Performance Work Statement for Enterprise Hosting Support Services

1. Scope: The Naval Air Warfare Center Aircraft Division (NAWCAD) Information Technology and Cyber Security (IT/CS) Department (AD 7.2) has a requirement to provide enterprise-wide Information Technology (IT) services to the Naval Air Warfare Center (NAWC), Naval Air Systems Command (NAVAIR), its respective customers, and other Department of the Navy (DON) components with the people, processes, facilities, technologies, skills, knowledge, and abilities necessary to support the development, planning, execution, monitoring, and life cycle support of IT/CS programs and associated activities.

The IT/CS Department follows a number of statutes and guidance, including the Clinger-Cohen Act of 1996, which, along with the Office of Management and Budget's Circular A-11, requires agencies to have processes and procedures in place to ensure that IT projects are being implemented at acceptable costs; within reasonable and expected time frames; and in a way that contributes to tangible, observable improvements in mission performance.

The IT/CS Department is structured into the following divisions: Customer Relationship Management/Horizontal Integration (7.2.1); Applications Integration and Business Intelligence (7.2.2); Customer Services and Operations (7.2.4); Cyber Security Services (7.2.6); and Business Operations (7.2D). Tasks are typically accomplished through integrated product or project teams, comprised of government and contractor personnel.

NAWCAD 7.2.1 Customer Relationship Management (CRM)/Horizontal Integration Division serves as the hub for sustainment of IT/CS investments within the NAVAIR community. CRM focuses on understanding the customer's business processes, gathering customer requirements, managing the requirement through the 7.2 Department, and ensuring the implementation of effective solutions consistent with Command, DON, and Department of Defense (DOD) Information Technology (IT) regulations, policies, and initiatives. The primary service offerings are IT Portfolio Management, which includes sub-services areas of Customer Relationship Management/Customer Experience Management (CRM/CEM) and Strategic Planning; and the NAVAIR National Helpdesk (NNHD).

- CRM/CEM provides strong strategic capabilities in technical architectures pertaining to horizontal integration of concepts, techniques, and technologies into customer communities and Strategic Planning is dedicated customer IT/CS liaison/expert level services to provide Government approved technology-based solutions to near-term and future IT/CS requirements for customers.
- The NAVAIR National Helpdesk (NNHD)provides 24x7x365 operations support to a world-wide user base. The primary objective of the Help Desk is to provide timely and efficient services including Tier 1/Tier II Support, Knowledge Management, Digital Signage, Automated Call Distribution, and Incident Tracking Administration to customers for national initiatives for over 500 Systems, Functions, Applications and Websites. The support to the Government provides establishing and maintaining an IT Service Management environment that aligns with the Information Technology Infrastructure Library (ITIL) V3 Framework and subsequent releases.

NAWCAD 7.2.2 Application Integration Business Intelligence Division and is responsible for the day-to-day operations, development, sustainment and management of web-based applications and technologies; and is responsible for providing products and services that encompass corporate management information systems, data warehousing, reporting, web applications, websites, and database/application hosting services to the NAWCAD, NAVAIR, DON and the fleet. Project teams perform application and database program requirements analysis, use cases, design, development, testing and implementation. Additionally, NAWCAD 7.2.2 is responsible for implementing software standards, new technologies used across NAVAIR, and operational processes. NAWCAD 7.2.2 services cover three primary areas: Business Intelligence and Data Management, Document Management, and Software and Applications Management.

- The Business Intelligence (BI) and Data Management services are to analyze, configure, document and implement business solutions, which provides customers with BI solutions and develop corporate decisions and strategy based on the current environment, as well as, historical trends.
- The service area of Document Management provides skilled resources in support of scanning and electronic document storage to support customers throughout NAVAIR and its respective customers.
- The service area of Software and Applications Management provides software development life cycle support for IT/CS corporate applications, business applications, commercial software, web applications, websites, and collaboration environments. Software and Applications Management consists of three (3) primary

sub-service areas 1) Applications Development and Maintenance; 2) Software and Web Administration; and 3) Database Administration.

NAWCAD 7.2.4 Customer Services and Operations Division provides a wide variety of services including:

- Integration and Systems Engineering perform all lifecycle support activities for all Government enterprise infrastructure hardware, software and management tools, which will include planning, designing, engineering, installing, monitoring, supporting, documenting, testing, configuring and reconfiguring, integrating, updating/upgrading, repairing, performing version control and managing the Government's IT environment.
- Navy/Marine Corps Intranet (NMCI)/Next Generation Enterprise Network (NGEN) Customer Technical Representative (CTR) support provides Deskside Services for the planning, submission, management of orders, site requirements plan support, group move support, software application support, technology refreshment support, customer liaison support and information research and dissemination. Support also includes Embedded NMCI POC services to support various Program Executive Offices (PEOs), Program Management Activities (PMAs) and competencies and facilitates fulfillment of required NMCI products and services.
- Video Technologies support provides for the design, implementation, installation, operation, and maintenance of video technology services for all NAVAIR, NAWCAD, Naval Air Warfare Center Weapons Division (NAWCWD) and NAVAIR Fleet Readiness Centers (FRCs). This includes fixed special purpose Video Teleconference (VTC) facilities that are installed in multi-purpose conference rooms, auditoriums, class rooms, and a few personal office systems. Video technology services include research, design, planning, development, implementation, installation, modification, asset/ lifecycle management, and maintenance of these systems, as well as the procurement of incidental equipment/material. Classified and Unclassified Meeting facilitator services and audio/video conference bridge management are also provided.
- Defense Messaging/Organizational Messaging provides classified and unclassified support and service to various NAVAIR, FRC, and Naval Supply Systems Command (NAVSUP). The IT/CS Defense Messaging/Organizational Messaging supports applicable DON Official Information Exchange (OIX) Naval messaging solutions; Navy Regional Enterprise Messaging System (NREMS) classified solution and Navy Interface for Command Email (NICE) unclassified messaging solution. Services include technical and operational support to include End user training, Defense Message System Message Dissemination System (DMDS) message releasing and processing, along with support for the administrative management, processing, storage and distribution of both unclassified and classified (Secret) messages.
- The Base Telephone Office (BTO) provides approximately 28,500 voice telecommunication lines and associated services, low bit rate video circuits and data communication links for the IT/CS customer community. The BTO also manages wireless communication services, Defense Information Systems Agency (DISA) circuits, Government Emergency Telecommunications Service / Wireless Priority Service (GETS/WPS), Continuity of Operations Plan (COOP) services, satellite phones and provides networks support to the National Help Desk (NHD), Video Teleconferencing Team (VTT) and miscellaneous commands requests.
- The Network Infrastructure Team (NIT) is responsible for design, installation, and maintenance of all fiber/copper facilities inside/outside plant in support of all data and voice networks. The NIT also manages Video transmission facilities for Patuxent River and St Inigoes Visions/video services, provides Open Settlement Protocol (OSP) locating services for all infrastructure and escorts for sensitive network infrastructure locations.

