SECTION C – DESCRIPTION/SPECS/WORK STATEMENT

SPECIFICATIONS/STATEMENT OF WORK/PERFORMANCE WORK STATEMENT

Revision dated 1 May 2018

Work under this performance-based contract shall be performed in accordance with the following description/ specifications/ statement of work (SOW) which herein shall be referred to as Performance Work Statement (PWS):

1.0 PURPOSE

1 BACKGROUND

Space and Naval Warfare Command (SPAWARSYSCOM) is an Echelon II organization whose mission is to invent, acquire, develop, deliver and support integrated and interoperable C4ISR, Business Information Technology (IT) and Space capabilities in the interest of national defense. As an Echelon III command under SPAWARSYSCOM, Space and Naval Warfare Systems Center, Atlantic (SPAWARSYSCEN Atlantic's) supports the command mission by providing support capabilities for Department of Defense (DoD), Joint, Coalition, and other federal government agencies. The work to be performed under this TO is focused on SPAWARSYSCEN Atlantics C4ISR capabilities specific to Business and Health Information Technology (IT) engineering support.

SPAWARSYSCEN Atlantic's IT products and systems engineering capabilities enable the Navy's Bureau of Medicine and Surgery (BUMED), the Navy Medicine Information Systems Support Activity (NAVMISSA), the Air Force Medical Operations Agency (AFMOA) the Air Force Medical Service, (AFMS) as well as United States Army Medical Command (MEDCOM), the United States Army Medical Technology Center (USAMITC) and the Defense Health Agency (DHA) to design, deploy, integrate, secure and sustain Health information technology (Health IT) solutions and systems in an integrated environment that interface and communicate jointly that supports the delivery of healthcare worldwide for the DoD's sailors, airmen, soldiers and their dependents.

SPAWARSYSCEN Atlantic's Health IT engineering support delivered to the DoD's Military Health System (MHS) and executed by the Defense Health Agency (DHA), keeps our most important weapon system, the "Human Weapon System," our military active duty and reserve servicemen and women, "medical ready" and "healthy" in order to defend the United States of America.

The DHA as a combat support agency (CSA) combined with the medical departments (Navy, Army, AF Medicine) are chartered by DoD to oversee and implement "standard," "integrated," and "inter- operable," Information Technology solutions in order to support the delivery of healthcare at Military Treatment Facilities (Hospitals and Clinics) and Medical Support Commands worldwide.

To ensure and meet the DoD's directives and objectives that Health IT solutions and operations be standard, integrated, and inter-operable throughout the MHS, the DHA was stood up October 1st 2013 to assume responsible of the delivery of IT to the Medical Services. The DHA will transition over the next several years IT programs and assume execution responsibility. Today, and until full transition and full operating capability is achieved, the DHA funds Health IT initiatives directly within the DHA organization, as well as funds each Medical Service to execute IT programs.

SPAWARSYSCEN Atlantic receives tasking and funding from DHA and the three Medical Service Department's for its engineering services support today, and this PWS will support tasking and funding from Navy Medicine as well as funding from the other medical services and DHA to ensure Navy and DHA IT architectures, products and solutions are integrated and inter-operable to meet DoD, Navy, DHA, and Defense Healthcare Management System Modernization (DHMSM) and the Defense Medical Information Exchange (DMIX) directives.

1 SCOPE

This performance work statement (PWS) will provide worldwide enterprise Health IT engineering support in the areas of system engineering, systems administration, enterprise network, network security, infrastructure engineering, infrastructure modernization, IT systems, systems deployment and integration, as well as information assurance and system support services for Navy Medicine, the DHA, Healthcare Management System Modernization Program Office (DHMSM), Defense Medical Information Exchange Program Office (DMIX) other DoD Medical departments (AF Medicine and Army Medicine) that require connectivity and integration into the Military Health System Intranet and the Medical Community of Interest network that Navy Medicine and DHA own and operate.

This TO supports BUMED and NAVMISSA's Health IT initiatives and will meet a requirement that Enterprise and MTF Health IT systems implemented in Navy Medicine and DHA be interoperable and integrated. Navy Medicine, Air Force Medicine and Army Medicine Health IT solutions are being consolidated and integrated, and while operating independently in specific MTF's and regions of the world, the IT solutions must be standardized and interchangeable, and integrate with each other. This TO supports both this integration as well support the specific engineering required to deliver each task within this PWS for Navy Medicine as well as the other DoD medical departments and DHA.

The contractor shall provide engineering support in the areas of system engineering, enterprise network, network security, infrastructure engineering, cyber security, platform infrastructure engineering, systems testing, systems integration, as well as information assurance for Navy Medicine, the DHA, DHMSM, DMIX and other DoD Medical departments that require connectivity and integration into the Military Health System Intranet (MHSi) and the Medical Community of Interest network (MEDCOI) in order to support current and future EHR capabilities. An in-depth understanding of the Defense Health Agency and Navy Medicine enterprise systems architecture, network, security, and accreditation architecture is required in order to execute the tasking in this PWS. An in depth knowledge and experience also must include technology implementations, operations and lifecycle support within the Navy Medicine Enterprise and the DHA.

The tasking set forth below is intended to encompass the full operating lifecycle networks, network/application services and the health care applications they support. It includes from inception to operations network protection architecture, design, integration/deployment, operation and active network defense (computer network defense). Active network defense is supplemented by external assessment known as red teaming which identifies critical gaps and vulnerabilities which are used as feedback to the architect/design/deploy/operate/defend lifecycle. Support for the network itself is not enough as the critical assets it is built to support are the health care applications and their supporting computing services such as directory services. All of these items critically tie together for delivery of functional applications on a secure network.

2.0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

All work shall be accomplished using the best commercial practices and current acceptable industry standards. In accordance with Defense Acquisition Policy changes, maximum utilization of non-government standards will be made wherever practical. Where backward compatibility with existing systems is required, selected interoperability standards will be invoked. For purposes of bidding, the following documents are not exclusive; however, all contractors shall be able to meet those cited.

2.1 REQUIRED DOCUMENTS

The following instructional documents are mandatory for use. Unless otherwise specified, the document's effective date of issue is the date on the request for proposal.

	Document Number	**Title**
a.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM)

	Document Number	Title
b.	DoDI 5220.22	DoD Instruction – National Industrial Security Program
c.	DoD 5200.2-R	DoD Regulation – Personnel Security Program
d.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12
e.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08
f.	DoDD 8500.1	DoD Directive – Information Assurance
g.	DoDI 6205.4	Department of Defense Instruction, Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense
h.	DoDI 8500.2	DoD Instruction – Information Assurance (IA) Implementation
i.	DoDI 8510.01	DoD Information Assurance Certification and Accreditation Process, 28 Nov 07
j.	DoDD 8570.01	DoD Directive – Information Assurance Training, Certification, and Workforce Management
k.	DoD 8570.01-M (to be updated to DoD 8140)	Information Assurance Workforce Improvement Program (Information Resource Management, Knowledge/Skills-Based Workforce)
l.	SECNAVINST 4440.34	Secretary of the Navy Instruction – Implementation of Item Unique Identification within the DoN, dtd 22 Dec 09
m.	SECNAVINST 5239.3B	DoN Information Assurance Policy, 17 Jun 09
n.	SECNAVINST 5510.30	DoN Regulation – Personnel Security Program
o.	SPAWARINST 3432.1	SPAWAR Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
p.	SPAWARINST 4440.12	Management of Operating Materials and Supplies (OM&S), Government Furnished Property (GFP), Contractor Acquired Property (CAP), Property, Plant and Equipment (PP&E), and Inventory
q.	SPAWARINST 5721.1B	SPAWAR Section 508 Implementation Policy, 17 Nov 09
r.	NAVSUP P-723	Navy Inventory Integrity Procedures, April 2012
s.	NIST SP 800-Series	National Institute of Standards and Technology Special Publications 800 Series – Computer Security Policies, Procedures, and Guidelines
t.	COMUSFLTFORCOM/COMPACFLTINST 6320.3A	Commander US Fleet Forces Command/Commander US Pacific Fleet Instruction, Medical Screening For US Govt Civilian Employees, Contractor Personnel, and Guests prior to embarking Fleet Units, of 7 May 13
u.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08
v.	DoD 5220.22-M	DoD Manual – National Industry Security Program Operating Manual (NISPOM)
w.	DoD 5200.2-R	DoD Regulation – Personnel Security Program

	Document Number	Title
x.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12
y.	DoDD 5220.22	DoD Directive – National Industrial Security Program
z.	DoDD 8500.1	DoD Directive – Information Assurance
aa.	DoDI 8500.2	DoD Instruction – Information Assurance (IA) Implementation
bb.	SECNAVINST 5510.30	DoN Regulation – Personnel Security Program
cc.	SPAWARINST 3432.1	SPAWAR Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
dd.	CJCSM 6510.03	Department of Defense Cyber Red Team Certification and Accreditation, dated 2/28/2013
ee.	CJCSM 6510.01B	DoD Cyber Incident Handling Program, dated 7/10/2012
ff.	DoDI O-8530.2	Support to Computer Network Defense (CND), dated 3/9/2001
gg.	NIST SP 800-Series	National Institute of Standards and Technology Special Publications 800 Series – Computer Security Policies, Procedures, and Guidelines

2.2 GUIDANCE DOCUMENTS

The following documents are to be used as guidance. Unless otherwise specified, the document's effective date of issue is the date on the request for proposal.

