Compliance) in compliance with MIL-STD-810G Series (Appendix A).
2. Be capable of displaying on multiple screens or monitors at the same time.

##### 2-in-1 Detachable

A 2-in-1 detachable is a portable computer which shares characteristics of both tablets and laptops. The Contractor shall provide a 2-in-1 detachable device which will be in the form factor of a laptop computer, but allow the screen to detach and operate as a fully-functional tablet computer.

##### Zero Client or Thin Client

The Zero Client or Thin Client is a lightweight computer developed for remote connection to another computer or server (Physical or Virtual) to fulfill its computational roles (i.e., file, storage, data processing, application hosting). The Contractor shall provide a Zero/Thin Client solution which will enable the end user to interface with server hosted and shared virtualized applications or desktops.

##### Ultra-Small Desktop

An Ultra-Small Desktop computer allows for placement in tight spaces, including behind a computer monitor. The Contractor shall provide an Ultra-Small Desktop which will meet general performance requirements as enunciated for General Purpose (GP) Desktop/Laptop/Tablet (Section 3.2.3.1.1).

3.2.3.2 **IT Accessibility Requirements**

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

Products, platforms and services delivered as part of this work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines.

### State of the Shelf (SOTS)

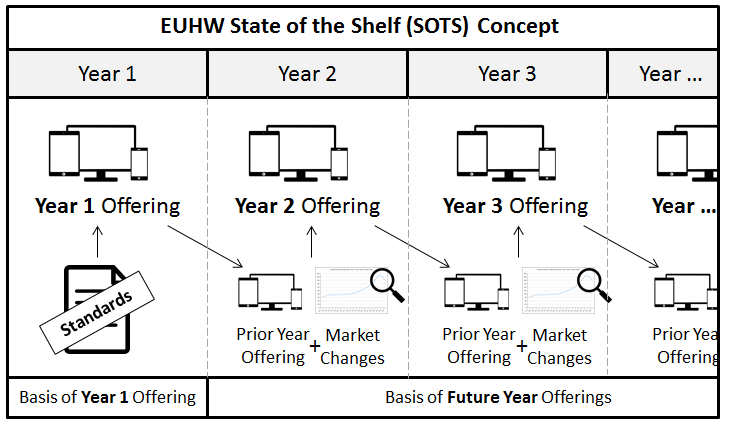
The Government expects to review and update its EUHW device categories annually as offered under the End User Hardware Device Categorization (Section 3.2.3.1). To do so it will use a SOTS methodology to ensure the EUHW devices available on the EUHW contract are current state with evolving commercial capabilities offered in the EUHW market.

#### EUHW SOTS Definition and Methodology

EUHW SOTS is defined as the concept of reviewing and updating all EUHW device offerings no less than once per year. Updates will be predicated upon a review of EUHW categories and are considered open reviews to assess incorporation of market technological advancements, feature enhancements and expansions, and market-driven performance increases. These review updates shall be based on an initial established set of threshold standards for each category. Each category will then be revisited/enhanced every year thereafter, based on the commercial market.

The Contractor shall ensure new/proposed devices comply with DoD cybersecurity accreditation standards. A graphic representation of the SOTS concept is also depicted in EUHW State of the Shelf (SOTS) Concept (Figure 3.2.4.1).

Figure 3.2.4.1: EUHW State of the Shelf (SOTS) Concept



#### EUHW SOTS Implementation

EUHW SOTS enables EUHW capability improvements to occur on a fixed yearly review schedule.

The Contractor shall:

1. Submit the next year's SOTS offering in accordance with Yearly SOTS Offering (CDRL A203). All Energy Star features shall be enabled to the maximum extent practicable.
2. Identify a commercial catalog, catalogs, or portions of a catalog, from which it will provide the items.
3. Identify the catalog for each EUHW category by unique name/publication number or similar unique identifier.
4. Identify all subsequent publications of that catalog (e.g. descendants or logical derivatives).
5. Make copies of the catalogs, including catalog changes, available electronically to the Government to establish the price baseline for the application of contractual discounts of existing items, catalog additions, and to facilitate appropriate adjustments (i.e. technical specifications).
6. Maintain an archive of the catalogs and any catalog changes thereto for the life of this contract and all task orders.
7. Deliver, for each new offering, six (6) EUHW devices; with four (4) going to the United States Navy (USN) and two (2) going to the United States Marine Corps (USMC).
8. Deliver two (2) EUHW devices to each DOD Agency/MILDEP upon their entry into the contract and initial order of EUHW. Deliver, for each new offering thereafter, two (2) EUHW devices to each DOD Agency/MILDEP ordering EUHW on this contract.
9. Provision and fulfill orders with the new EUHW devices upon completion of Cybersecurity Authorization.