NAWCAD 7.2.6 Cyber Security Division has the responsibility to develop, implement, and maintain an effective Cyber Security Program. This includes labs and test environments under its cognizance operating at an acceptable level of risk, ensuring the Confidentiality, Availability and Integrity (CAI) of these systems and networks. Service provided include timely and technically accurate Cyber Security services that comply with the DON, Department of Defense (DOD), Federal Information Security Management Act (FISMA), and other national level mandated policies. Support is provided in the areas of Computer Network Defense (CND), Compliance and Assessments (C&A), as well as Information Systems Security Management (ISSM) support. Risk assessment is conducted to identified IT assets utilizing available cyber threat and vulnerability information and provide risk recommendations as well as provide technical expertise/capability to identify security-related issues of both current and planned systems and networks and associated architecture on the NAVAIR enterprise and Research Development Test & Engineering (RDT&E) classified and unclassified networks.

The NAWCAD 7.2D Business Operations provides overall support for business operations, management and administrative functions and security for the purpose of enabling an efficient and effective business environment for the entire NAWCAD 7.2 IT/CS Department.

1.1. Service Delivery Environment

1.1.1. The Service Delivery Environment is comprised of a series of interconnected IT systems whose purpose is the integration of information, applications, and processes throughout NAVAIR's global operations footprint, as well as across Department of Navy (DON) and Department of Defense (DOD) organizational boundaries. IT is a significant enabler of the NAVAIR war-fighter mission. As such, NAWCAD 7.2 requires continuing support for the operations, maintenance, and IT engineering activities of the NAWCAD 7.2 IT environment. NAWCAD 7.2 provides services to a world-wide user base. Successful NAVAIR mission achievement mandates IT services that are well integrated, flexible, and adaptable with the ability to rapidly scale in response to NAVAIR's dynamic mission requirements. In order to achieve government objectives, NAWCAD 7.2 requires the services of a highly qualified IT service provider with the skills and experience to provide enterprise-wide application(s), server, storage, data protection/recovery, voice, video, and data telecommunications support. In addition, requirements include planning, acquiring, provisioning, operating, administering, troubleshooting, repairing and managing all aspects of NAVAIR's centrally and remotely located IT solutions.

NAWCAD 7.2 delivers enterprise-wide systems that support the community with financial, data analytics, business solutions, science and technology, acquisition, logistics and RDT&E information. NAWCAD 7.2 is seeking assistance in establishing operations in a Commercial Cloud Computing facility. Cloud computing and related "X-As-A-Service" models [Hardware-As-A-Service (HAAS), Capacity-As-A-Service (CAAS), Infrastructure-As-A-Service (IAAS), Platform-As-A-Service (PAAS), Software-As-A-Service (SAAS)] are increasingly important to NAWCAD. The need to deliver support to the fleet with increased efficiencies (cheaper, faster solutions) is driving these cloud-based services. Policies, such as the Navy's "Cloud First," further directs the need to move to cloud services. Whether or not the cloud deployment model is private, community, public, or hybrid, NAWCAD is seeking assistance in establishing this operating environment that provides better protection, transport, and reliability for business and services and data.

A hybrid environment using commercial and private cloud computing capabilities will improve the organization's ability to ensure the continuity, integrity, and availability of business and data. The requirements are applicable to both the current on premise environments and the cloud environment. While a few infrastructures related tasks may be cloud centric, over-all tasking and deliverables are environment independent. Interoperability between the two environments is anticipated.

The on premise environment hosts multiple systems and applications for a variety of Navy customers. The confidentiality, availability, and integrity of these systems is critical to the successful execution of operations. System domain examples include:

- Data Analytics/Business Intelligence
  Warehouse Analytical Report System (WARS)
  NAVSUP SAS/Netezza (NBIS)
  Logistics Data Warehouse
- Science and Technology
  Science and Technology Alignment and Investment Reporting System (STAIRS)
  Flight Clearance/Airworthiness
- Logistics
  Joint Deficiency Reporting System (JDRS)
  Deckplate (maintenance/flight/usage data warehouse)
  Joint Technical Data Integration (JTDI)
- RDT&E
  Naval Infrastructure and Capability Tool (NICAP)
- Structural Appraisal and Fatigues Effects (SAFE)

1.1.2. Government owned IT infrastructure requiring support includes, but not limited to: Development, test, quality assurance (QA) and production application servers, web portal servers, database servers, middleware servers, Internet/intranet servers/devices, email/collaboration servers, Domain Name System (DNS) servers, proxy servers and file/print servers. Storage Area Network (SAN) storage arrays, Network Attached Storage (NAS) devices, data warehousing and other data storage systems.

Hardware and software tools, utilities, and other supporting infrastructure used to manage the resources and services.

1.1.3. The Contractor shall perform all of its IT Service Area delivery activities in close cooperation and coordination with the government all other relevant IT service providers. This cohesive working relationship shall ensure successful ongoing day-to-day service delivery for all Contractor IT Service Area and corresponding Sub-Service Areas as referenced in Table below.

Service Areas	Sub-Service Areas	Technical Domain Areas
Enterprise Hosting(On-Premise, Cloud and Hybrid)	Integration and Systems Engineering	– Integration, and Engineering – Process, Configuration Management, Acquisition
	Systems Administration	– Data Center Operations – Applications Administration – Operating Systems Administration – Data Solutions
	Managed Service Organization (MSO)	– Navy Cloud Broker Business Solutions

2. Applicable documents:

2.1 Department of Defense specifications
The Government will provide the Contractor copies of, or access to, all required directives, publications, and documents, as available.
A comprehensive list of Navy regulatory documents can be found at the DON Chief Information Officer (CIO) IT Policy and Guidance website, http://www.doncio.navy.mil/. Throughout the life of this task order, if any policy, instruction, or regulation is replaced or superseded, the replacement or superseding version shall apply. The Contractor is responsible for researching and complying with any additional regulations applicable to the specific task area. Applicable documents are listed below, but are not limited to:

2.1.1 Section 508 Amendment to the Rehabilitation Act of 1973 http://www.section508.gov/
2.1.2 NASPAXRIVINST 12610.7G Employee Reporting Procedures During Emergency Situations, 02 June 2014
2.1.3 SECNAVINST 5239.3B DON Information Assurance Policy, 17 JUN 2009
2.1.4 SECNAV M-5239.1, DON Information Assurance Manual
2.1.5 NAVAIR 5252.209-9510(e)(5) Organizational Conflicts of Interest (Services)
System Authorization Access Request -Navy (SAAR-N) form (OPNAV 5239/14 (Rev 9/2011)
2.1.6 SECNAVINST 5211.5E DON Privacy Act Program, 10 Oct 2008
2.1.7 SECNAVINST 5510.30B DON Personnel Security Program Instruction, 06 OCT 2006
2.1.8 DOD-D-5220.22 National Industrial Security Program, 18 MAR 2011
2.1.9 DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 Dec 2005 (Incorporating Change 3, 24 Jan 2012)
2.1.10 DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management, 15 August 2004, Certified Current as of 23 April 2007
2.1.11 DON letter 5239 NAVAIR 726/2322 of 18 Feb 09, NAVAIR Data at Rest Policy