	Document Number	Title
a.	MIL-HDBK-61A	Configuration Management
b.	MIL-STD-130N	DoD Standard Practice – Identification Marking of US Military Property
c.	MIL-STD-881C	Work Breakdown Structure for Defense Materiel Items
d.	MIL-STD-1916	DoD Test Method Standard – DoD Preferred Methods for Acceptance Of Product
e.	DoDI 3020.41	DoD Instruction – Operational Contract Support (OCS), of 20 Dec 10
f.	DoDI 4161.02	DoD Instruction – Accountability and Management of Government Contract Property, Apr 27,2012
g.	DoDD 5000.01	DoD Directive – The Defense Acquisition System
h.	DoDI 5000.02	DoD Instruction – Operation of the Defense Acquisition System
i.	ISO 9001 (ANSI/ASQ Q9001)	International Organization for Standardization (American National Standard Institute/American Society for Quality) – Quality Management Systems, Requirements
j.	ISO/IEC 12207	International Organization for Standardization/ International Electrotechnical Commission: Systems and Software Engineering – Software Life Cycle Processes
i.	ISO/IEC 15288	International Organization for Standardization/ International Electrotechnical Commission: Systems and Software Engineering – System Life Cycle Processes

	Document Number	Title
j.	IEEE Std 12207-2008	Systems and Software Engineering – Software Life Cycle Processes
k.	ANSI/EIA-748A	America National Standards Institute/Electronic Industries Alliance Standard – Earned Value Management (EVM) Systems
l.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
m.	DTM-08-003	Directive-Type Memorandum 08-003 – Next Generation Common Access Card (CAC) Implementation Guidance, December 1, 2008
n.	FIPS PUB 201-1	Federal Information Processing Standards Publication 201-1 – Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
o.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification
p.	N/A	SSC Atlantic Contractor Checkin portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/Contractor+Checkin
q.	[N/A]	SSC Atlantic OCONUS Travel Guide portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/OCONUS+Travel+Guide
r.	SPAWARSYSCENLANTINST 12910.1A	Deployment of Personnel and Contractor employees to Specific Mission Destinations, 28 Dec 09
s.	N/A	SSC Atlantic Contractor Checkin portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/Contractor+Checkin
t.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
u.	DTM-08-003	Directive-Type Memorandum 08-003 – Next Generation Common Access Card (CAC) Implementation Guidance, December 1, 2008
v.	FIPS PUB 201-1	Federal Information Processing Standards Publication 201-1 – Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
w.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification

2.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents. Specifications and commercial/industrial documents may be obtained from the following sources:

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO., Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor

Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization's website.

3.0 PERFORMANCE REQUIREMENTS

The following paragraphs list all required support tasks that shall be required throughout the contract life. The contractor shall provide necessary resources and knowledge to support the listed tasks within 30 days of award. The contractor shall complete all required tasks while controlling and tracking performance and goals in terms of costs, schedules, and resources.

In the performance of this work, the contractor shall be required to utilize a government provided XenClient computing platform image (http://www.citrix.com/products/xenclient/how-it-works/specifications.html).

In accordance with DoD 8570.01-M many of contractor personnel performing under this TO will require certification at one of the approved baseline certification levels. Certification level is specified for each relevant subtask below. Contractor personnel shall obtain all appropriate certifications prior to beginning work under those sub-tasks.

Note: In compliance with SPAWARINST 4720.1A – SPAWAR Modernization and Installation Policy, all contract installation work performed aboard Navy ships and Navy shore sites is under Installation Management Office (IMO) supervision; otherwise, a formal exemption request has been approved. In accordance with the Fleet Readiness Directorate Standard Operating Procedure (FRD SOP), COMSPAWARSYSCOM letter Ser FRD/235 dated 24 Apr 12, the contractor shall, ensure proper notification and status updates of installation work performed outside of SSC Atlantic respective Areas of Responsibilities (AORs) are provided to the SPAWAR Officer in Charge (OIC) or applicable Geographic Lead.

3.1 PROGRAM MANAGEMENT SUPPORT

3.1.1 Program Management Planning Documentation Development

In support of SSC Atlantic Defense Health tasking the contractor shall provide program management services to include the creation of program management plans (PMP). The contractor shall develop all of the following sections of a program management plan:

- Program Charters
- Change Management
- Plans Work Breakdown
- Structures Risk
- Management Plans
- Roles and Responsibility matrices
- Scope Management Plans
- Statements of Work
    - Staffing Plans
    - Communications Plans
    - Quality Plans

Additionally, the contractor shall assist in the development of schedules and tracking associated with that to include cost and performance tracking. The contractor shall use Earned Value Management (EVM) for the purpose of tracking cost, schedule and performance on projects. Additionally, program support for recording technical meeting minutes and generation of meeting agendas will also be required. (CDRL A001)

CDRL #	Description	PWS Reference Paragraph
A001	Program Management Reports, General	#3.1.1

3.1.2 Program Affordability Management

In support of SSC Atlantic Defense Health tasking the contractor shall assist the government program manager in performing Program Affordability Management studies. The studies will identify, qualitatively characterize, and quantify program costs, benefits and risks. The contractor shall use a repeatable methodology for generating accurate estimates of costs, schedule, scope, and benefits which will increase the reliability of such estimates. Artifacts to assist in the process of determining program affordability will include:

- Analysis of Alternatives (AoA)
- Performance Based Logistics (PBL) Business Case Analysis (BCA) Economic (Cost/Benefit) Analysis
- Cost versus Capability Trade Studies
- Clinger-Cohen Act Compliance Assessments
- Post Deployment Assessments (Benefit Realization Studies)

The contractor shall also provide Program Affordability Management services which will assist the government in developing program budget formulation, budget execution tracking, and unfunded requirements processing in accordance with Financial Management Regulations and the DoD Planning, Programming, Budgeting & Execution System (PPBES). The contractor shall assist in the preparation Office of Management & Budget (OMB) E300 Exhibits, Acquisition Program Baselines, and related financial management documentation. (CDRL A001)

CDRL #	Description	PWS Reference Paragraph
A001	Program Management Reports, General	#3.1.2

3.1.3 Cost Estimation Services

As an important subset of overall program affordability management the contractor shall provide cost estimation services to assist SSC Atlantic in assessing program costs. The contractor shall assist the government in the development of risk-adjusted estimates of life cycle costs and benefits (or opportunity costs) that are then statistically combined to derive economic metrics such Return-

On-Investment (ROI), Benefit Cost Ratio, Payback Period, or Internal Rate of Return (IRR) using present value economic analysis techniques. These metrics will be included with strategic alignment, mission effectiveness, and other non-financial benefit criteria to complete a balanced scorecard evaluation of competing program alternatives. Analysis of alternatives will use the balanced scorecard methodology to support business process improvement initiatives as well as IT portfolio selection, oversight and governance. Analysis of alternatives or business case analysis will allow the SSC Atlantic to compare multiple projects not only on expected costs but also on benefits and business value.

The contractor shall use methodologies for Life Cycle Cost Estimation (LCCE), Life Cycle Benefit Estimation (LCBE), and Economic Analysis (EA) that have been formally reviewed and approved by the Office of the Secretary of Defense (OSD) Director, Cost Assessment & Program Evaluation (DCAPE, formerly Office of the Director, Program Analysis & Evaluation). (CDRL A001)

CDRL #	Description	PWS Reference Paragraph
A001	Program Management Reports, General	#3.1.3

3.1.4 Analysis of Alternatives (Planning, Alternatives Analysis, Reporting, Briefing)

The contractor shall conduct a thorough, detailed, and structured analysis of technical alternatives (AoA).

The AoA approach will include:

- A Review of functional and technical requirements and specifications
- Development of detailed evaluation criteria (cost, benefit, functional, technical, schedule) Established scoring and weighting methodologies
- Development of an AoA Plan
- Coordination and obtaining key stakeholder buy-in to evaluation criteria, scoring methods, weighting, and the overall plan.
- Conducting the structured analysis
- Generating a detailed report with recommendations, along with required technical and executive level briefings

The approach to be used will include generation of draft and final deliverables for Government reviewand approval; and engagement with key stakeholders to ensure consensus with both the process as well as the recommendations at the conclusion of the AoA. (CDRL A001)

CDRL #	Description	PWS Reference Paragraph
A001	Program Management Reports, General	#3.1.4

3.1.5 Trade studies (Technology Assessments and Insertion)

The contractor shall provide resources with a sound understanding of current technologies and technology trends, including systems hardware, software, systems architecture and design strategies, and key technologies of direct relevance and potential value to SSC Atlantic customers.

Combined with market research and an understanding of customer requirements, the contractor shall employ a structured, AoA-type approach when conducting trade studies and trade-off analyses in support of technology assessments, technology refresh initiatives, and the insertion of key technologies into an enterprise to realize a return on investment (ROI). (CDRL A001)

CDRL #	Description	PWS Reference Paragraph
A001	Program Management Reports, General	#3.1.5

3.2 INFRASTRUCUTRE ARCHITECTURE DEVELOPMENT

3.2.1 Architecture, Design, and Senior Engineering Support

The contractor shall provide senior level enterprise architecture consulting services for program supporting Defense Health customers. This support is essential to the establishment of the Medical Community of Interest (Med COI) Network supporting the DHMS Electronic Healthcare Record (EHR). These services will include the development of DoD Architecture (DODAF) artifacts which will include:

- All Viewpoint (AV)
- Capability Viewpoints (CV)
- Data and Information Viewpoint (DIV)
- Operational Viewpoint (OV)
- Project Viewpoint (PV)
- Services Viewpoint (SvcV)
- Standard Viewpoint (StdV)
- Systems Viewpoint (SV)

Additionally, the contractor shall provide network and network protection architectures that are compliant with all DoD Information Assurance (IA) requirements. The contractors shall support these designs/architectures through the DoD certification and accreditation process.

In addition to the development of network and network protection architectures, the contractor shall assist in the development of enterprise datacenter and server computing/service delivery (cloud computing) requirements documents and architecture designs. These requirements documents should leverage industry best practices and the architecture designs must be compliant with all DoD IA requirements.

In support of the integration of DoD networks in support of the EHR, the contractor shall leverage experience in each of these areas listed above to develop:

- Requirements Documents
- Concepts of Operations (CONOPS)
- System specification and design documents
- System implementation plans
- System sustainment plans (CDRL A002)

CDRL #	Description	**PWS Reference Paragraph**
A002	Technical/Analysis Reports, General	#3.2.1

3.2.2 IT Strategic Planning

The contractor shall provide support to senior strategic planning offices within DHA and DHMS. The contractor shall develop IT strategic plans that are mapped to organizational goals and objectives, and that track to capital planning and investment control (CPIC) processes for managing IT investment. This strategic and tactical planning approach must be fully compliant with Office of Management and Budget (OMB) guidelines and directives—and must also be linked into the overall, organizational EA and enterprise lifecycle management (ELM). (CDRL A002)

CDRL #	**Description**	**PWS Reference Paragraph**
A002	Technical/Analysis Reports, General	#3.2.2

3.3 ADVANCED CYBER/INFRASTRUCUTRE DESIGN AND TESTING

DoD 8570.01-M Category – IASAE II certification, with corresponding Operating System certification

3.3.1 Network Protection Infrastructure Design Efforts

The contractor shall apply a systems design approach to the directed efforts to ensure that the mission objectives and criteria requirements of specified systems are fulfilled. Emphasis shall be on the demonstration of clear, definable and auditable duplication of performance, logistics supportability, reliability, and maintainability of the item, subsystems, and systems. The contractor shall also provide demonstration that system designs include consideration for future scalability and adaptability of all item, subsystems, and systems. The contractor shall provide the following support:

Provide Information Assurance (IA) and network engineering support during requirements discussions and definition and contribute to required project meetings as necessary.
Provide security requirements, design, installation and integration recommendations for network and other security systems as defined above.