### EUHWaaS Device Refresh

For EUHW device delivery, the Network Manager will be responsible for unpacking, installing, and removing retrograde material post-delivery. EUHWaaS Device Refresh, also known as “seat refresh,” is the periodic replacement of hardware devices. Changes to the refresh schedule will be managed via a Schedule Change Control Board (SCCB) and will be published by the Government on a monthly basis.

The Contractor shall:

1. Replace all Legacy EUHWaaS within 36 months of contract award.
2. Replace all EUHWaaS within 36 months of initial delivery.
3. Develop, submit and execute the EUHWaaS Refresh Plan (CDRL A204).
4. Surge delivery volume by an estimated fifteen percent (15%), as ordered, in any year.
5. Deliver EUHWaaS refresh devices no earlier than three (3) days prior to the refresh date and no later than one (1) day prior to the refresh date, to specified location(s) as defined by the order.

### EUHWaaS Deployable Computing

Deployable computing services are provided to end users deployed to or stationed in an expeditionary or field environment which requires integration of the end user device into another network.

The Contractor shall:

1. Provide imaged hardware for Pack-Up Kit (PUK) and deliver to requesting commands operating EUHWaaS Deployable Computing devices within ninety-six (96) hours prior to the deployment date listed on the embarkable request. PUKs consist of:
2. Five percent (5%) whole unit (i.e., additional EUHWaaS devices) and five percent (5%) replacement device storage (i.e., replacement internal storage) of total deployed hardware devices (fractional percentages will be rounded up to the next whole number) with a minimum of one (1) each.
3. BIOS and Unified Extensible Firmware Interface (UEFI) password for unit IT personnel to properly manage hardware devices while on deployment.
4. Provide PUK HW items that are compatible with the requesting Command’s existing EUHWaaS devices.
5. Deliver imaged replacement devices and repair parts to the requesting location.
6. Provide imaged replacement storage drives upon return which are compatible with the unit’s EUHWaaS Deployable Computing devices in the quantity required to allow a one-for-one drive swap to speed the reconnection of the unit’s EUHW Deployable Computing devices to the Network.
7. Establish and execute process for authorizing government technicians to remove, replace, and repair equipment without voiding the Contractor's warranty.
8. Coordinate with the Network Manager in support of the returning unit and return of PUKs.

### Service Management of EUHWaaS Devices

Service Management of EUHWaaS devices will be performed by the Network Manager to coordinate troubleshooting, repair, and restoration of inoperable EUHWaaS devices.

The Contractor shall:

1. Support the Network Manager’s ability to troubleshoot EUHWaaS issues to include loaner devices and spares, in coordination with the Network Manager.
2. Troubleshoot, test, repair, restore, or replace inoperable EUHWaaS devices no later than seventy-two (72) hours after receiving the service request.

### EUHW Service Desk Functionality

The Navy (USN) intends to use the Network Manager as the initial entry point for all EUHWaaS issues and intends to go directly to the manufacturer for warranty issues involving purchased hardware. The USMC intends to use the MCEN Service Desk as the initial entry point for all non-deployed EUHW issues. All other DoD organizations will use their own Service Desk or a single consolidated DoD Service Desk as their entry point for all EUHW issues.

The Contractor shall:

1. Provide Service Desk to respond to the Network Manager Service Desk for EUHWaaS and EUHW support in their execution of troubleshooting activities.
2. Coordinate and establish authorization process to qualify Network Manager technicians to repair devices while maintaining warranty.
3. Submit a Contractor’s Service Desk Summary Report (SDSR) for all USMC trouble calls received (CDRL B301).

### Legacy EUHWaaS Support Services

Legacy EUHWaaS devices are currently provisioned and installed on the NMCI by the incumbent Contractor. The Contractor is required to enter into a business arrangement with the incumbent Contractor to ensure the Government’s continued use of the legacy EUHW devices until each device is refreshed under this contract.