3. Requirements

3.1 General Requirements

3.1.1 Compatibility - The Contractor shall maintain the capability to prepare documents and software packages compatible with the Government IT environment through the security classification of the DD-254. The current operating environment required for this contract includes:

Microsoft Windows 10
Microsoft Project 2010
Microsoft Office Professional Plus 2010
Adobe Acrobat XI (reader)
Internet access
See 3.3.1 for a representative hardware inventory of the Government IT Environment

The Contractor shall maintain the ability to interface with and transfer data to and from requiring office software applications and their upgraded versions. The Contractor shall maintain state-of the-art virus software and ensure that all media are virus free when delivered. The Contractor shall be capable of Internet and LAN communications with the NAWCAD IT/CS Department (AD 7.2). Contractor personnel shall be capable of maintaining real-time communications, both voice and data transfer capabilities, with NAWCAD IT/CS Department (AD 7.2) during working hours whether at Contractor work site or on travel.

3.1.2 Work Location and Facilities

3.1.2.1 Work location: Approximately 100 percent of work will be performed at Government sites. The Contractor shall support the NAVAIR enterprise-wide environment within the Continental United States (CONUS), which is comprised of facilities at Patuxent River, Maryland, Patuxent River remote facilities (St.Inigoes, Solomon's Island Naval Center, Washington Liaison Office in Arlington VA, and leased spaces within the 30 mile range); China Lake, California; San Diego/North Island, California; Point Mugu, California; Jacksonville, Florida; Cherry Point, North Carolina; Lakehurst, New Jersey; and Orlando, Florida. The Contractor shall provide remote support to areas outside Patuxent River. Work in support of this PWS shall be primarily performed at Patuxent River, MD; however, the place of performance is not limited to the above location due to the evolving, integrated, and capability-focused enterprise requirements throughout NAVAIR. Contractors performing on-site support will be provided but are not limited to: access to workspaces, telephones, printers, facsimile machines, copy machines, shredders, computers, and network access including web servers and applicable databases or other applications necessary to carry out assigned tasks.

3.1.2.2 Meeting support: The contractor shall have the capability to host and conduct meetings at the classification levels up to classified with the capacity to support a minimum of 10 persons and have contractor furnished telephone and VTC capability, as well as sufficient equipment to conduct meetings with presentations including compatible software as required in Paragraph 3.1.1).

3.1.3 Contract Status reporting. The contractor shall provide the following documentation.

3.1.3.1 Monthly Progress and Financial Status Report: The contractor shall provide a progress and financial status report in accordance with the Contract Data Requirement List (CDRL A001). The report shall include work accomplished since submittal of the last report, both monthly and cumulative man-hour labor costs expended by labor category and material and travel costs.

3.1.3.2 The following contract deliverables shall be provided under this task order (See Exhibit A).
3.1.3.3 All CDRLs within this PWS shall be posted to the Government's IT knowledge management repository (e.g., SharePoint). Notice of posting shall be sent to relevant Government addressees.

Exhibit A

CDRL	Title	Date 1 Submission	Frequency
A001	Monthly Status and Financial Status Report	45DACA	MNTHLY
A002	NAWCAD Trusted Cloud Credential Manager Policy	ASREQ	ASREQ
A003	CSP Administrator Account Management Policy	ASREQ	ASREQ
A004	Governance and Design Documents, Templates, Plans, and Diagrams	ASREQ	ASREQ
A005	Customer/Cost Management Policy	ASREQ	ASREQ
A006	Agnostic NAWCAD CSP Management Policy	ASREQ	ASREQ
A007	Physical to CMDB Delta Report	120DACA	Semi-Annual
A008	Capacity Report	45DACA	MNTHLY
A009	Operational Reporting	45DACA	MNTHLY
A010	Lifecycle Management and Technology Refreshment Reporting	120DACA	YRLY
A011	Planning and Analysis Reports	ASREQ	ASREQ
A012	Feasibility Studies	ASREQ	ASREQ
A013	IT Asset Database Reporting	ASREQ	ASREQ
A014	Asset Management Reporting	90DACA	ASREQ
A015	Inventory Reporting	60DACA	QTRLY
A016	Configuration Management Reporting	45DACA	ASREQ
A017	Requirements, Function/Technical Design, and Architecture Documentation	ASREQ	ASREQ
A018	Quality Management Reporting	120DACA	ASREQ
A019	Exit/Transition Out Plan	ASREQ	ASREQ
A020	Incident/Problem Management Reporting	45DACA	ASREQ
A021	System Defense and Anomaly Reporting	ASREQ	ASREQ
A022	Compliance Report	45DACA	MNTHLY
A023	Desktop Guides	180DACA	Semi-Annual

3.1.4 Work Schedule to include Compressed Work Schedule (CWS), overtime, holidays, and installation closure.

3.1.4.1 Work schedule: The Contractor shall provide the required services and staffing coverage during core/normal working hours. Core/normal working hours are usually 8.5 hours (including a 30-minute lunch break), from 0700-1700 each Monday through Friday (except on the legal holidays specified in paragraph 3.1.4.4). Additionally, four (4) twenty-four (24) hours periods (typically the second and fourth Saturday/Sunday) are scheduled per month to provide windows of time for system security compliance, upgrades, implementations, and other maintenance activities requiring service disruption. These are commonly referred to as Outage Weekends. The Contractor shall provide on-site IT Service Area Delivery for all Service Areas during core business hours.

3.1.4.2 PAXR Operations Monitoring will provide 24 x 7 x 365 operational situational awareness of the on premise and cloud infrastructure using monitoring tools provided by NAWCAD. The Contractor shall work closely with enterprise hosting infrastructure and systems administrators during events and incidents. The Contractor will respond to Tier I events and incidents according to documented Event Response Procedures and escalate to Tier II or Tier III support as required. They will coordinate with NAVAIR National Helpdesk (NNHD) on events and incidents. They will create and maintain 24 x 7 x 365 support processes. The Contractor, during maintenance windows, will perform maintenance functions according to Configuration Control Board (CCB) approved tickets and work orders. Contractor work schedules shall be coordinated with the Technical Point of Contact (TPOC) and Contracting Officer Representative (COR) to ensure: 1) coverage during critical periods and critical tasking, 2) coordination of tasks involving other Contractors, and 3) security compliance for buildings/areas where access is controlled. (b) (3) 10 U.S.C. § 130

(b) (3) 10 U.S.C. § 130

Additionally, as determined by the government, certain support teams under this contract, shall be available to support after hours and weekend maintenance activities outside core hours (0700-1700, Monday through Friday) as Tier II or Tier III support which may include patching, testing, troubleshooting, and customer requests. The Contractor shall staff personnel that are able to respond to service requests notifications within 30 minutes and report to work or login to begin working within 2 hours of request. On-call coverage should not negatively impact the ability of resources to cover core business hours.