CDRL #	**Description**	**PWS Reference Paragraph**
A002	Technical/Analysis Reports, General	#3.3.1

3.3.2 Internet Protocol Version 6 (IPv6) Testing

The contractor shall assess each component submitted in a design, used in a lab environment or deployed for production use to determine IPv6 capability. The contractor shall follow the government provided IPv6 Test Plan to determine IPv6 capability. The contactor shall also provide COTS solutions that are IPv6 capable. An IPv6 capable system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific criteria to be deemed IPv6 capable are devices in Conformance to the DoD Information Technology Standards Repository (DISR) developed DoD IPv6 Standards Profile. Systems being developed, procured or acquired shall comply with the Global Information Grid Architecture and DISR standard IPv6 Capable definition.

An IPv6 Capable system must meet the IPv6 base requirements defined in the "DoD IPv6 Standards Profile v3.0" dated June 13, 2008. IPv6 traffic throughput and load testing shall be performed with the government furnished BreakingPoint load tester. (CDRL A002)

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.3.2

3.3.3 Product Evaluations

The contractor shall assess various network protection and infrastructure products against a set of criteria provided by the government. This will include building candidate configurations, testing configurations to validate manufacturer performance and capabilities claims. Performance testing shall be conducted in the government lab utilizing the BreakingPoint load tester. At the completion of the testing, the contractor shall provide a report to the government detailing the results of the testing and a recommendation for product selection. (CDRL A002)

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.3.3

3.4 CYBER/INFRASTRUCUTRE IMPLEMENTATION SUPPORT

3.4.1 Network Protection System Integration

DoD 8570.01-M Category – CND Infrastructure Support certification, IAT II certification, with corresponding Operating System certification

The contractor shall apply a systems design approach to the directed efforts to ensure that the mission objectives and criteria requirements of specified systems are fulfilled. Emphasis shall be on the demonstration of clear, definable and auditable duplication of performance, logistics supportability, reliability and maintainability of the item, subsystems, and systems. The contractor shall also provide demonstration that system designs include consideration for future scalability and adaptability of all item, subsystems, and systems. Preliminary, interim, final assessments, recommendations, and reports shall be delivered as a written technical report. The contractor shall:

- Perform studies, analyze system and/or equipment performance and submit recommendations for development, upgrades, modifications, or alterations of hardware and/or software as appropriate to improve system operation and enhance security posture in the field environment.
- Perform site surveys and deliver survey reports as required to support the installation of Network Infrastructure, Application and Security Systems.
- Recreate scientifically within a laboratory environment an operational environment for local evaluation of field needs. This "modeled" environment may then be manipulated to determine improvements in security posture.
- Perform pre-install population, configuration, and testing of systems.
- Provide onsite engineering support for the installation and upgrade of Network Infrastructure, Application and Security Systems.
- Perform system operation verification test (SOVT) for installed and upgraded systems.

3.5 NETWORK SECURITY OPERATIONS SUPPORT

3.5.1 Network Operations Center Support

DoD 8570.01-M Category – CND Infrastructure Support certification, IAT II certification, with corresponding Operating System certification

The contractor shall work in support of a SSC Atlantic established network operations center. This network operations center will support the security and network components of the MHS Intranet/MedCOI. In support of the network operations center the contractor shall:

Investigate and troubleshoot network and security components of the MHS Intranet/MedCOI infrastructure.
Utilize the designated configuration management system for the MHS Intranet/MedCOI to make all approved configuration changes to MHS Intranet/MedCOI network and security components.

Provide expertise in configuring, maintaining, upgrading and troubleshooting Cisco switches, routers and firewalls, Juniper routers and firewalls, Palo Alto firewalls, F5 load balancers, InfoBlox DNS appliances, Fidelis XPS security appliances, Citrix NetScaler products, McAfee and SourceFire Intrusion Detection and Prevention products and **TACLANE KG-175 series High Assurance IP Encryptors.**

Provide shift work support to enable 24x7 support of the network and security components of the MHS Intranet/MedCOI

Work with manufacturer Tier 3 support to resolve trouble tickets.
Document all work performed in support of trouble tickets using the approved MHS trouble ticketing system.

3.6 COMPUTER NETWORK DEFENSE SERVICES

3.6.1 Cyber Threat Analysis Support

DoD 8570.01-M Category – CND Analyst certification, IAT II certification, with corresponding Operating System certification. Top Secret/SCI clearance required

The contractor shall provide support for the ongoing analysis of threats capable of impacting resources being serviced by the NSOC CNDSP activity based on review of programmatic, technical, and IA Certification and Accreditation documentation and daily review of open source / unclassified and classified threat warnings and bulletins. Individuals will have at least two years of experience in CND technology or a related field. Specifically, the contractor shall: (CDRL A002)

- Execute, draft, edit, and maintain standard operating procedure (SOP) documentation.
- Review IA certification and accreditation documentation, programmatic, and technical documentation for the NSOC and Network Protection Suites
- Review IA certification and accreditation documentation, programmatic, and technical documentation for each system or program of record serviced by the NSOC CNDSP
- Review the SOPs and CNDSP programmatic documentation for the NSOC
- Perform daily review of cyber threat warnings, bulletins, alerts, and incident reporting documentation and databases produced by the Director of National Intelligence (DNI), National Intelligence Counsel (NIC), Defense Intelligence Agency (DIA), National Security Agency (NSA), United States Strategic Command (USSTRATCOM), United States Cyber Command (USCYBERCOM), military service cyber intelligence support activities, Central Intelligence Agency, Department of Homeland Security, US Computer Emergency Response Team, and coalition and allied partners.
- Perform daily review of open source / unclassified sources of cyber threat warnings, vulnerability announcements, from the DoD Information Assurance Vulnerability Management program, National

Institute of Standards and Technology (NIST) National Vulnerability Database (NVD), SANS Institute and Internet Storm Center, security vendor advisories, and other cyber security new media sources for information that may impact operations

- Perform analysis and identify threats, vulnerabilities, or change to the level of risk associated with continued operations. Assess the level of threat associated with the circumstances and provide reporting to CNDSP management. Reporting shall include specific information and sources used in the analysis, summary information, threat content, and recommendations for managing, mitigating, or avoiding the associated risk associated with the threat.
- Communicate to CNDSP subscribers the results of the threat analysis and the associated reporting. Assist CNDSP subscribers with comprehending the reporting, perform supplemental research, and guidance on implementing the prescribed risk mitigation strategy.
- Coordinate and deconflict threat analysis activities and reporting with existing NSOC IAVM program infrastructure.
- Coordinate the results of threat analysis with the current network monitoring resources for the creation of user defined signatures and other alerting capabilities as necessary to manage risks
- Obtain 'known-bad' file hash value lists of malicious activity from classified and open source resources and coordinate with NSOC HBSS and network monitoring resources the incorporation of this new data for continued monitoring
- Mentor junior cyber threat analysts and assist with construction of a robust cyber threat analysis capability in the NSOC
- Provide on-call support for mission critical activities during non-core business hours consistent with CNDSP requirements.
- Participating in program reviews and onsite certification evaluations
- Coordinate with Incident Response, IAVM, CND Analysis, Fusion, and Monitoring, and CND Infrastructure Support staff as necessary to meet CNDSP requirements.

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.6.1

3.6.2 IA Vulnerability Management and Vulnerability Management System Support

DoD 8570.01-M Category – CND Auditor certification and IAT II or IAT III certification, with corresponding Operating System certification.

Lead and directly participate in activities traditionally associated with the DoD Information Assurance Vulnerability Management (IAVM) program. Primarily responsible for routine, DoD SCVVI tool, VMS operations; assuring and tracking compliance with IAVM messages and USCYBERCOM directives; and performing liaison with military health service (MHS) medical applications being serviced by the Network Security Operations Center (NSOC) Computer Network Defense Service Provider (CNDSP). Also register and maintain the compliance status of all operational network protection (NP) related hardware and software, including NPS components deployed to Service MTFs, the MHS Intranet, and other MHS data centers supported by DHA. Specifically, the contractor shall:

- Execute, draft, edit, and maintain standard operating procedure (SOP) documentation.
- Perform Vulnerability Management Service (VMS) configuration, use, populating with DoD SCVVI tool results, and report generation to support the IAVM program
- Perform DoD SCVVI tool and manager servers and performing associated monthly and ad-hoc scans as required on the Network Protection Suites (NPS) and DHA owned and managed systems located in the MHS DMZs, MHS Intranet, or MHS Enclaves. Such scans and associated IAVM compliance reporting shall be tailored to meet the needs of the individual Program Management Office (PMO)
- Manage, disseminate, interpret, and track compliance with IAVM associated messages including Alerts (IAVA), Bulletins (IAVB), and (IAVT) Technical Bulletins
- Test available vendor provided patches or remediation procedures in the DHA IA lab for issues prior to implementation in the production environment. Documenting installation procedures and distributing

these procedures to DHA sites and other POCs for their use

- Obtain from supported entities required security policy compliance documentation and artifacts; assess compliance with requirements; and develop Plans of Action and Milestone (POA&M) documentation for any DHA owned or managed assets that cannot be patched as necessary to achieve IAVM compliance Implement a DoD IAVM program utilizing risk management principals
- Assume responsibility for the NSOC's execution of the DoD IAVM program and oversee and direct the activities for a team of support analysts
- Maintain existing standard operational procedure (SOP) documents and draft new SOPs as necessary Participate in and contribute to regularly scheduled NSOC meetings
- Provide status reports on IAVM activities
- Provide status reports on NSOC CNDSP supported entities' INFOCON compliance status
- Support the NSOC's CNDSP 24x7 Watch capabilities by executing IAVM-related duties consistent with CNDSP requirements during non-core business hours as needed. Duties include monitoring, acknowledging receipt, obtaining status, perform liaison and analysis as necessary, and report compliance with USCYBERCOM directives including INFOCONs, OPORDs, WARNORDs, ODMs, CTOs, and NTDMs Participating in program reviews and onsite certification evaluations
- Coordinate with Incident Response, Cyber Threat Analyst, CND Analysis, Fusion and Monitoring, HBSS support, Incident Response, and CND Infrastructure Support staff as necessary to meet CNDSP requirements