The Contractor shall:

1. Perform Service Management of Legacy EUHWaaS in accordance with Section 3.2.7 Service Management of EUHWaaS.
2. Perform Service Desk Services for Legacy EUHWaaS in accordance with Section 3.2.8 EUHW Service Desk Funtionality.
3. Perform Equipment Recall of Legacy EUHWaaS in accordance with Section 3.4.2 Equipement Recall.
4. Manage Legacy EUHWaaS assets in accordance with Section 3.4.4.1.d EUHWaaS Asset Management.
5. Perform Hardware Disposal of Legacy EUHWaaS in accordance with Section 3.4.6 Hardware Device Return and Disposal.

### EUHWaaS Buy-Back

At any point throughtout contract period of performance, at the Government’s request, the Contractor shall make available for sale or transfer the installed EUHWaaS devices to the successor EUHW Contractor and/or the Government. In the absence of mutual agreement otherwise, the price will be determined based upon the calculation(s) of EUHWaaS Hardware Buy-Back (Attachment 9).

## Service Order Management

Service Order Management is the planning, submission, review, funding, approval, receipt, delivery (to include initial ordering, modification, discontinuance, and cancellation of services), validation, device pickup/delivery, and reporting on services contained in the Service Catalog in the Government Owned and Managed Ordering (GOMO) Application. The GOMO Application includes, but is not limited to, RAPT and NMCI Enterprise Tool (NET).

### Contractor Ordering Application Integration

The Contractor shall:

1. Integrate their ordering applications with the GOMO Application as outlined in GOMO Interface Control Document (ICD) (Attachment 13) within ninety (90) days of contract award.
2. Comply with all current cybersecurity and Information Assurance (IA) manuals, instructions and guides as listed in Appendix A.
3. Provide new and/or modified Contractor service offerings and service attributes for incorporation in the NEN Service Catalog via the identified GOMO Application.
4. Acknowledge, track, and send status of received task/delivery orders and any modification to the GOMO Application, including but not limited to the following required notifications:
   * 1. Order Acknowledgement Notification – Send an electronic acknowledgement notification within twenty-four (24) hours of receipt of an order in the Contractor’s system.
     2. Delivery Scheduled – Send an electronic order status notification.
     3. Delivery Complete – Provide GOMO Application with Asset and Configuration data as listed in Navy Logistics Asset Data Attributes (Attachment 5) associated with Task Orders.
5. Submit electronic invoices to Government workflow tool for routing to Government financial systems or other Government processes, and provide copy of submitted invoice to GOMO Application:
6. Provide actual dates and quantities of orders.
7. Reconcile discrepancies between the Government and Contractor records.
8. Review and approve bilateral modifications to task/delivery orders within one (1) day.
9. Interface with the GOMO Application detailed in GOMO ICD (Attachment 13).
10. Provide datasets and relevant elements which comply with the ICD.
11. Include secure transactions in conformance with DoDI 8520.02 Public Key Infrastructure (PKI) (Appendix A).

## Logistics Management

Logistics Management includes the personnel, processes, and tools required to ensure resources are available and accessible to enable and sustain EUHW services throughout the contract.

### Supply Chain Risk Management

The Government will monitor supply, disposal, and destruction practices, review the Contractor processes for compliance to governing policy and contract requirements, and will direct corrective action if deficiencies are found.

The Contractor shall:

1. Execute the SCRM Plan (Attachment 15), a subset of the Program Protection Implementation Plan (PPIP) (CDRL A205) for the entire contract performance period..
2. Esure that the PPIP (CDRL A205) content is updated, as needed, based upon the NEN Security cocerns.
3. Execute the PPIP (CDRL A205) for the entire contract performance period.
4. Allow the Government access to warehouse, depot, and staging facilities for the purposes of audit and inspection of supply functions, supply chain risk management activities, and storage media storage, disposal, demilitarization, and destruction.

### Equipment Recall

The Contractor shall:

1. Notify the Contracting Officer’s Representative (COR) in writing within twenty-four (24) hours of learning of a recall, including the recall notice details, list of affected equipment, and where applicable, safety mitigation procedures.
2. Pick-up safety-related recall equipment, and ship replacement equipment within twenty-four (24) hours from when direction from the COR is received.
3. Pick-up non-safety-related recall equipment, and ship replacement equipment within seven (7) days from when direction from the COR is received.

### Purchased EUHW Warranty Management

With exception of USMC, the Government will interface directly with the manufacturer for warranty issues involving purchased hardware. The USMC will use the MCEN Service Desk as the initial entry point for all non-deployed EUHW issues.