3.1.4.3 Compressed Work Schedule (CWS): CWS is an alternative work schedule to the traditional five 8.5 hour workdays (which includes a 30-minute lunch) worked per week. Under a CWS schedule, an employee completes the following schedule within a two-week period of time: eight weekdays are worked at 9.5 hours each (which includes a 30-minute lunch), one weekday is alternately worked as 8.5 hours (which includes a 30-minute lunch) and one weekday is not worked by the employee. The result is 80 hours worked every two weeks, with 44 work hours one week and 36 work hours the other. The Contractor may allow its employees to work a CWS schedule provided the requirements of this PWS are met. If the contractor chooses to allow its employees to work a CWS schedule in support of this contract, any additional costs associated with the implementation of the CWS schedule vice the standard schedule are unallowable costs under this contract and will not be reimbursed by the Government. Additionally, the CWS schedule shall not prevent Contractor employees from providing necessary staffing and services coverage as required by the Government to the ACOR/COR. The Government reserves the right to terminate CWS on a case-by-case basis.

3.1.4.4 Holidays: With the exception of 24x7 service areas and critical systems coverage, the contractor is permitted to observe the legal holidays in accordance with company policy.

The Government observes the following holidays:

New Year's Day, January 1
Martin Luther King's Birthday, the third Monday in January

President's Birthday, the third Monday in February
Memorial Day, the last Monday in May
Juneteenth, June 19
Independence Day, July 4
Labor Day, the first Monday in September
Columbus Day, the second Monday in October
Veteran's Day, November 11
Thanksgiving Day, the fourth Thursday in November
Christmas Day, December 25

3.1.4.5 Installation closure: When Federal facilities are closed by the Government, or when Federal employees are officially excused from work due to a holiday or a special event, severe weather, a security threat, or any other Government facility related problem that prevents Federal personnel from working at the Government facility, contractor personnel assigned to work at that facility in support of such Federal employees shall follow their parent company's policies.

While generally contractor personnel may not perform work on-site at a Government facility without oversight from Federal personnel, in very limited circumstances, work being performed by contractor personnel may be deemed mission essential and performance of such mission essential work may be authorized to continue at the Government facility despite the facility being otherwise closed for normal operations. The circumstances permitting work being performed by contractor personnel to be deemed mission essential are extremely limited and generally only apply to performance of efforts related to public health, safety, or matters related to national security. The cognizant Contracting Officer must concur with any determination that work being performed by contractor personnel is mission essential.

Please note, that under this contract, there will be select contractor personnel responsible for providing contractor support services to mission-essential federal employees and functions. The Government will identify these mission essential functions and the contractor will be responsible for supporting these mission essential functions, and shall provide the requisite qualified personnel to ensure the continuity of operations. The contractor will provide the names of these designated contractor personnel and they will be provided to the appropriate facility management areas to ensure access is permitted in case of installation closure or restricted access as per NASPAXRIV INSTRUCTION 12610.7G, revised 01/03/2013.

3.1.4.6 Overtime: Overtime cannot be charged directly to the contract unless first approved in writing by the Chief of the Contracting Office.

3.1.4.7 Telework Availability: Telework under this contract may be authorized; however, the contractor must provide their Telework policy detailing the roles, responsibilities, security, safety, and requirements for adherence by the contractor in coordination with the TPOC/COR.

3.1.5 Other Direct Costs:

3.1.5.1 Travel: A Not to Exceed (NTE) amount will be included as a line item to be used on a cost-reimbursable basis.

3.1.5.2 Material: All materials not depleted during the performance of this contract shall become Government property upon completion of this contract. The Contractor shall document the transfer of the materials in the monthly progress report and appropriate Government documentation. The Contractor shall transfer all materials not depleted to the COR by way of Material Inspection and Receiving Report (DD Form 250). A Not to Exceed (NTE) amount will be included as a line item to be used on a cost-reimbursable basis.

Materials needed to immediately respond to system development requirements, system failures, and system operation requirements shall be provided by the Contractor when essential to performance and not provided by the Government. List of Anticipated Materials may include, but are not limited to: Network Switches, Data Storages, desktop services, servers, blade servers and enclosures, disk shelf, licenses, tapes, hard drives, security appliances, Cloud spaces, Electronic Component Cleaning Materials, Deliverable/Documentation Consumables, Solder Supplies, Shipping/Freight Supplies/Services, and other materials in accordance with

the PWS tasking. Prior to procurement of any IT related items (as defined below), the Contractor shall prepare an IT approval request via the Navy Information Dominance Approval System (NAV-IDAS), which ensures IT procurements comply with the DoD and DON statutory and regulatory requirements.

Definition of IT related items. Any equipment or interconnected system and/or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data information. Includes personal computers, laptops, printers, software, servers, hubs, routers, phones, facsimile machines, and any related maintenance, telecommunications, training, or other support services.

3.1.6 Subcontractors: Provisions stated herein shall be clearly and effectively communicated to all subcontractors providing support under this contract. All provisions of this PWS shall flow down to subcontractors providing support under this contract.

3.1.7 Management of Contractor Personnel: The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances will the Government assign tasks to, or prepare work schedules for, individual contractor employees. The Contractor shall manage its employees and guard against any actions that are of the nature of personal services, or give the perception of personal services.

3.1.7.1 Training: The Contractor shall provide qualified personnel who are capable of assuming their duties at contract award. Training for Contractor personnel shall be at the Contractor's expense with the exception of internal training of the contractor's job responsibilities or knowledge transfer of modified or new requirements. The Contractor shall ensure that adequate staffing levels are maintained and service is not disrupted while personnel attend training. The Contractor shall provide verification to the Government that all employees receive necessary training via the Compliance Report (CDRL A022).

3.1.8. Transition Out Strategy

The Contractor's overall transition out strategy shall be built around maintaining the mission of the division with minimal impact, not only in terms of timeliness of performance but also to ensure that critical data and knowledge transfer occurs. Upon termination or expiration of the contract, the Contractor shall ensure an orderly transition of responsibilities, while minimizing impact to the operation. The Contractor shall submit a Transition Out Plan, to include the minimum elements listed below:

Task Order Leadership
b) Key positions
c) Orderly materials transfer
d) Knowledge transfer
e) Information / data transfer
f) Impacts
g) Risk
h) Schedule

- Work Turnover. The Contractor shall provide a plan of action to effectively transfer tasked work that is in process at the expiration or termination of the contract to the successor company. Establish and maintain effective communication with the incoming contractor or Government personnel for the period of transition via weekly status meetings.