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.6.2

3.6.3 Host Based Security System (HBSS) Support

DoD 8570.01-M Category – CND Infrastructure Support certification, IAT II certification, with corresponding Operating System certification

The contractor shall configure, install, host and perform operations and maintenance for the NSOC's HBSS ePolicy Orchestrator servers and client-side application system components, as well as support the implementation and maintenance of HBSS for the NSOC's systems and other tools used by for management of the network protection suites and MHS Intranet. The operations and maintenance of the NSOC's HBSS resources are critical and facilitate comprehensive CND monitoring via the NSOC's security event and incident management (SEIM) analysis tools. Specifically, the contractor shall:

- Execute, draft, edit, and maintain standard operating procedure (SOP) documentation.
- Provide support and technical assistance to MHS applications and program of record systems' established configuration management bodies to facilitate those systems' participating in the NSOC's current HBSS implementation. This includes installing, configuring, troubleshooting, testing, and providing instruction to system administrators and configuration managers on how to configure HBSS without suffering unacceptable performance degradation.
- Participating in program reviews and onsite certification evaluations
- Coordinate with Incident Response, Cyber Threat Analyst, CND Analysis, Fusion and Monitoring, IAVM, and CND Infrastructure Support staff as necessary to meet CNDSP requirements (CDRL A002)

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.6.3

3.6.4 IA Program Management Support

DoD 8570.01-M Category – IAM Level I or IAM II certification

The contractor shall correspond with DHA, MHS health application Program Management Offices, Configuration Management Boards, Certification Authorities, and Designated Accrediting Authorities, and other NSOC CNDSP-supported entities to ensure documentation vitally necessary to the NSOC CNDSP staff for the accomplishment of the mission is obtained and updated as necessary. Specifically, the contractor shall:

- Execute, draft, edit, and maintain standard operating procedure (SOP) documentation.
- Solicit, obtain, track, and coordinate the proper use of certification and accreditation documentation from supported MHS Health by the NSOC CNDSP from supported entities
- Perform requirements analysis for NSOC CNDSP subscribers' educational/training/awareness requirements and needs. Coordinate with supported entities' training providers to ensure annual IA training materials are prepared and delivered. Also delivering this required training to supported entities, if necessary, and tracking the compliance status of individual supported entities
- Coordinate with CND Analysis, Fusion, and Monitoring, Incident Response, Cyber Threat Analyst, IAVM, HBSS support, CND Infrastructure Support, and CNDSP Management staff as necessary to meet CNDSP requirements
- Correspond with DHA, USCYBERCOM, CC/S/As, NSOC supported entities, and other third parties as necessary to ensure CNDSP liaison and reporting requirements are satisfied. This includes vulnerability, threat, remediation, mitigation & lessons-learned, situational awareness, scheduled
- outages and routine administrative CNDSP matters
- Perform requirements analysis associated with ongoing CNDSP operations, develop POA&Ms, and draft resource requirement and management plans
- Utilize the NSOC's KBS portal to ensure efficient communications with third parties
- Maintain and update the NSOC CNDSP organization chart and POC and Recall Rosters for the NSOC CNDSP, NSOC CNDSP supported entities, antivirus and Commercial Off The Shelf (COTS) security products vendors, supported IAVM entities, Intelligence community, law enforcement / counter intelligence community, CND technical experts in other DoD organizations, and DoD Privacy office Maintain the current NSOC CNDSP Application Package and ensure the resulting POA&M document and associated SOPs are updated and accurate
- Coordinate with SPAWAR command POCs and NSOC managers as appropriate to obtain and maintain NSOC's DoD 8570.01-M certification compliance and report status
- Maintain the NSOC CNDSP's annual activities and shared situational awareness calendar on the KBS portal
- Maintain appointment letters (e.g. Designated Approving Authority, Certification Authority, IAM, and IAO positions) for key NSOC CNDSP personnel and supported entities or subscribers
- Maintain and track the NSOC CNDSP's compliance with CJCSM 6510.01 requirements for privileged access and are Level 1 certified
- Maintain NSOC CNDSP's prospective employee and contractor screening and verification of qualifications records
- Participating in program reviews and onsite certification evaluations (CDRL A002).

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.6.4

3.6.5 CND Analysis, Fusion, and Monitoring Support

DoD 8570.01-M Category – CND Analyst certification, IAT II certification, with corresponding Operating System certification. Top Secret/SCI clearance required

The contractor shall provide network intrusion detection and monitoring, HBSS-related monitoring, correlation analysis using the NSOC's security event and incident management (SEIM) analysis tools, and support as required for the fielded CND Analysis Suite for subscribers of the Network Security Operations Center (NSOC) Computer Network Defense Service Provider (CNDSP) and other supported components. Specifically, the contractor shall:

- Execute, draft, edit, and maintain standard operating procedure (SOP) documentation.
- Provide coordination of significant incidents with USCYBERCOM and supported entities to ensure proper analysis is performed and timely and accurate reporting of the incident is affected.
- Provide, develop, and maintain a network forensic analysis capability to enhance response to, support of, and investigation into significant incidents to provide a clearer view of the exploits, vulnerabilities, and tactics, techniques, and procedures (TTPs) used to cause the incident.
- Provide support for the NSOC's CND Analysis, Fusion, and Monitoring 24x7 support capability during non-core business hours consistent with CNDSP requirements as needed
- Participating in program reviews and onsite certification evaluations
- Coordinate with Incident Response, Cyber Threat Analyst, IAVM, HBSS support, and CND Infrastructure Support staff as necessary to meet CNDSP requirements (CDRL A002)

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.6.5

3.6.6 Computer Network Defense Incident Response Analysis and Support

DoD 8570.01-M Category – CND Incident Responder and IAT II certification, with corresponding Operating System certification. Top Secret/SCI clearance required

The contractor shall provide computer network defense incident response and support, correlation analysis, and support for the fielded CND analysis suite for subscribers of the Network Security Operations Center (NSOC) Computer Network Defense Service Provider (CNDSP) and other supported components. Also assist with the maintenance of current NSOC CNDSP SOPs and support to CND Analysis, Fusion and Monitoring group. Specifically, the contractor shall:

- Execute, draft, edit, and maintain standard operating procedure (SOP) documentation.
- Maintain existing NSOC Incident Response SOP ensure associated documentation and capabilities remain compliant with CJCSM 6510.01A and other applicable policy directives
- Ensure incidents are properly entered into appropriate automated reporting systems
- Provide coordination of significant incidents with USCYBERCOM and supported entities to ensure proper analysis is performed and timely and accurate reporting of the incident is affected. Ensure incidents are properly entered into appropriated automated reporting systems
- Provide, develop, and maintain a forensic capability to enhance response to, support of, and investigation into significant network incidents in order to provide a clearer view of the exploits, vulnerabilities, and
- TTPs used to cause the incident.
- Provide support for the NSOC's Incident Response 24x7 support capability during non-core business hours consistent with CNDSP requirements as needed
- Provide network forensics support to the NSOC's CND Analysis, Fusion, and Monitoring capability Participating in program reviews and onsite certification evaluations
- Coordinate with CND Analysis, Fusion, and Monitoring, Cyber Threat Analyst, IAVM, HBSS support, and CND Infrastructure Support staff as necessary to meet CNDSP requirements (CDRL A002)

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.6.6

3.6.7 Computer Network Defense Service Provider Manager Support

DoD 8570.01-M Category – CND-SP Manager and IAM I or IAM II certified. Top Secret/SCI clearance required

Contractor shall act as CND–SP Manager which oversee the CND-SP operations within their organization. CND-SP

Managers are responsible for producing guidance for their network enclave or enclave, assisting with risk assessments and risk management for organizations within their network enclave or enclave, and are responsible for managing the technical classifications within their organization. Specifically, the contractor shall:

- Execute, draft, edit, and maintain standard operating procedure (SOP) documentation.
- Implement and enforce CND policies and procedures reflecting applicable laws, policies, procedures, and regulations
- Manage the publishing of CND guidance (e.g., IAVAs and TCNOs) for the enclave constituency.
- Provide incident reports, summaries, and other situational awareness information to higher headquarters. Manage an incident (e.g., coordinate documentation, work efforts, resource utilization within the organization) from inception to final remediation and after action reporting.
- Manage threat or target analysis of CND information and production of threat or target information within the network or enclave environment.
- Manage the monitoring of external CND data sources to maintain enclave situational awareness. Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other CND information.
- Lead risk analysis and management activities for the network or enclave environment.
- Track compliance audit findings, incident after-action reports, and recommendations to ensure appropriate mitigation actions are taken.
- Participating in program reviews and onsite certification evaluations
- Coordinate with CND Analysis, Fusion, and Monitoring, Cyber Threat Analyst, HBSS support, Incident Response, CND Infrastructure Support, IAVM, and External Assessment staff as necessary to meet CNDSP requirements

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.6.7

3.7 ADVERSARIAL ASSESSMENT SUPPORT

3.7.1 DOD CYBER RED TEAM OPERATIONS SUPPORT

DoD 8570.01-M Category – CND Auditor certification and IAT II or IAT III certification, with corresponding Operating System certification. Top Secret/SCI clearance required

The contractor shall support the USSTRATCOM accredited Red Team at SSC Atlantic which performs adversarial assessments against subscriber networks. The red team shall be used to assess the network and system security posture of MedCOI connected sites. The contractor shall work as part of the red team to support onsite and remote assessments. Specifically, the contractor shall:

- Develop custom code to penetrate network and system defenses to include development of malware, root kits and remote access tools
- Develop tactics, techniques and procedures for network penetration and data exfiltration Develop phishing and spear phishing campaigns
- Conduct open source research on target sites and personnel to include use of pre-texting as allowed under the SSC Atlantic red team authorities
- Participate in developing after action reports, out briefs and vulnerability mitigation recommendations. Utilize compromised assets to conduct playbooks in order to assess effectiveness of detection and response capabilities of the Computer Network Defense Service Provider.
- Support maintenance of red team processes to ensure continuing accreditation of red team in accordance with CJCSM 6510.03.
- Support the creation and maintenance of a persistent penetration testing network that can be used to originate phishing campaigns and handle command and control communications across the DoD Information Network boundaries.
- Conduct penetration testing of equipment (hardware and software) being planned for use by the by the

Computer Network Defense Service Provider in defense of the MedCOI network. (CDRL A002)

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.7.1

3.7.2 CYBER RED TEAM INFRASTRUCTURE

In support of the red team the contractor shall provide a non-attributable network that can be utilized to conduct campaigns/operations against targeted subscriber infrastructure. By the nature of the methods to be utilized as part of the red team operations, this network shall be provided using a commercial Internet and computing service provider. (CDRL A002)

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.7.2

3.8 APPLICATION SUPPORT

3.8.1 HAIMS Support

DoD 8570.01-M Category –IAT I or II certification, with corresponding Operating System certification.