For all USMC purchased EUHW, the Contractor shall:

* 1. Resolve Warranty Trouble Tickets as follows:

1. Utilize one (1) service trouble ticket per serialized EUHW asset from the time of initiation until it is resolved.
2. Log all follow-up inquiries under the original trouble ticket and provide email work status updates to the trouble ticket initiator when there is a change in the status of the trouble ticket, until the ticket has been closed.
3. Send trouble ticket closure notification emails to the qualified technician(s) when the Contractor believes all required action has been taken to resolve the problem. Qualified technicians are defined to include specified military personnel, Government civilians, and Network Managers who have obtained the required technical training as evidenced by their completed award of an Information Technology (IT) related Military Occupational Specialty (MOS), or COMPTIA A+ certification, or any approved equivalent certifications.
4. Do not permanently close trouble tickets until the problem is resolved and fully accepted by the qualified technician(s).
   1. Track and manage warranties for newly procured Government equipment in accordance with Instructions for Electronic Submission of Warranty Tracking and Administration Information for Serialized Items (Attachment 15) and DFARS 252.246-7006 (CDRL A206 Warranty Tracking and Administration for Serialized Items).
   2. Provide initial entry into Contactor Support Request System 24/7 for the duration of the commercially available warranty for all EUHW devices under this contract via the following three (3) methods:
5. Worldwide toll-free telephone number.
6. Website Uniform Resource Locator (URL).
7. Direct email account.
   1. Respond to qualified technicians who have provided a .mil (dot-mil) e-mail address.
   2. Ensure replacement parts are compliant with the device specifications.
   3. Replace unrepairable devices with the newest model approved in accordance with Section 3.2.4 State of the Shelf (SOTS). Changes in equipment location or the unit to which the equipment is assigned will have no effect on the Contractor’s responsibility to provide warranty support in accordance with the contract.
   4. Ensure no counterfeit or grey-market parts are provided as replacements in accordance with DFARS 252.246.7007 and DoDI 4140.67, DoD Counterfeit Prevention Policy (Appendix A).
   5. Manage and enter all registration information into its warranty database prior to delivering the equipment.
   6. Authorize qualified technicians to remove, replace, and repair equipment without voiding the Contractor's warranty. If the Contractor requires additional certification, this may be accomplished by allowing the qualified technicians to access the Contractor’s certification process by entering a 'passcode' instead of a credit card number to obtain a Personal Identification Number (PIN). The Contractor may provide an area on its website which allows qualified technicians to complete an initial registration in order to obtain a ‘passcode’.
   7. Submit a USMC Direct Access Report (CDRL B302) of personnel who have been granted direct access to Contractor’s technical reference documents. If the Contractor has a tool utilized to track qualified technicians, the Contractor shall maintain the data in the tool, and the Government will not be required to update or maintain the data in the Contactor’s tool.
   8. Provide the qualified technician a unique website URL address with direct access to their Service Desk technicians and service representatives to verify and validate the following. If for any reason the URL changes, the Contractor shall provide the new URL to the DON COR within twenty-four (24) hours:
   9. Trouble Ticket Status.
   10. EUHW-Specific Warranty and Technical Information.
   11. Equipment recall information.
   12. Shipment Status of replacement part and/or repaired EUHW.
   13. Provide the following documentation via their warranty URL:
8. Electronic User Manual.
9. Material Safety Data Sheets (MSDS).
10. Technical Manuals.
    1. Provide warranty status updates to include:
11. An e-mail acknowledgement within four (4) hours to the qualified technician who initiated the request for service.
12. All work in progress and any changes to the ticket.
13. A closing update to the qualified technician who initiated the trouble ticket.
    1. Provide warranty repair to include:
14. Repair within seventy-two (72) hours of when the EUHW asset is returned to the Contractor’s facility.
15. Notification to the qualified technician if the EUHW cannot be repaired and provide the shipping information for the replacement EUHW.
16. Return of the repaired EUHW within same timeline as the EUHW was shipped to the Contractor.
17. Updating the Item Unique Identification (IUID) registry.
18. Transfer of warranty information to the replacement item.
    1. Ship replacement parts within twenty-four (24) hours of receipt of a trouble ticket.
    2. Notify the qualified technician to return all failed parts when required, and provide return shipping container, appropriate packaging material, and a return label when shipping the replacement part to the qualified technician.
19. The Government will not return internal storage devices. The Contractor shall request the serial number of the failed internal storage device, if required. The Government will not fill out any Contractor internal storage device destruction forms. Authorize removal of storage media without voiding EUHW device warranties.
20. The Contractor shall notify the COR if failed parts are not received at Contractor’s facility within thirty (30) days of shipment.