- Quality Assurance. The Contractor shall provide a plan of action to ensure continuation of quality review processes during the transition period to the successor company.

- Risk Mitigation Strategies. The Contractor shall provide a plan of action to mitigate contract performance risks (quality and schedule) encountered during the transition period.

- Data/Information Transfer. The Contractor shall provide a plan of action for the efficient inventory and transfer of program data to the successor company.

The Enterprise Hosting Support Services Transition Plan shall identify how the transition will minimize the impact on current mission / activities while ensuring the completeness of the transition; who / what is impacted by the transition; the activities that need to be accomplished in order to successfully effect the transition, the impact on the organization; the roles and responsibilities of all who participate in the transition plan; the detailed schedule to be followed in order to successfully affect the transition and how any issues or discrepancies will be resolved.

CDRL A017 – Requirements, Function/Technical Design, and Architecture Documentation
CDRL A018 - Quality Management Reporting
CDRL A019 – Exit/ Transition Out Plan

3.1.9 Program Unique Requirements: Security Clearances/Protection of Classified Material. The Contractor shall conform to the provisions of the DOD-D-5220.22, 'National Industrial Security Program (NISP)', and shall obtain and maintain security clearances for Contractor employees requiring access to classified information and/or entry to controlled areas. The Contractor shall comply with SECNAVINST 5510.30B and SECNAV M-5510.30 to assure that the proper investigation is conducted for Contractor personnel. All Contractor personnel shall have the ability to obtain a TOP SECRET clearance as identified by the Government. The Contractor shall comply with SECNAVINST 5510.30B and SECNAV M-5510.30 to assure that the proper investigation (SSBI) is conducted for those Contractor personnel that require privileged access as defined in SECNAV 5239.1 or NAVAIR (NAWCAD) 5510.30.

3.1.9.1 The Contractor shall educate and brief employees concerning the handling and protection of classified material, and other security measures as described herein in accordance with DOD-D-5220.22, NISP. Contractors shall comply with mandates for annual security training. Interim clearances from Contractors will be accepted for no greater than a period of up to twelve months of performance unless approved by the Command ISSM and Command Security Manager. Full clearance levels must be acquired as soon as possible and maintained throughout the performance of the task order. The Contractor shall comply with the security and certifications requirements as listed in this PWS and the DD-254.

3.1.9.2 Cyberspace Workforce Management. All Contractor personnel working this Task Order shall comply with the policy established in the Secretary of the Navy Instruction (SECNAVINST) – 5239.20A, "Department of the Navy Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification, along with SECNAV M-5239.2, 'DON Information Assurance Manual. The Contractor personnel shall have the required SECNAV M-5239.2 baseline certification based on assigned specialty area prior to performing work on the task order.

Exceptions to this requirement shall require approval from Site ISSM or Command ISSM shall not exceed 6-month duration to become compliant with the requirements of this task order. All Contractor personnel providing services under this task order shall comply with all NAVAIR and DON IA policies and guidance where applicable and any training or certification required to comply with this directive is at the expense of the Contractor.

CDRL A022 – Compliance Report

3.1.9.3 Government Provided Vehicle / NAVFAC P-300 Publication

The Government will provide a vehicle for the transport of Enterprise Hosting materials and/or to provide services to Patuxent River facilities. The Contractor shall adhere to NAVFAC P-300 Publication in operating government equipment / vehicles in performance of this task order. The Contractor resources shall be certified by the Contractor, at the Contractor's expense, as being fully qualified to operate the equipment / vehicles which they are assigned.

3.2 Security

3.2.1 Citizenship Requirements: Only U.S. citizens may perform under this contract. If the Contractor cannot find qualified U.S. citizens to perform the work, the Contractor shall submit a citizenship waiver request with justification to the Government Security Office. The waiver request should include:

a. The individual's name, date and place of birth, position title, and current citizenship.
b. A statement that a qualified U.S. citizen cannot be hired in sufficient time to meet the contractual requirements.
c. A statement of the unusual expertise possessed by the applicant.
d. A statement that access will be limited to a specific government contract (specify contract number).
e. A statement that the Contractor has obtained an export license for the information required to perform the contract.

3.2.2 Investigative Requirements
Unclassified: All Contractor personnel must be eligible to perform Non-Critical Sensitive work as defined by SECNAV M-5510.30. All Contractor personnel are required to have a favorably adjudicated Tier-3 investigation from the Office of Personnel Management. The Contractor shall submit a request for personnel security investigation to the Government Security Office. The Government Security Office shall initiate the Contractor's Electronic Questionnaire for Investigations Processing (eQIP)), shall do a preliminary screening of the Contractor's eQIP for suitability and derogatory information. The Contractor employee shall provide all requested information pursuant to the Privacy Act of 1974. The Government Security Office may deny the Contractor access to Government facilities and information and may prohibit the Contractor from performance of sensitive duties for failure to provide requested information or when derogatory or adverse information is present on the Contractor's eQIP. In such cases, the Contractor employee may not perform on the Contract.

Classified: All Contractor personnel shall maintain security clearance eligibility commensurate with the level of classification of the work performed as annotated in the Contract's DD-254, Contract Security Specification. The Contractor is responsible for ensuring that all personnel receive the requisite investigation and are favorably adjudicated in accordance with DoDM 5220.22, National Industrial Security Program Operating Manual. Contractor employees who fail to meet security clearance requirements may not access classified information or perform sensitive duties. In such cases, the Contractor employee may not perform on the contract.

3.2.3 Common Access Card (CAC)/Public Key Infrastructure (PKI), System Authorization Access Request (SAAR-N).

3.2.3.1 SAAR-N: All contractor personnel requiring access to Government Information Technology (IT) systems shall have an approved System Authorization Access Request (SAAR-N) Form OPNAV 5239/14 (Rev Sep 2011) on file, and complete required Annual Information Awareness Training. New employees must submit their SAAR forms within thirty (30) days of their first day of work. Instructions for processing the SAAR-N forms are available at: http://www.cnrc.navy.mil/publications/Forms/OPNAV_5239_14_SAAR_N.pdf. SAAR-N forms shall be submitted to the Contracting Officer's Representative (COR), Government Technical Point of Contact (TPOC), or to the assigned government Trusted Associate Sponsorship System (TASS) Trusted Associate.