The contractor shall support Healthcare Artifact and Image Management Solution (HAIMS) server installation, upgrade, integration, and functional testing. As a result, the contractor shall field teams of qualified personnel that are subject matter experts and experienced in installation, upgrade and functional testing of HAIMS infrastructure and software. These installation upgrade and testing efforts will include server builds and testing, VMware configurations, and network and server system configurations.

3.8.1.1 HAIMS Site Surveys

The contactor shall provide qualified and experienced subject matter experts on-site to complete the following tasks at site facility and computer data centers:

- Perform site surveys and deliver survey reports as required to support the installation of HAIMS hardware. Results to include: rack spacing, power and cooling requirements, and Network Protection Suite (NPS) bandwidth analysis.
- Provide on-site surveys to evaluate and document requirements for hardware installations. Provide bandwidth analysis and document results as required.

3.8.1.2 HAIMS Server Installation, Upgrades, Integration and Functional Testing

The contactor shall provide qualified and experienced subject matter experts on-site to perform installation, upgrade and testing of HAIMS hardware, Operating System (OS), and required HAIMS software.

- Provide on-site hardware installations, upgrades of OS and software for Sustainment of fielded systems. Provide qualified and experienced subject matter experts on-site to integrate and conduct functional tests for HAIMS software and servers.
- Integrate and test systems upgraded.
- Convert systems from satellite HAIMS systems to Regional Repository systems
- Prepare installation, upgrade and integration documentation reports as required.
- Prepare post site deliverable reports as well as System Operation Verification Test (SOVT) for integrated and upgraded systems.

3.8.1.3 HAIMS System Integration

The contractor shall apply a systems design approach to the directed efforts to ensure that the mission objectives and

criteria requirements of specified systems are fulfilled. Emphasis shall be on the demonstration of clear, definable and auditable duplication of performance, logistics supportability, reliability and maintainability of the item, subsystems, and systems. The contractor shall also provide demonstration that system designs include consideration for future scalability and adaptability of all item, subsystems, and systems. Designs shall adhere to the principles of the Acquisition Reform Program. Preliminary, interim, final assessments, recommendations, and reports shall be delivered as a written technical report. The contractor shall:

- Recreate scientifically within a laboratory environment an operational environment for local evaluation of field needs. This "modeled" environment may then be manipulated to determine improvements in security posture.
- Perform Network Infrastructure, Application and Security System COTS product review and evaluations. Perform pre-install population, configuration, and testing of systems.
- Provide onsite engineering support for the installation and upgrade of HAIMS systems. Perform system operation verification test (SOVT) for installed and upgraded systems. Provide Tier III help desk support for installed HAIMS systems

3.8.1.4 HAIMS System Training

The contractor shall train Government and new personnel relative to the operation and maintenance of the installed subsystems. When onsite installations are performed, the contractor shall also provide training to onsite personnel on the operation and maintenance of the fielded systems.

3.8.1.5 HAIMS Application Support

The contractor shall provide Tier III support by providing 24x7 subject matter expert (SME) support for the HAIMS system and infrastructure as well as system administration support for the VMware system configurations. Support for the HAIMS VMware environment and application systems will be 24x7 Monday through Sunday. The MHS NSOC will be responsible for monitoring the systems on a 24x7 basis and will escalate to Tier 3 support as needed.

The contractor shall provide system administration level support of the HAIMS software and will escalade to the Application developers as needed. Root level system administrator functions will be provided such as an administrator account for management and system backup. The contractor shall provide support for troubleshooting all infrastructure related issues to the HAIMS system. This will include network, server hardware, operating system, and virtualization technology supporting the operating systems. This will not include application development or problems resulting from faults within the application. Once troubleshooting reveals an application level error/issue, those tickets will be transferred to the HAIMS developers.

3.8.2 Enterprise Directory Services Support

DoD 8570.01-M Category –IAT I or II certification, with corresponding Operating System certification.

The contractor shall provide directory services to all authorized Joint Active Directory (JAD) DHA users. Directory Service users are personnel from Defense Health Agency, medical centers, hospitals, clinics, support and other commands that support the delivery and provision of military healthcare. The users are located worldwide and need access to this service at all times from different time zones. These personnel rely on Directory Services for Authentication and Access Control. This tasking includes configuration, management and support of the Defense Health Agency Joint Active Directory (JAD) forest, Management of "trusts" between the Army Medicine, Navy Medicine and External Organizations, Group Policy Support, and Domain Name Service (DNS) Support. Support will also include:

- Administration, troubleshooting and support for the JAD authentication and access control of systems and users enterprise-wide.
- Centralized control of system accounts and passwords and password recovery capability for Enterprise Service (ES) components.
- Control and log access to critical components of the ES architecture by Organizational Unit (OU)

administrators and other authorized users.

- Administration, troubleshooting and support for the JAD Forest Management Management of the forest root domain
- Sustainment and overall maintenance of the schema
- Administration, troubleshooting and support for JAD Trust Management
- Establish and maintain 'trusts' between the JAD Enterprise Forest and External Organizations as directed by the government project lead and following the guidance provided in the Information Management/Information Technology (IM/IT) Standards Manual
- Administration, troubleshooting and support for JAD Group Policy
- Contractor shall provide Group Policy management and administration of Default Domain Policies for the Enterprise, to be used primarily for the centralized administration of resources. Provide backup and recovery support of site group policies.
- Administration, troubleshooting and support for JAD Domain Name Service (DNS) systems and services
- Shall provide support to maintain the DNS requirements (both internal and external) of the ES AD/Exchange environments.
- Management of the multiple DNS records required for ES
- Administration, troubleshooting and support for JAD Windows Internet Name Service (WINS) systems and services
- Provide support to maintain the Enterprise WINS requirements for the DHA environment Provide WINS service at the enterprise level only
- Conduct Information Assurance Vulnerability Alert (IAVA) Management services following DHA validation process for all Enterprise devices under this task

3.8.3 APPLICATION VIRTUALIZATION SUPPORT

As part of the application delivery within the DHA, SSC Atlantic has developed and deployed an application hosting platform which utilizes Citrix XenApp to support thin delivery of DHA applications to end users quickly, securely and with minimal dependence on end user computing platform specifications. In support of this the contractor shall:

- Support the development of application delivery utilizing Citrix XenApp software
- Troubleshoot and resolve application errors and issues that arise from applications operating within the XenApp environment
- Monitor and troubleshoot performance related issues with XenApp virtualized applications. Develop support for application credentials to be delivered via single sign-on technology Support implementation and troubleshooting of Kerberos Constrained Delegation for XenApp environments

CDRL #	Description	PWS Reference Paragraph
A002	Technical/Analysis Reports, General	#3.8

3.9 Property/Inventory Tracking

3.9.1 In accordance with FAR 52.245-1, the contractor shall create and maintain internal records of all government property accountable to the TO, including Government-furnished and Contractor- acquired property. Each item delivered and/or ordered shall be recorded in an inventory tracking report (CDRL A017). At a minimum, the report shall track the following information: item description, order date, serial number, model number, lot number, delivery location, and the manufacturer warranty period and expiration date, if applicable. This information shall be tracked and available for government review as needed, and the information shall have the ability to be sorted and manipulated by any of the input fields. Separate from the government tracking system, the information in the contractor's records is a backup to the government records; therefore, the government shall own all data rights to the collected information.

5.4.3.2 The contractor shall provide a monthly Integrated Program Management Report (IPMR) (A010) which combines the Contract Performance Report (CPR) with the Integrated Master Schedule (IMS) into a single report. Specific requirements are noted in CDRL DD Form 1423 and DID DI-MGMT-81861 where Formats 1-7 are required.

5.4.4 For program dollar values equal to or exceeding $20M, Schedule Risk Assessment is optional. For program dollar values equal to or exceeding $50M, Schedule Risk Assessment is required.

5.4.5 The contractor shall engage jointly with the Government's program manager in Integrated Baseline Reviews (IBRs) to evaluate the risks inherent in the TO's planned performance measurement baseline. Initially, this shall occur as soon as feasible but not later than six months after TO award, and subsequently, following all major changes to the baseline. Each IBR should verify that the contractor is using a reliable performance measurement baseline, which includes the entire TO scope of work, is consistent with TO schedule requirements, and has adequate resources assigned. Each IBR should also record any indications that effective Earned Value Management (EVM) is not being used. IBRs should also be conducted on subcontracts that meet or exceed the EVM threshold. The prime contractor shall lead the subcontractor IBRs, with active participation by the Government.

6.0 QUALITY

6.1 QUALITY SYSTEM

Upon TO award, the prime contractor shall have and maintain a quality assurance process that meets TO requirements and program objectives while ensuring customer satisfaction and defect-free products/process. The quality system shall be documented and contain procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system based on a contractor's internal auditing system. Thirty (30) days after TO award, the contractor shall review and concur to the Quality Assurance Surveillance Plan (QASP) and any other quality related documents (A011) as required in the TO. The quality system shall be made available to the government for review at both a program and worksite services level during predetermined visits.

Existing quality documents that meet the requirements of this TO may continue to be used. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan and development of quality related documents as needed. At a minimum, the contractor's quality system shall meet the following key criteria:

- Establish documented, capable, and repeatable processes Track issues and associated changes needed
- Monitor and control critical product and process variations Establish mechanisms for feedback of field product performance
- Implement and effective root-cause analysis and corrective action system Establish methods and procedures for continuous process improvement

6.2 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified by the respective WBS, POA&M, or quality system, and the contractor shall deliver related quality plan/procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related services, documents, and material in a category when noncompliance is established.