### Asset Management

Asset Management is the identification, tracking, control, and accounting of assets (hardware and software) throughout the assets’ life-cycle to provide operational and cost visibility.

The Contractor shall:

1. Affix permanent asset tags to EUHW devices.
2. Asset tags shall consist of:
3. Plastic or plastic-like, coated, smear-proof, non-removable, and sufficiently sturdy to last through the expected life of the system, in accordance with MIL-STD-130N (Appendix A).
4. Black lettering placed on a white background and be affixed on an external surface wherever it is most conspicuous and visible, not blocking access panels or fan compartments.
5. Asset Tag number, with accompanying barcode (linear or 2d); this is a unique identifier generated by the Contractor.
6. Serial number, with accompanying barcode (linear or 2d).
7. Manufacturer.
8. Model.
9. Hostname.
10. Service Desk Contact Information (phone, email, website).
11. Provide replacement asset tags for unreadable or missing tags.

#### EUHWaaS Asset Management

The Contractor shall:

1. Submit an asset data file to the Network Manager-provided asset database to include data attributes as defined in Navy Logistics Asset Data Attributes (Attachment 5) and be itemized by serially-managed EUHW devices.
2. Include internal storage unit serial numbers with each EUHW device.
3. Update the asset data file within twenty-four (24) hours of EUHW device delivery as well as EUHW device decommission.
4. Use read-only access to the Network Manager-provided asset database to monitor asset data accuracy and resolve discrepancies with the Network Manager.
5. Ensure USMC EUHWaaS devices are marked with two (2) asset tags, the Marine Corps Identification Plate (MCIP), and the device asset tag as described in USMC Logistics Asset Data Attributes (Attachment 16).

#### Purchased EUHW Asset Management

The Contractor shall:

1. Affix IUID tags in accordance with DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property, May 19, 2011 (Appendix A).
2. Ensure USMC EUHW devices are marked with two (2) asset tags, the Marine Corps Identification Plate (MCIP), and the device asset tag as described in USMC Logistics Asset Data Attributes (Attachment 16).

### Shipping, Packing, Tracking, Handling, Storage, and Transportation Requirements

Shipping, Packaging, Tracking, Handling, Storage, and Transportation is the combination of resources, processes, procedures, design considerations, environmental considerations, and methods to ensure all systems, equipment and support items are preserved, packaged, handled, transported, and stored properly. CONUS includes all 50 states, the District of Columbia and Puerto Rico; OCONUS includes all sites not within CONUS.

The Contractor shall:

1. Deliver all ordered items to a specified location in CONUS or OCONUS as defined by the order.
2. Deliver EUHW within five (5) days of order receipt.
3. Use delivery carrier of the Contractor’s preference.
4. Include a tracking number assigned to the shipment and provide the tracking number to the ordering activity CTR/COR (as applicable) on the order via email. Include in the email the date order was shipped and estimated delivery date. Ensure a www “hot-link” and if possible, a toll free number to the carrier is included in the email.
5. Ensure no partial shipments unless explicitly authorized in the order.
6. Handle and store hazardous material and parts in accordance with the Occupational Safety & Health Administration (OSHA) 29 Code of Federal Regulation (C.F.R.) § 1910 Occupational Safety and Health Standards.
7. Package and transport hazardous material and parts in accordance with: a) Hazardous Material Transportation Act, 1975, Title 49 U.S.C 5101-5127; and b) 49 C.F.R. Parts 100-185 Hazardous Materials Regulations.
8. Follow packaging guidelines:
   * 1. Components of a workstation may be packaged in separate boxes to form a complete package.
     2. A complete package consists of all components, to include associated items required to set up and operate properly.

#### USMC Purchased EUHW Shipping Requirements

The Contractor shall:

1. Submit USMC Status Report (CDRL B303) for each active order.
2. Submit an electronic copy of the Bill of Materials (BOM), as well as a completed USMC Asset Shipment Report (CDRL B304) to the COR within two (2) days of a shipment date.
3. Ensure that EUHW Asset Shipment Reports (CDRL B304) are not combined, and only include related information for one order.
4. Only be responsible for CONUS shipping of USMC OCONUS orders; Government will coordinate final delivery OCONUS for USMC orders.