3.2.3.2 Common Access Cards (CAC) / Local Badges Contractor CACs and facility specific identification badges will be issued by the Government to on-site contractor personnel and shall be visible at all times while personnel are at the Government site. The contractor shall furnish all requested information required to facilitate issuance of identification badges and shall conform to local CAC requirements. All CACs and identification badges issued to Contractor employees shall be returned to the Government Security Department at the Government site in accordance with local CAC requirements following completion of the contract, relocation or termination of an employee, or upon request from the Contracting Officer's Representative. The Government will provide the contractor access to Government facilities, as required, for performance of tasks under this contract. Contractor personnel shall comply with local CAC requirements.

3.2.2.3 Security Classification Specification (DD Form 254)
The Contractor shall comply with security requirements specified in the DD-254 attached to this task order. Information or data that the Contractor accesses shall be handled at the appropriate classification level. Unclassified information shall be handled as "For Official Use Only". Distribution is authorized to the

Requiring Office's Organization and supported Activity only. Other requests for deliverables under this contract shall be referred to the TPOC/COR of this task order for approval.

3.2.4 Information Security. If the work is performed at the Contractor's facility, the Contractor shall implement and maintain security procedures and controls to prevent unauthorized disclosure of classified information and controlled unclassified information (CUI) and to control distribution of CUI in accordance with DoD 5220.22-M (NISPOM), and SECNAV M-5510.36. If the work is performed at the Government facility, the DON Automated Data Processing (ADP) Security Program outlined in SECNAVINST 5239.3B, 'DON Information Assurance Policy' and SECNAV M-5239.1, 'DON Information Assurance Manual,' apply to efforts under this task order. Contractor personnel providing services under this task order shall comply with all federal, DOD, and DON IA policies. The Contractor shall comply with SECNAVINST 5510.30B and SECNAV M-5510.30 to assure that the proper investigation (SSBI) is conducted for those Contractor personnel that require IT Level 1 access. The Contractor shall coordinate with the COR to identify applicable positions.

3.2.4.1 Marking: All information generated by the Contractor shall be properly marked. For Official Use Only information generated and/or provided under this contract shall be marked in accordance with DoDM 5200.01. Technical information shall also be marked with appropriate Distribution Statements and Export Control warnings in accordance with DoDD 5230.24 and program Security Classification Guidance

3.2.4.2 Public Release: No information pertaining to this contract shall be released for public dissemination, including posting to any social media sites such as Facebook or Twitter, unless it has been approved for public release by appropriate U.S. government authority. Proposed public releases shall be submitted for approval prior to release through PEO (T), Public Affairs Office, 47123 Buse Road, RADM William A. Moffett Building, Patuxent River, MD 20670-1547.

3.2.4.3 Loss, Compromise, and/or Electronic Spillage of Classified or Controlled Unclassified Information: All instances of loss, compromise, and electronic spillage of classified or controlled unclassified information shall be reported to the COR, TPOC and Government Security Office within 24 hours of the incident occurring.

3.2.5 Operations Security (OPSEC): The Contractor shall comply with activity OPSEC program instructions, guidance, and contribute to organization-level OPSEC efforts. The Contractor will include OPSEC as part of its ongoing security awareness program and take all required NAWCAD 7.2 OPSEC training. The Contractor will protect identified critical information, sensitive unclassified information and activities, which, if divulged, could further compromise classified or sensitive information or operations, or degrade the planning and execution of operations performed by the RO and contractor in support of the mission.

While performing aboard NAVAIR or NAVAIR sites, the Contractor shall comply with facility OPSEC program instructions and contribute to organization-level OPSEC efforts, including OPSEC as part of its ongoing security awareness program and take all required Agency training; being responsive to the Supporting OPSEC Manager on a non-interference basis; and protecting sensitive unclassified information and activities, which could compromise classified information or operations, or degrade the planning and execution of operations performed by the RO and contractor in support of the mission.

3.2.6 Anti-Terrorism Force Protection and Emergency Management.
The work performed on this contract is not Emergency Essential in accordance with OPNAVINST 3440.17A and Government Emergency Management, Antiterrorism and/or Continuity of Operations Plans. Contractor personnel shall comply with all Government Emergency Management, Antiterrorism and/or Continuity of Operations Plans and directives. Non-Essential Contractor personnel shall not report for work at Government facilities upon declaration of Force Protection Condition CHARLIE or in any event or emergency where Government official's direct curtailment of operations to "Mission Essential Only". All Contractor personnel assigned to a government facility shall complete annual Antiterrorism (Level One) and Active Shooter training.

3.2.7 Program Unique Requirements

3.2.7.1 Disclosure of Information:

Contractor employees shall not discuss or disclose any information to which they are exposed during the execution of contract tasking to parties other than the originator of the information, authorized Government investigative personnel, the Contracting Officer, or COR personnel. Improper disclosure of sensitive information may be grounds for removal of Contractor personnel.

3.2.7.2 DOD 8570.01-M Information Assurance Workforce Improvement Program DOD Directive provides guidance for the identification and categorization of positions and certification of personnel conducting Cyber Security functions within the DOD Workforce supporting the DOD Global Information Grid (GIG) per DOD Instruction 8500.2 (Reference (b)). The DOD Cyber Security Workforce includes, but is not limited to, all individuals performing any of the Cyber Security functions described in Directive 8570-01-M. All contractor personnel supporting this task order must comply with DOD Directive 8570.01-M, where applicable and any training required to comply with this directive is at the expense of the contractor. The TPOC will assign the appropriate certification category based on the duties and responsibilities being performed, relative to the current published DOD 8570 Manual. Upon subsequent release of DODI 8140.01, the Contractor shall adhere to updated guidance on cyber security workforce qualifications.

3.3 Detailed Support Requirements:

3.3.1 Government Technical Environment
A representative hardware inventory of the Government IT Environment consists of the following:

TYPE	OS_TYPE	
APPLIANCE	(b) (3) 10 U.S.C. § 130	
APPLIANCE Total		
Virtual Servers		
	(b) (3) 10 U.S.C. § 130	
Virtual Server Total		
Physical Servers		
	(b) (3) 10 U.S.C. § 130	
Physical Server Total		
Sever Total		
Switch		
	(b) (3) 10 U.S.C. § 130	

TYPE	OS_TYPE	
	(b) (3) 10 U.S.C. § 130	
Switch Total		

DATA STORAGE & PROTECTION	(b) (3) 10 U.S.C. § 130	

Historically the network transport environments include: (b) (3) 10 U.S.C. § 130

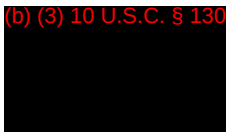
With the exception of voice infrastructure, (b) (3) 10 U.S.C. § 130

A representative software inventory of the Government IT Environment consists of the following:

(b) (3) 10 U.S.C. § 130

Operating Systems:

(b) (3) 10 U.S.C. § 130


(b) (3) 10 U.S.C. § 130

3.3.2 Enterprise Hosting Services: Contractor shall perform Enterprise hosting support services tasks in such a manner as to ensure a high quality of continuity of services and effective utilization of resources across service areas. The Contractor shall establish and execute a well-coordinated, collaborative, tightly integrated and cross-disciplined IT service provider team in order to effectively and efficiently optimize delivery and performance of IT services and establish reliable, resilient, flexible, and scalable IT environment to support the Government in achieving and sustaining the IT related mission.