6.3 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as

assigned and identified by the respective WBS, POA&M, or quality system, and the contractor shall submit related quality objective evidence upon request. Quality objective evidence (A011) shall include any of the following as applicable:

<!--[if !supportLists]-->· <!--[endif]-->Detailed incoming receipt inspection records

<!--[if !supportLists]-->· <!--[endif]-->First article inspection records

<!--[if !supportLists]-->· <!--[endif]-->Certificates of Conformance

<!--[if !supportLists]-->· <!--[endif]-->Detailed sampling inspection records based upon MIL-STD-1916 (Verification Level III)

<!--[if !supportLists]-->· <!--[endif]-->Quality Measurement and Analysis metrics/data

The Government reserves the right to perform any inspections or pull samples as deemed necessary to assure that the contractor provided services, documents, material, and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

6.4 QUALITY MANAGEMENT DOCUMENTATION

In support of the TO's Quality Assurance Surveillance Plan (QASP) and Contractor Performance Assessment Reporting System (CPARS), the contractor shall provide the following documents: Cost and Schedule Milestone Plan (A012) submitted 10 days after TO award, and Contractor CPARS Draft Approval Document (CDAD) Report (A013) submitted monthly.

7.0 DOCUMENTATION AND DELIVERABLES

7.1 CONTRACT DATA REQUIREMENT LISTINGS (CDRLs)

The following CDRL listing identifies the data item deliverables required under this TO and the applicable section of the PWS for which they are required. Section J includes the DD Form 1423s

that itemize each Contract Data Requirements List (CDRL) required under the TO. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs generated under each task. No CDRL classified TOP SECRET with SCI shall be developed.

CDRL #	Description	PWS Reference Paragraph
A001	Program Management Reports, General	3.1
A002	Technical/Analysis Reports, General	3.2, 3.3, 3.6,
A003	Task Order Status Report (TOSR)	5.2.1.1, 8.1.2
A004	Task Order Closeout Report	5.2.1.2, 11.5
A005	Cyber Security Workforce (CSWF) Report	5.2.1.3, 8.1.2
A006	Contractor Manpower Quarterly Status Report (QSR)	5.2.1.4
A007	Invoice Support Documentation	5.2.1.5
A008	Limitation Notification & Rationale	5.2.1.6, 5.2.1.7
A009	Contract Work Breakdown Structure (CWBS)	5.4.3.1
A010	Integrated Program Management Report (IPMR)	5.4.3.2
A011	Quality Documentation	6.1, 6.3
A012	Cost and Schedule Milestone Plan	6.4
A013	Contractor CPARS Draft Approval Document (CDAD) Report	6.4

A014	OCONUS Deployment Documentation and Package	14.4
A017	Inventory Tracking Report	3.9.1

7.2 ELECTRONIC FORMAT

At a minimum, the Contractor shall provide deliverables electronically by email; hard copies are only required if requested by the government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, and etc., are provided in a format approved by the receiving government representative. All data shall be provided in an editable format compatible with SSC Atlantic corporate standard software configuration as specified below.

Contractor shall conform to SSC Atlantic corporate standards within 30 days of TO award unless otherwise specified. *The initial or future upgrades costs of the listed computer programs are not chargeable as a direct cost to the government.*

	Deliverable	**Software to be used**
a.	Word Processing	Microsoft Word
b.	Technical Publishing	PageMaker/Interleaf/SGML/ MSPublisher
c.	Spreadsheet/Graphics	Microsoft Excel
d.	Presentations	Microsoft PowerPoint
e.	2-D Drawings/ Graphics/Schematics (new data products)	Vector (CGM/SVG)
f.	2-D Drawings/ Graphics/Schematics (existing data products)	Raster (CALS Type I, TIFF/BMP, JPEG, PNG)
g.	Scheduling	Microsoft Project
h.	Computer Aid Design (CAD) Drawings	AutoCAD/Visio
i.	Geographic Information System (GIS)	ArcInfo/ArcView
j.	Monthly Task Order Reports	Health System Financial/Contract Tool

7.3 INFORMATION SYSTEM

7.3.1 Electronic Communication

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the government. The contractor shall be capable of Public Key Infrastructure client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on TO shall be accessible by email through individual accounts during all working hours.

7.3.2 Information Security

The contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. Unclassified DoD information shall only be disseminated within the scope of assigned duties and with a clear expectation that confidentiality will be preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

7.3.2.1 Safeguards

The contractor shall protect government information and shall provide compliance documentation validating they are meeting this requirement. The contractor and all utilized subcontractors shall abide by the following safeguards:

a. Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.
b. Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.
c. Sanitize media (e.g., overwrite) before external release or disposal.
d. Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. NOTE: Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with

   ASD-NII/DOD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage." Solutions shall meet FIPS 140-2 compliance requirements.

e. Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.
f. Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application- provided password protection level encryption.
g. Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.
h. Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).
i. Provide protection against computer network intrusions and data exfiltration, minimally including the following:

1. Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware

1. Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

2. Prompt application of security-relevant software patches, service packs, and hot fixes.

a. As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).
b. Report loss or unauthorized disclosure of information in accordance with contract or agreement requirements and mechanisms.

7.3.2.2 Compliance

The contractor shall include in their quality processes procedures that are compliant with information security requirements.

8.0 SECURITY

8.1 ORGANIZATION

8.1.1 Security Classification

As specified in clause 5252.204-9200, classified work shall be performed under this TO. The contractor shall have at the time of TO award and prior to commencement of classified work, a TOP SECRET with Sensitive Compartment Information (SCI) access facility security clearance (FCL).

The following PWS task(s) requires access to classified information up to the level of SECRET: 3.2, 3.3, 3.4, 3.5, 3.6 (with exceptions) and 3.8. The following PWS task(s) requires access to classified information up to the level of TOP SECRET/SCI: 3.6.1, 3.6.5, 3.6.6, 3.6.7 and 3.7. PWS task(s) Para 3.1 do not required access to classified information. The SECRET level tasking involves access to SIPRNet requiring a SECRET level clearance is required for that access. For the TOP SECRET/SCI tasking, access to intelligence information, JWICS/NSANet and weekly meetings held at the SCI level are required necessitating the need for the clearance. Clearance is required to access and handle classified and personal personnel material, attend program meetings, and/or work within restricted areas unescorted. Access to SCI will be limited to U.S. Government Facilities or other U.S. Government sponsored SCI Facilities (SCIFs) authorized on the DD254. Generation of SCI deliverables is not authorized.

8.1.2 Security Officer

The contractor shall appoint a Security Officer to support those contractor personnel requiring access to government facility/installation and/or access to information technology systems under this TO. The Security Officer shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on contract. Responsibilities include entering and updating the personnel security related and mandatory training information within the Staffing Plan document, which is part of TOSR Attachment 1 (A003) – applicable Staffing Plan sheets include: Security Personnel Tracking sheet, CAC SPAWAR Badge Tracking sheet, Mandatory Training Sheet. If applicable, Security Officer shall also update and track CSWF data (CDRL A005).

8.2 PERSONNEL

The contractor shall conform to the security provisions of DoD 5220.22M – National Industrial Security Program Operating Manual (NISPOM), SECNAVINS T 5510.30, DoD 8570.01M/DoD-8140, and the Privacy Act of 1974. Prior to any labor hours being charged on contract, the Contractor shall ensure their personnel possess and can maintain security clearances at the appropriate level(s), and are certified/credentialed for the Information Assurance Workforce (IAWF)/Cyber Security Workforce (CSWF), as applicable. At a minimum, the contractor shall validate that the background information provided by their employees charged under this TO is correct, and the employee shall hold a minimum of a trustworthy determination. *Cost to meet these security requirements is not directly chargeable to task order.*

NOTE: Prior to commencement of work on this TO, all contractor personnel (including administrative and subcontractor personnel) shall have, at a minimum, a favorable Trustworthiness Determination, which is determined by a National Agency Check with Local Agency Check and Credit Check (NACLC) and favorable FBI fingerprint checks. If a final determination is made that an individual does not meet or cannot maintain the minimum standard for a Public Trust Position, then the individual will be permanently removed from SSC Atlantic facilities, projects, and/or programs. If an individual who has been submitted for a security clearance is "denied" for a clearance or receives an "Interim Declination" that individual shall be removed from SSC Atlantic facilities, projects, and/or programs until such time as the investigation is fully adjudicated or the individual is resubmitted and is approved. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on task and contract.

8.2.1 Personnel Clearance

The majority of personnel associated with this TO shall possess a SECRET clearance although some personnel shall require personnel having higher clearance levels such as TOP SECRET with SSBI. At the Government's request, on a case-by case basis, Top Secret (TS) clearances that consist of a Single Scope Background Investigation (SSBI) shall be eligible for access to Sensitive Compartmented Information (SCI). These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data as required. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the Defense Industrial Security Clearance Office (DISCO) and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as required by DoDD 8500.1, Information Assurance and DoDI 8500.2, Information Assurance (IA) Implementation. Any future revision to the respective directive and instruction shall be applied to the TO level as required. Contractor personnel shall handle and safeguard any unclassified but sensitive and classified information in accordance with appropriate Department of Defense security regulations. Any security violation shall be reported immediately to the respective Government Project Manager.

8.2.2 Access Control of Contractor Personnel

8.2.2.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the government facility/installation.

a. The majority of government facilities require contractor personnel to have an approved visit request on file at the facility/installation security office prior to access. The Contractor shall initiate and submit a request for visit authorization to the COR in accordance with DoD Manual 5220.22M (NISPOM) not later than one (1) week prior to visit – timeframes may vary at each facility/installation. For admission to SPAWARSYSCEN Atlantic facilities/installations, a visit request shall be forwarded via Space and Naval Warfare Systems Center Atlantic, P.O. Box 190022, North Charleston, SC 29419-9022, Attn: Security Office, for certification of need to know by the specified COR. For visitation to all other govt. locations, visit request documentation shall be forwarded directly to the on-site facility/installation security office via approval by the COR.
b. Depending on the facility/installation regulations, contractor personnel shall present a proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement.

NOTE:
SPAWARSYSCEN Atlantic facilities located on Joint Base Charleston require a Common Access Card (CAC) each time physical installation access is required. Contractor shall contact SPAWARSYSCEN Atlantic Security Office directly for latest policy.

c. As required, a temporary or permanent automobile decal for each contractor personnel may be issued. The contractor assumes full responsibility for the automobile decal and shall be responsible for the return and/or destruction of the automobile decal upon termination of need or of personnel.
d. All contractor persons engaged in work while on Government property shall be subject to inspection of their vehicles at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location

8.2.2.2 Identification and Disclosure Requirements

As required in DFARS 211.106, Contractors shall take all means necessary to n o t represent themselves as government employees. All Contractor personnel shall follow the identification and disclosure requirement as specified in clause 5252.237-9602.