### Hardware Device Return & Disposal

The Network Manager or Government shall have the responsibility for the removal and disposal of all EUHW internal storage devices. No internal storage devices will be returned to the Contractor once the devices have been connected to a Government network.

The Contractor shall:

1. Demilitarize and dispose of all returned EUHW in accordance with DoD Manual 4160.28-V2 and DON CIO Message 281759Z (Appendix A).
2. Immediately return any inadvertently received storage media back to the originator.
3. Authorize removal of storage media by authorized third parties without voiding device warranties.
4. Update the DoD IUID Registry within five (5) days of when purchased EUHW devices are returned.
5. Remove IUID marking or asset tags from purchased EUHW device.
6. Provide return shipping container, appropriate packaging material, and a return label upon seat refresh, end of order, or return of inoperable device.

## Transition Services

Transition services ensure continued uninterrupted, quality service levels to end users, and are the planning and execution of activities necessary for phase-in of EUHW services. Phase-in services include activities necessary to ensure the Contractor is ready to begin execution of EUHW services. Phase-out will occur during the final years of the contract with orders ramping down during the transition period.

The Contractor shall develop, deliver, and execute a Phase-in Plan (CDRL A207).

## Program Security

While there is no requirement for the Contractor to access North Atlantic Treaty Organization (NATO) information on this contract, Naval Intelligence Security Policy Directive 17-008 states that those contractors that are SCI cleared with SIPRNet accounts shall be read-on for NATO access (in the event of inadvertent disclosure to NATO information) and complete the derivative classification training prior to being granted access to SIPRNet; training is provided by the facility security officer.

The Contractor shall:

1. Obtain and manage DoD-approved Cybersecurity Workforce (CSWF) certifications appropriate for each category and level in accordance with SECNAV M-5239.2 and DoD 8570.01 as required (CDRL A208 Contractor Personnel Access List Report).
2. Make appropriate IT Level assignments (by position) in accordance with SECNAV M-5239.2 and DD Form 254 section for IT Systems Personnel Security Program Requirements (CDRL A208 Contractor Personnel Access List Report).
3. Ensure Contractor personnel who do not have the correct, current certifications and background investigations are denied access to DoD information and systems for the purpose of performing network functions.
4. Submit a Program Protection Implementation Plan (PPIP) (CDRL A205 Program Protection Implementation Plan (PPIP)).
5. Notify in writing, the Trusted Agent, Contracting Officer, and Program Security Manager within 24 hours of discovering any Common Access Card (CAC) lost, stolen, or destroyed; the CAC will be revoked and application for a replacement shall be submitted.
6. Submit to Program Security, the final disposition of CACs and their return to the Government (CDRL A208 Contractor Personnel Access List Report).
7. Report all security incidents via email to the NEN Program Security Manager. A security incident is an incident involving a Contractor or Subcontractor employee that involves personnel adjudication criteria as described in DoDM 5200.02.
8. Report all cyber incidents covered by DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, via email to the NEN Program Security Manager; in addition to the required reporting to DoD at <http://dibnet.dod.mil>.
9. Ensure Contractor employees and Subcontractor employees identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or other correspondence related to this contract.
10. Ensure Contractor employees are clearly identifiable while on Government property by wearing appropriate picture badges.
11. Provide a list of personnel requiring picture badges to the COR to verify that the contract or delivery/task order authorizes performance at specified Government installations. A contractor picture badge may be issued to contractor personnel by the issuing office upon receipt of a valid visit request from the Contractor and a picture badge request from the COR. The Contractor shall ensure requests are submitted timely so as not to delay work.
12. Assume full responsibility for the proper use of identification badges and shall be responsible for the return of the badge upon termination of personnel or expiration or completion of the contract.
13. Forward to issuing office(s) a list of all unreturned badges with a written explanation of any missing badges at the completion of the contract.
14. Ensure Contractor-occupied facilities (on Department of the Navy or other Government installations) such as offices, separate rooms, or cubicles are clearly identified with Contractor supplied signs, name plates or other identification, showing that these are work areas for Contractor or subcontractor personnel.

## Service Level Management

Service Level Management includes the resources, processes, metrics, systems, and measurement approaches necessary to assess the state of compliance with EUHW schedule and performance requirements.

The Government will verify and validate the performance of the Contractor, in accordance with the Quality Assurance Surveillance Plan (QASP) (Attachment 12), in providing services at the levels specified in Service Level Requirements (Attachment 11). The Contractor shall submit CDRL A209 SLR CONOPS in response to Attachment 11.