3.3.3 Stability and Continuity of Workforce: The Contractor shall ensure stability and continuity of the work force, maintaining an adequate work force for growth requirements and the uninterrupted performance of all tasks defined within this task order.

3.3.4 Technological Advances: The Contractor shall remain current on technological advances relevant to the requirements and capabilities supported and provide documented recommendations on strategic planning for future initiatives that offer cost savings and efficiencies. The Contractor shall provide recommendations to sustain and improve existing and new business systems IT capabilities.
A010 Lifecycle Management and Technology Refreshment Reporting

3.3.5 Sustained Systems: All systems shall be sustained such that they satisfy organizational requirements for timely, effective and efficient collection, processing and storing of data, system application and data availability to customers. Systems shall be inherently capable of producing information required by managers and working level personnel when required.

3.3.6 NAWCAD 7.2 Work Acceptance Processes: The Contractor shall adhere to the 7.2 Work Acceptance Processes, which will be provided as Government Furnished Information after award.

3.3.7 Command, DOD / DON Initiatives: Support activities shall comply with Command initiatives (e.g., Navy ERP, AIRSpeed, etc.) and DOD / DON initiatives, standards, policies, and mandates (e.g., DON Application and Database Management System (DADMS), DOD IT Portfolio Repository (DITPR-DON), Defense Business Transformation Guidance, Navy Enterprise Application Developer's Guide (NEADG), industry provided developer guidance, Clinger Cohen Act, Federal Information Security Management Act (FISMA), and/or Web Enablement).

3.3.8 Innovative Solutions: Because of the broad area of tasking and the costs involved, the Contractor shall recommend innovative solutions to provide 24x7x365 coverage while keeping in mind cost, schedule, and performance attributes.

3.3.9 Enterprise-Wide IT Support Services: The Contractor shall provide enterprise-wide IT support services to manage the Government's enterprise-wide IT server and storage computing environments; NAVAIR Headquarters and all Component Commands Aircraft Division (AD), Weapons Division (WD), and Fleet Readiness Centers (FRCs). The Government will coordinate priorities for all tasks and activities essential for the Government to optimize enterprise-wide IT resource operational performance.

3.3.10 Designated Points of Contact (POC's): When requested by the Government, the Contractor shall designate individual(s) POC's to address IT server, storage technology, and service delivery issues. The POC's shall develop and make recommendations on potential courses of action and develop actionable plans to address Government approved course(s) of action. The assigned individuals shall have the relevant expert level expertise in the subject area assigned, which includes:

a) Server and storage performance and process management, architecture, design, configuration, and technology management
b) Server and storage security management and protection
c) Standards and quality assurance management
d) IT environment configuration and capacity management
e) Technology refresh and IT modernization planning
f) Network technologies and solutions
g) IT related subject areas where the Government deems it lacks appropriate skills and proficiency
h) Mobile Computing Platforms

i) Mobile Device Management Services
j) Cloud computing and related "X-As-A-Service" models [Hardware-As-A-Service (HAAS), Capacity-As-A-Service (CAAS), Infrastructure-As-A-Service (IAAS), Platform-As-A-Service (PAAS), Software-As-A-Service (SAAS)] operations in a Commercial Cloud Commuting facility.

3.3.11 Program Management: The Contractor shall provide on-site working level program management for the management and oversight of all tasking performed under this task order.

• The Contractor shall provide an on-site program manager who shall be responsible for management and oversight of work performance for this contract. Program management duties include:
a) Serving as a POC for customer relations
b) Ensuring adequate program controls are applied to each task area including scheduling, resource allocation, direction, cost quality control, report preparation, establishing and maintaining records, and resolution of customer complaints
c) Resolving quality, timeliness, and accuracy issues
d) Reviewing Contract Data Requirements List (CDRLs) for quality before submission to the Government
e) Providing a means of immediately contacting her/him or designated alternate, 7 days a week, 24 hours a day, 365 days a year. The Contractor shall ensure the management or designated alternate makes verbal contact with the TPOC within sixty (60) minutes.
f) Attending meetings with the COR or TPOC to discuss performance under the task order or resolution of any perceived performance problems.

The Contractor shall provide administrative support necessary to coordinate and assist 7.2 business and management operations. In support of this tasking, the contractor shall be responsible for:
a) Providing advisory and draft documentation support for the creation of internal and external briefings, graphs, white papers, organizational charts and operational reports using identified government standard applications
b) Operating facsimile, reproduction, shredding, printing, and scanning equipment
c) Collecting information to support various data calls
d) Coordinating and scheduling of meetings, focus groups, and training events
CDRL A002- NAWCAD Trusted Cloud Credential Manager Policy
CDRL A003 - CSP Administrator Account Management Policy
CDRL A004 - Governance and Design Documents, Templates, Plans and Diagrams
CDRL A005 - Customer/Cost Management Policy
CDRL A006- Agnostic NAWCAD CSP Management Policy
CDRL A016 – Configuration Management Reporting

3.3.12 Contractor Coordination Requirement: The Contractor shall successfully integrate and coordinate all activity needed to execute the tasking, the timeliness, completeness and quality within this task order, as well as, the integration with all other potential vendors (task orders) supporting the AD / AIR 7.2 organization. The Contractor shall support operations, manage projects, and deliver services such that external collaboration with Subject Matter Experts (both government and Contractor Support Services (CSS)) shall be efficiently and effectively accommodated as required by the government.

3.3.13 Support Response Requirements: The Contractor shall manage service delivery and perform its services in accordance with the support response requirements as described below. The Contractor shall use established incident management processes to respond to customer requests. Trouble tickets/incidents shall be acknowledged within thirty (30) minutes of assignment and customer contacted via phone.

3.3.14 Support Solutions: The Government is willing to consider recommendations for other IT Service Area delivery support solutions keeping in mind the goal is to achieve maximum coverage and incident response at the least cost.

3.3.15 Routine Incident Response: The Contractor shall support the NAVAIR incident response process for routine incidents. Routine incidents are those incidents that have limited impact to NAVAIR operations

and do not pose a significant impact to customers or threat to DOD data or service delivery. These could include events such as a server outage, appliance malfunction, minor malware incidents, network outage, and GENSER SECRET and below level spillages.

3.3.16 Enterprise Hosting Performance Requirements: The following sections outline the specific technical, program management and support requirements.