8.2.2.3 Government Badge Requirements

As specified in contract clause 5252.204-9202, some contract personnel shall require a government issued picture badge. While on government installations/facilities, contractors shall abide by each site's security badge requirements. Various government installations are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards. Contractors are responsible for obtaining and complying with the latest security identification requirements for their personnel as required. Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, and/or SF85P for CAC card) to the applicable government security office via the COR. The contractor's appointed Security Officer, which is required in clause 5252.204-9200, shall track all personnel holding local government badges on this TO.

8.2.2.4 Common Access Card (CAC) Requirements

Some government facilities/installations (e.g., Joint Base Charleston) require contractor personnel to have a Common Access Card (CAC) for physical access to the facilities or installations. Contractors supporting work that requires access to any DoD IT/network also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The Contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

a. In accordance with Directive-Type Memorandum (DTM-08-003), issuance of a CAC will be based on the following four criteria:

1. eligibility for a CAC – to be eligible for a CAC, Contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of the government on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification.
2. verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associated Sponsorship System (TASS) (formally Contractor Verification System (CVS)).
3. completion of background vetting requirements according to FIPS PUB 201-1 and DoD Regulation 5200.2-R – at a minimum, the completion of Federal Bureau of Investigation (FBI) fingerprint check with favorable results and submission of a National Agency Check with Local Agency Check and Credit Check (NACLC) to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. NOTE: Personnel requiring a CAC under SSC Atlantic shall contact the SSC Atlantic Security Office to obtain the latest requirements and procedures.
4. verification of a claimed identity – all personnel will present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list shall be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

a. When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC shall have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory IA Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual IA training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the SSC Atlantic Information Assurance Management (IAM) office:

1. For annual DoD IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requiring initial training and do not have a CAC, contact the SSC Atlantic IAM office at phone number (843)218-6152 or email questions to ssc_lant_iam_office.fcm@navy.mil for additional instructions. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html.

2. For SAAR-N form, the contract shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the SSC Atlantic IAM office at or from the website: https://navalforms.documentservices.dla.mil/. Digitally signed forms shall be routed to the IAM office via encrypted email to ssclant_it_secmtg@navy.mil.

8.2.2.5 Contractor Check-in and Check-out Procedures

All SSC Atlantic contractor personnel requiring or possessing a government badge and/or CAC for facility and/or IT access shall have a SSC Atlantic government sponsor and be in compliance with the most current version of Contractor Check-in and Check-out Instruction and Forms as posted on the Command Operating Guide (COG) website. At TO award throughout TO completion, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this TO within the required timeframe as cited in the Check-in and Check-out instructions. Contractor's Security Officer shall ensure all contractor employees whose services are no longer required on contract return all applicable government documents/badges to the appropriate government representative. NOTE: If the contractor does not have access to the SPAWAR COG website, the contractor shall get all necessary Instruction and Forms from the COR.

8.2.3 IT Position Categories

In accordance to DoDI 8500.2, SECNAVINST 5510.30, DoD 8570.01 and applicable to unclassified DoD information systems, a designator shall be assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R and SECNAVINST 5510.30, the IT Position categories include:

IT-I (Privileged)

IT-II (Limited Privileged) IT-III (Non-Privileged)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The Contractor PM shall assist the Government Project Manager or COR in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), and National Agency Check (NAC) adjudication shall be performed in accordance with DoDI 8500.2 and SECNAVINST 5510.30. IT Position Categories shall be determined based on the following criteria:

8.2.3.1 IT-I Level (Privileged) - Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudicated SSBI or SSBI-PR. The SSBI or SSBI-PR shall be updated a minimum of every 5 years.

8.2.3.2 IT-II Level (Limited Privileged) - Positions in which the incumbent is responsible for the-direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a

favorably adjudicated NAC.

8.2.3.3 IT-III Level (Non-privileged) - All other positions involved in computer activities. Incumbent in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudicated NAC.

8.2.4 Security Training

Regardless of the TO security level required, the contractor shall be responsible for verifying applicable personnel (including subcontractors) receive all required training. At a minimum, the contractor's designated Security Officer shall track the following information: security clearance information, dates possessing Common Access Cards, issued & expired dates for SSC Atlantic Badge, Information Assurance (IA) training, Privacy Act training, and Information Assurance Workforce (IAWF)/Cyber Security Workforce (CSWF) certifications, etc. The contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22M.

8.2.5 Disclosure of Information

Contractor employees shall not discuss or disclose any information provided to them in the performance of their duties to parties other than authorized Government and contractor personnel who have a "need to know". Any information or documentation developed by the contractor under direction of the government shall not be used for other purposes without the consent of the government Contracting Officer. Any developed documentation containing PII information shall be marked accordingly in either the header or footer of the document: "FOUO – Privacy Sensitive.

Any misuse or unauthorized disclosure may result in both criminal and civil penalties."

8.3 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. As directed in DoDD 5205.02E and SPAWARINST 3432.1, SSC Atlantic's OPSEC program implements requirements in DoD 5205.02 – OPSEC Program Manual. Note: OPSEC requirements are applicable when contract personnel have access to either classified information or unclassified Critical Program Information (CPI)/sensitive information.

8.3.1 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the SPAWARINST 3432.1 and existing local site OPSEC procedures. The contractor shall development their own internal OPSEC program specific to the contract and based on SSC Atlantic OPSEC requirements. At a minimum, the contractor's program shall identify the current SSC Atlantic site OPSEC Officer/Coordinator.

8.3.2 OPSEC Training

Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. Training may be provided by the government or a contractor's OPSEC Manager and shall, as a minimum, cover OPSEC as it relates to contract work, discuss the Critical Information applicable in the TO, and review OPSEC requirements if working at a government facility. Any training materials developed by the contractor shall be reviewed by the SSC Atlantic OPSEC Officer, who will ensure it is consistent with SSC Atlantic OPSEC policies. OPSEC training requirements are applicable for personnel during their entire term supporting SPAWAR contracts.

8.3.3 SSC Atlantic OPSEC Program

Contractor shall participate in SSC Atlantic OPSEC program briefings and working meetings as required, and the contractor shall complete any required OPSEC survey or data call within the timeframe specified.

8.3.4 Classified Contracts

OPSEC requirements identified under a classified contract shall have specific OPSEC requirements listed on the DD Form 254.

8.4 DATA HANDLING AND USER CONTROLS

8.4.1 Data Handling

At a minimum, the contractor shall handle all data received or generated under this TO as For Official Use Only (FOUO) material. Any classified information received or generated shall be handled in accordance with the attached DD Form 254 and in shall be in compliance with all applicable PWS references and to other applicable Government policies and procedures that include DOD/Navy/SPAWAR.

8.4.2 Effective Use of Controls

The contractor shall screen all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect contract related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. This includes ensuring that provisions are in place that will safeguard all aspects of information operations pertaining to this TO in compliance with all applicable PWS references. Compliance with Para 7.3.2.1, Data-at-Rest, is required on all portable electronic devices including storage of all types. Encryption/digital signing of communications is required for authentication and non-repudiation.

9.0 GOVERNMENT FACILITIES

As specified in the TO, Government facilities (i.e., office space, computer hardware/software, or lab space) will be provided to those labor categories that would otherwise adversely affect the work performance if they were not available on-site. All Contractor personnel with supplied government facilities shall be located in San Antonio, TX, Aurora, CO, Washington, DC or SSC Atlantic in Charleston, SC. Note: *The burdened labor rate for those contractor personnel designated as "government site" shall include overhead costs allocable to government site work, consistent with the contractor's established accounting practices.*

Work under this TO shall be done during normal working hours when practical. However, due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended hours including weekend work may be required. Extended working hours resulting in no additional cost to the Government may be approved in writing by the COR with a copy to the Contracting Officer. Extended working hours resulting in additional cost to the Government shall be requested through the COR and approved in writing by the Contracting Officer. Approval by the Contracting Officer is required prior to extending hours beyond normal working hours. Requests for extended hours shall include the employee name, labor category, and justification for the overtime or extended work week.

10.0 CONTRACTOR FACILITIES

A significant portion of tasking under this TO will require close liaison with the government. The contractor shall be prepared to establish a local facility within a 10 mile radius of SSC Atlantic. Close proximity allows for proper contract administration duties. The contractor's facility is not necessary for the exclusive use of this contract and can be utilized on a shared basis. The Charleston local facility shall include sufficient physical security to protect government assets. The contractor's facility shall meet all location and size requirements to perform work requirements within 30 days after TO award. Facility space shall include offices, conference rooms, lab work, and a staging area for materials and equipment, as required.

11.0 CONTRACT PROPERTY ADMINISTRATION

11.1 PROPERTY TYPES

Contract property can either be intangible (i.e., intellectual property and software IAW FAR Part 27) or tangible (i.e., government property IAW FAR Part 45). The contractor shall have established property management procedures and an appropriate property management point of contact who shall work with the assigned Government Property Administrator (PA) to ensure their property management system is acceptable. This contract will have the following property in support of the tasking requirements in PWS Para 3.0.

11.1.1 Intangible Property – Intellectual/Software

11.1.1.1 Government Furnished Information (GFI)

Intellectual property includes Government Furnished Information (GFI) which includes manuals, drawings, and test data that is provided to contractor for performance of a contract. Depending on the document, certain information (e.g., technical specifications, maps, buildings designs, schedules, etc.) shall require addition controls for access and distribution. Unless otherwise specified, all GFI distribution and inventory shall be limited to need-to-know and returned at completion of the TO. The following table lists GFI that shall be provided to the contractor after TO award.

Item #	Description
N/A	CNDSP Standard Operating Procedures
N/A	Red Team Standard Operating Procedures
N/A	XenClient computing platform image

11.1.2 Tangible Property – Government Property (GP)

Government property shall be utilized on contract which includes all property owned or leased by the Government. Government property consists of Government-furnished property (GFP) and Contractor-acquired property (CAP). Under this TO, the following government property shall be applicable:

11.1.2.1 Government-furnished Property (GFP) Not Applicable

11.1.2.2 Contractor-acquired Property (CAP)

Contractor Acquired Material (CAM) – Contractor Acquired Material (CAM) – Operating Material and Supplies (OM&S) which includes materials purchased and shipping costs incurred by the contractor in direct support of the task that will be incorporated into, or attached to a deliverable end item or that may be consumed or expended in performing a TO.