The Contractor shall:

1. Ensure all performance data from Contractor owned/operated tools and systems are accessible to Government SMEs.
2. Retain all performance data for the entire life of the contract.

# Appendix A Reference Documents

|  |
| --- |
| **Reference Documents** |
| DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting |
| Defense Federal Acquisition Regulation Supplement (DFARS) Clause 246.870-2(a) Contractors’ Counterfeit Electronic Part Detection and Avoidance, October 21, 2016 |
| DFARS 252.246.7007 Contractor Counterfeit Electronic Part Detection and Avoidance System |
| Committee on National Security Systems (CNSS), Policy No. 11 |
| Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, January 2017 |
| DoD Manual 4160.28 Volume 2, Change 1, Defense Demilitarization: Demilitarization Coding, December 1, 2017 |
| DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP), April 3, 2017 |
| DoDD 8140.01, Cyberspace Workforce Management, August 11, 2015 (Note: 8140 replaces the 8570 directive); |
| DODD 8570.01-M, Information Assurance (IA) Workforce Improvement Program Manual, January 24, 2012 Incorporating Change 4 November 10; |
| DoDI 4140.67, DoD Counterfeit Prevention Policy; |
| DoDI 5000.64, Accountability and Management of DOD Equipment and Other Accountable Property, 19 May 2011; |
| DoDI 8500.01, Cybersecurity, March 14, 2014; |
| DODI 8520.02 Public Key Infrastructure (PKI); |
| DON CIO Message Processing of Electronic Storage Media for Disposal 281759Z 12 AUG12; |
| Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), Security Requirements for Cryptographic Modules; |
| FedRAMP; https://www.fedramp.gov/documents/. |
| Military Standard 810G, Environmental Engineering Considerations And Laboratory Tests, 14 April 2015; |
| MIL-STD-130N, DOD Standard Practice Identification Marking of US Military Property, 16 November 2012; |
| Naval Intelligence Security Policy Directive 17-008; |
| NEN Operating Model |
| SECNAV M-5239.1 DON Information Assurance Manual |
| SECNAV M-5239.2, June 2016 Cyberspace Information Technology And Cybersecurity Workforce Management And Qualification Manual, June 2016; |
| SECNAVINST 5239.19 Department Of The Navy Computer Network Incident Response And Reporting Requirements; |
| SECNAVINST 5239.3B Navy Information Assurance (IA) Policy; |
| SECNAVINST 5239.3C Department Of The Navy Cybersecurity Policy; |
| Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) |
| Security Agreement (DD Form 441): Appendage to Department of Defense Security Agreement (OMB No. 0704-0194) |

**Note:** *References to a) Code of Federal Regulation (C.F.R.) and b) United States Code (U.S.C.) can be viewed respectively at a) http://www.gpo.gov and b) https://www.ecfr.gov.*

# Appendix B CDRLs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CDRL** | **Title** | **First Delivery** | **Frequency** | **PWS Section** |
| A201 | Program Management Plan | 30 Days after Contract Award (DAC) | Annually | 3.1.2.a. |
| A202 | Monthly Status Report | 30 DAC | Monthly | 3.1.2.b. |
| A203 | Yearly State of the Shelf (SOTS) Offering | Nine Months After Contract Award | Annually | 3.2.4.2.a. |
| A204 | EUHWaaS Refresh Plan | IAW Phase-in Plan | Monthly | 3.2.5.c |
| A205 | Program Protection Implementation Plan (PPIP) | 45 DAC | As Needed | 3.4.1, 3.6.d |
| A206 | Warranty Tracking and Administration for Serialized Items | USN: 30 Days After First Government Property procurement; USMC: 2 Days After Shipment | As Needed | 3.4.3.b. |
| A207 | Phase-in Plan | 15 DAC | One Time | 3.5 |
| A208 | Contractor Personnel Access List Report | 30 DAC | Monthly | 3.6.a, 3.6.b, 3.6.f |
| A209 | Service Level Requirement (SLR) Concept of Operations (CONOPS) | 30 DAC | As Needed | 3.7 |
| B301 | USMC Service Desk Summary Report | 30 DAC | Monthly | 3.2.8.c. |
| B302 | USMC Direct Access Report | 30 DAC | Quarterly | 3.4.3.j. |
| B303 | USMC Status Report | 1 Day After Delivery Order | As Needed | 3.4.5.1.a. |
| B304 | USMC Asset Shipment Report | 2 Days After Delivery Order | As Needed | 3.4.5.1.b., 3.4.5.1.c. |
|  | | | | |

# Appendix C Acronyms

| **Acronym** | **Definition** |
| --- | --- |
| aaS | As-a-Service |
| BIOS | Basic Input Output System |
| BOM | Bill of Materials |
| CAC | Common Access Card |
| CDRL | Contract Data Requirements List |
| CMVP | Cryptographic Module Validation Program |
| CNSS | Committee National Security Systems |
| CO | Contracting Officer |
| CONUS | Continental United States |
| COR | Contracting Officer’s Representative |
| CSOP | Contract Security Oversight Program |
| DAWIA | Defense Acquisition Workforce Improvement |
| DBIDS | Defense Biometric Identification System |
| DFARS | Defense Federal Acquisition Regulation Supplement |
| DoD | Department of Defense |
| DON | Department of the Navy |
| DPM | Deputy Program Manager |
| EUHW | End User Hardware |
| EOL | End-of-Life |
| FAR | Federal Acquisition Regulation |
| FIPS | Federal Information Processing Standard |
| GFI | Government Furnished Information |
| GO/CO | Government Owned/Contractor Operated |
| GO/GO | Government Owned/Government Operated |
| GOMO | Government Owned and Managed Ordering |
| GP | General Purpose |
| GPO | Group Policy Objects |
| HST | Handling, Storage, and Transportation |
| HW | Hardware |
| IA | Information Assurance |
| ICD | Interface Control Document |
| IUID | Item Unique Identification |
| IT | Information Technology |
| LMSD | Lost, Missing, Stolen, or Damaged |
| MCEDS | Marine Corps Enterprise Desktop Standard |
| MCEN | Marine Corps Enterprise Network |
| MCIP | Marine Corps Identification Plate |
| MOS | Military Occupational Specialty |
| MSDS | Material Safety Data Sheets |
| MSR | Monthly Status Report |
| NEN | Naval Enterprise Network *(refers to the PMO/ all related NEN oversight bodies for implementation of NGEN)* |
| NET | NMCI Enterprise Tool |
| NGEN | Next Generation Enterprise Network  *(refers to the IT architecture / related network services infrastructure)* |
| NIPRNet | Non-classified Internet Protocol Network |
| NIST | National Institute of Standards and Technology |
| NMCI | Navy Marine Corps Intranet |
| NPRM | Navy Process Reference Manual |
| OCONUS | Outside the Continental United States |
| ONE-Net | OCONUS Navy Enterprise Network |
| PCO | Procuring Contracting Officer |
| PKI | Public Key Infrastructure |
| PM | Program Manager |
| PMO | Program Management Office |
| PMP | Program Management Plan |
| PMR | Program Management Review |
| PMS | Performance Management System |
| POC | Point of Contact |
| PoP | Period of Performance |
| PUK | Pack Up Kit |
| PWS | Performance Work Statement |
| QASP | Quality Assurance Surveillance Plan |
| RAPT | Requirements Award Process Tool |
| SCRM | Supply Chain Risk Management |
| SDSR | Service Desk Summary Report |
| SIPRNet | Secret Internet Protocol Network |
| SLR | Service Level Requirement |
| SME | Subject Matter Expert |
| SMIT | Service Management Integration and Transport |
| SOTS | State of the Shelf |
| SPT | Shipping, Packaging, Tracking |
| SW | Software |
| TA | Trusted Agent |
| TASS | Trusted Associate Sponsorship System  *(replaces the former Contractor Verification System (CVS))* |
| TPM | Trusted Platform Module |
| UEFI | Unified Extensible Firmware Interface |
| URL | Uniform Resources Locator |
| USG | United States Government |
| USMC | United States Marine Corps |
| USG | United States Government |
| USN | United States Navy |
| WMI | Windows Management Instrumentation |

| **General Reference Sources** - **Acronyms** | **General References / Overall Sources for Acronyms** |
| --- | --- |
| DON Cyber Glossary | Department Of The Navy Cyber Glossary: Terms And Definitions; Developed By OPNAV N2N6 In Collaboration With DON CIO And USMC C4 Cybersecurity Directorates; incorporated sources: various, including Joint Pub 3-12 Cyberspace Operations; Published: December 11, 2017; location: http://www.doncio.navy.mil/ContentView.aspx?id=9828 |