Contractor Acquired Equipment (CAE) – Property, Plant and Equipment (PP&E) which includes equipment, machine tools, test equipment, etc. Contractor Acquired Equipment is required for this TO and includes cell phones for 80 of the 92 contractors on the program. Cell phones will be utilized by contractors that travel or for the CNDSP Continuity of Operations purposes.

11.2 TRACKING AND MANAGEMENT

11.2.1 Contractor Property Management System

In accordance with FAR clause 52.245-1 and DFARS clause 252.245-7003, the contractor shall establish and maintain an acceptable property management system that is subject to review and approval by the KO and contract government Property Administrator. The contractor's property management system shall adhere to the applicable

prescribed requirements in FAR clause 52.245-1.

11.2.2 Government Property Administrator

In accordance with FAR 42.201, the contract property administrator under this contract is designated as Defense Contract Management Agency (DCMA). The contractor shall work with the designated contract property administrator to ensure compliance with the contract's property requirements.

11.2.3 Property Transfer between Government and Contracts

Contractors shall not take receipt or transfer custody of any government property without possessing proper contractual authority; i.e.; item specifically is identified as GFP in the TO. Per DoDI 4161.02, the government will utilize electronic transaction when transferring GFP to the contractor (specified by contract number) and upon return of the property to the government. The contractor shall use WAWF to receipt property transfer or use Defense Logistics Management System (DLMS) standard logistics transaction set 527R to provide materiel receipt acknowledgement. The applicable contract number shall be cited to properly track property shipments.

Note: If electronic receipt is not available, at a minimum, the transfer or property shall not occur without proper paperwork; e.g., Requisition and Invoice/Shipping Document (DD1149) or COMSEC Material Report (SF153).

11.2.4 GFP Tagging and Item Unique Identification (IUID) Registry

In accordance with DFARS clause 252.245-7001, contractor shall tag, label, or mark all GFP items not previously tag, labeled, or marked. In accordance with DFARS clause 252.211-7007 (revised Aug 2012); the contractor shall ensure applicable Government Furnished Property (GFP) is identified in the DoD Item Unique Identification (IUID) Registry and its integral GFP Module. After a contractor takes possession of GFP, the contractor shall designate the item as GFP in the IUID Registry. If the item cannot be found in the IUID registry, the contractor shall enter the item. When GFP is returned to the government at the completion of the TO, the contractor shall update the IUID registry Custody status. If the GFP item is consumed, destroyed, scrapped, lost, or abandoned during the TO performance, the contractor shall update the item's status and annotate that it has been disposed.

11.2.4.1 IUID Reporting Criteria. Per DFARS 252.211-7003/7007, the contractor shall ensure GFP acquired items that are serialized regardless of unit acquisition cost are subject to Item Unique Identification (IUID) Registry Requirements. Contractor shall verify with government if questionable GFP items that are non-serialized or have an acquisition cost less than $5,000 require an item unique identification or a DOD recognized unique identification equivalent. Exceptions to IUID requirements will be determined by the government.

11.2.4.2 Exception to IUID Reporting Criteria. As cited in 245.102, CAP is one of the listed GFP items that do not required to be tagged, labeled, or marked as GFP; however, if any CAP is returned to the government, the contractor shall appropriately tag it and enter it into the IUID registry or other specified Government inventory system.

11.2.5 Government Property Records

In accordance with FAR 52.245-1, contractors and any subcontractors if applicable shall be responsible for establishing and maintaining records of Government Property in their possession – this includes GFP and CAP. For GFP only, the contractor shall ensure that items designated as Special Tooling (ST) and Special Test Equipment (STE) are correctly annotate in the SPAWAR approved GFP central Automated Information System (AIS). The contractor shall work with the COR and designated contract Property Administrator to maintain adequate GFP records which shall be forwarded as required to SSC Atlantic functional mailbox for tracking and centralization. The GFP and CAP records shall contain at a minimum the data elements as described in FAR 52.245-1 and shall be submitted for review as part of the TO status report (CDRL A003).

11.3 TRANSFERRING ACCOUNTABILITY

Government property cannot be transferred between contracts or TOs unless approval is obtained from the Contracting Officer, proper identification/tracking is maintained, and modifications are issued to both affected TOs.

Contractor shall ensure they have all necessary documentation required for authorized transfer of property from one TO to another. Transfer documentation shall specify the type, quantity and acquisition cost of each item being transferred. For CAP that is transferred to another TO, the items shall be considered GFP when retained by a contractor for continued use.

11.4 LOST OR DAMAGED ITEMS

Contractor shall promptly report to the COR and KO all lost and/or damaged government property. The requirements and procedures for reporting loss Government Property are specified in DFARS clause 252.245-7002.

11.5 INVENTORY DISPOSITION

When disposition instructions for GFP are contained in the accountable contract or on the supporting shipping documents (DD Form 1149), the Contractor shall initiate and submit an excess inventory listing to the Procuring Contracting Officer (PCO), via the activity Property Administrator.

When disposition instructions are not stipulated in the contract or supporting shipping document (DD Form 1149), an excess inventory listing is required that identifies GFP and, under cost reimbursement contracts, CAP. This list shall be submitted to the PCO, via the activity Property Administrator, at which time disposition instructions will be provided.

When GFP and CAP are provided on a TO, a final inventory reporting list shall be included in the TO Closeout Report (CDRL A004). At the time of the Contractor's regular annual inventory, the Contractor shall provide the PCO, via the assigned Property Administrator, a copy of the physical inventory listing. All contractor personnel shall be responsible for following the company's internal inventory management procedures and correcting any problems noted by the government property administrator.

11.6 PERFORMANCE EVALUATION

Non-compliance with the contract's Government Property terms and conditions shall negatively affect the contractor's annual Contractor Performance Assessment Reporting System (CPARS) rating.

12.0 SAFETY ISSUES

1 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned under this TO. Without government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system.

12.1.1 Performance at government facilities

In addition to complying to clause 5252.223-9200 Occupational Safety and Health Requirements, the contractor shall immediately report any accidents involving government or contractor personnel injuries or property/equipment damage to the contracting officer and COR. Additionally, the contractor is responsible for securing the scene and impounding evidence/wreckage until released by the contracting officer.

12.1.2 SAFETY EQUIPMENT

All personnel safety equipment required to perform work under this TO shall be provided by the Contractor and must be in satisfactory working order. Personal safety equipment shall include, but not be limited to -- hard-hats, safety shoes, safety gloves, goggles, hearing protection, non-flammable clothing for hot work personnel, gas/oxygen detectors for

confined spaces, face shields, and other types of safety equipment required to assure a safe work environment and compliance with applicable federal, state and local safety regulations.

12.1.3 SAFETY TRAINING

The contractor shall be responsible to train all personnel that require safety training. Specifically, where contractors are performing work at Navy shore installations, that requires entering manholes or underground services utility the contractor shall provide a qualified person as required in 29 CFR 1910 or 29 CFR 1926 or as recommended by the National Institute for Occupational Safety and Health (NIOSH) Criteria Document for Confined Spaces. Also, when contractors are required to scale a tower, all applicable personnel shall have Secondary Fall Protection and Prevention training.

13.0 SMALL BUSINESS SUBCONTRACTING PLAN

Not applicable.

14.0 TRAVEL

14.1 LOCATIONS

The majority of the work under this TO shall be performed at SSC Atlantic (Contractor and Government facilities). Travel shall be performed in accordance with clause 5252.231-9200. For costing purposes and to establish an ODC CLIN for estimated travel requirements, the following is provided as Attachment #8. Although estimated sites are provided as attachment #8, the contractor shall be prepared to travel to any of the following alternative sites noted in Attachment #9, Alternative Sites Dated 13 March 2018.

Note: Travel specifically to Iraq or Afghanistan shall not be performed under this TO.

14.2 PERSONNEL MEDICAL REQUIREMENTS

14.2.1 OCONUS Immunization Requirements

The contractor shall be required to travel to locations outside the Continental limits of the United States (OCONUS) both shore and afloat. Contractor employees who deploy to locations that require immunizations shall do so in accordance with Department of Defense Instruction (DoDI) 6205.4, Department of the Navy (DON), and Space and Naval Warfare Systems Center Atlantic Instruction (SPAWARSYSCENLANTINST) 12910.1.

14.3 LETTER OF AUTHORIZATION

Some travel shall require a Letter of Authorization (LOA). As noted in DFARS PGI 225.7402-3(e), a LOA is necessary to enable a contractor employee to process through a deployment processing center; to travel to, from, and within a theater of operations; and to identify any additional authorizations and privileges. The contractor shall initiate a LOA for each prospective traveler.

The contractor shall use the Synchronized Pre-deployment & Operational Tracker (SPOT) web-based system, at http://www.dod.mil/bta/products/spot.html, to enter and maintain data with respect to traveling/deployed personnel, and to generate LOAs. When necessary and if in the Government's interest, the contractor may also initiate a LOA request to provide an official traveler access to Government facilities and to take advantage of travel discount rates in accordance with Government contracts and/or agreements. All privileges, services, and travel rate discount access are subject to availability and vendor acceptance. LOAs shall be signed/approved by the SPOT registered Contracting/Ordering Officer for the applicable contract.

14.4 SPECIFIED MISSION DESTINATIONS

The contractor shall be required to travel to locations designated as Specified Mission Destinations which are listed in the latest SSC Atlantic OCONUS Travel Guide portal (latest link to be provided at TO award). In accordance with

DoDI 3020.41 and SPAWARSYSCENLANTINST 12910.1A, work to be performed at Specified Mission Destinations is subject to all relevant contract clauses, as well as the requirements set forth in the aforementioned guide. The contractor shall be able to meet all clause and guide requirements 35 days prior to travel within the applicable specified destinations.

When deployment to a Specified Mission Destination is required, the contractor shall be responsible for processing applicable deployment packages for its personnel in accordance with the SSC Atlantic OCONUS Travel Guide portal. Note: The portal is NOT the authoritative source, as it is only a guide. The contractor shall be responsibility to know and understand travel requirements as identified by the Combatant Command (COCOM) and applicable country. Commencing no later than seven

1. days after award requiring travel to specified mission destination(s), the contractor shall submit all required OCONUS Deployment Documentation and Package (A014) to the technical POC and/or Command Travel/Deployment Coordinator.

   [END OF PWS]