3.3.16.1 On-Site Service Delivery Managers
The Contractor shall identify On-Site Service Delivery Managers (SDMs). The Contractor's SDMs shall be "key personnel" and Team Leads responsible for coordinating and managing day-to-day service delivery of their respective Technical Domain. This includes all operational environments, organizational relationships, resource utilization, capacity management, and service delivery activities, in cooperation and coordination with Government personnel, other IT service providers, and all third-party providers associated with delivering or supporting the Government IT environment. The Contractor SDMs shall be responsible for providing support to optimize server and storage service delivery, minimize service disruptions and facilitate resolution of disputes and service delivery issues that may arise between the Contractor and other IT service providers.

3.3.16.2 On-Site Operation Managers: The Contractor shall provide at least one On-Site "Operations Manager" for the coordination and oversight of the entire Data Center (Table in 1.3.3 - Service Areas; Enterprise Hosting) operational activities to ensure all technical domains are meshed into a single operational hosting capability. The Contractor's Operations Management shall work closely with the Government Data Center Manager/Branch Head and present holistic analyses and situational awareness of operational issues, concerns, outages and service interruptions to provide the Government with advice and recommendations needed to select appropriate solutions or other courses of action.

3.3.16.3 On Premise and Cloud Growth and Scope: As an enterprise-wide hosting facility, the Data Center provides services to over 100,000 customers world-wide. Historically, it has encountered 83 new customers/projects a year. Even with this growth, in supporting Federal and Navy initiatives, such as the Data Center Optimization Initiative (DCOI), and other green initiatives, such as virtualization, the Data Center has achieved significant footprint reduction over the last ten years. The Enterprise Hosting Service Area provides reliable unclassified and classified secure technologies to deliver a range of enterprise level hosting capabilities to NAWCAD, NAVAIR, and other Navy customers. The team provides solutions utilizing a variety of environments and tool sets. The contractor will provide support to the entire technology stack of servers, networks, storage, communication devices, peripherals, applications, etc. ensuring the availability, integrity, and confidentiality of complete solutions required by our customers. Core services include systems administration of various operating system environments; networking communications support; data protection and recovery support; disaster recovery and continuity of operations support; project management; risk management; integration and engineering support; research; architectural design; information assurance support activities; system integration; acquisition management support; configuration management; monitoring of configurations, performance, system availability, and capacity; supporting maintenance and administration of application solutions; strategic planning; and customer technical assistance. All efforts support DOD/DON directives and policies. Additionally, as the team transitions through Next Generation Enterprise Network ((NGEN); NMCI) Contractor support will be required to ensure policies, processes, and procedures are developed and sustained in the new environment. Data Center personnel shall be required to work with the NGEN contractor as this contract evolves.

3.3.17 Schedule Maintenance Hours Requirement: Four (4) twenty-four (24) hours periods per month shall be scheduled on Saturday/Sunday to provide windows of time for system security compliance, upgrades, implementations, and other maintenance activities requiring service disruption. This support is considered to be part of the standard business operations core requirements and should be priced as part of the submission.

3.3.18 Integration and Systems Engineering: The Contractor shall work with the Government and other service providers to support integration, configuration, release and testing activities in support of, and in response to, Government mission requirements for secure, sustainable, and production-ready IT solutions in

compliance with, and adherence to, regulations as defined by the Government. A comprehensive list of Navy regulatory documents is located at the DON CIO IT Policy and Guidance website at http://www.doncio.navy.mil/.
The Contractor shall perform all lifecycle support activities for all Government enterprise infrastructure hardware, software and management tools, which will include installing, monitoring, supporting, documenting, testing, configuring and reconfiguring, integrating, updating/upgrading, repairing, performing version control and managing the Government's IT environment. Planning, designing, and engineering tasks could be performed by the Government or other service providers; however, the Contractor will be expected to participate in these events.

The Contractor shall assist with the preparation of the documentation to procure hardware, software, maintenance, licensing and supporting supplies utilizing NAVAIR acquisition management system tools such as Program Management Tool, NAVITAS, DADMS, etc., to include the preparation of required documentation for purchasing card and other orders.

The Contractor shall maintain, revise, update and/or create the as-built system configuration documentation to ensure that the documentation accurately reflects the configuration status at any given point in time. The Contractor shall coordinate with Government personnel to identify and recommend opportunities for continual service improvements, and plans and implements approved recommendations.

The Contractor shall provide engineering and implementation of infrastructure services and components defined in the DISA Secure Cloud Computing Architecture V2.9 (SCCA) and Cloud Computing Security Requirements Guide V1R3 (SRG) to architect the cloud computing environment. The Contractor shall consult with the Government team to produce working papers, such as policies, diagrams, templates, etc.

The Contractor must be a premier/preferred cloud services reseller to the government, to include but not limited to Amazon Web Services and Microsoft Azure.

3.3.18.1 Contractor Continual Service Improvement (CSI) Management Support: The Contractor shall provide CSI recommendations to enhance mission value, longevity, supportability, performance, maintainability, manageability, flexibility, scalability, capacity, availability and responsiveness. The Contractor's CSI recommendations shall encompass and include Service Delivery process improvements, as well as improvements that can be made to hardware, software and/or changes. The Contractor shall provide recommendations on how to achieve optimal usage and performance of system resources based upon the results of its industry subject matter expertise, product knowledge and ongoing system assessments and shall design and implement approved recommendations. The Contractor shall combine principles, practices, methods, and knowledge learned from Service Strategy, Service Design, and Service Operations to achieve incremental, as well as significant improvements in service quality, operational efficiency, and mission continuity. The Contractor shall ensure that all CSI recommendations continually align and realign IT services to the changing business needs by coordinating assessments, identifying, and implementing improvements to IT services that support business processes. The Contractor shall ensure that all recommended improvements support the lifecycle approach through Service Strategy, Service Design, and Service Operation. Recommended CSIs shall be designed to improve process effectiveness, efficiency, delivery performance, and cost effectiveness.

3.3.18.2 Service Strategy Management Support: The Contractor shall assist the Government in the collection and analysis of sufficient information to determine the most appropriate strategic courses of action related to NAVAIR direction or directives with a reasonable level of assurance that the overall mission benefits justify the potential costs and risks of a specific solution(s). The Contractor shall:

a) Provide recommendations on defining IT services offerings
b) Recommend system and service delivery changes that will enhance the IT value for government personnel
c) Provide recommendations and develop the business cases for strategic IT investments
d) Provide and maintain transparency and compliance with financial controls
e) Provide support for defining thresholds relating to the quality of IT services to be delivered
f) Identify, analyze, and recommend alternate paths for improving IT service quality

g) Recommend how to efficiently allocate IT resources across a portfolio of services
h) Recommend processes for resolving conflicting demands for shared IT resources

3.3.18.3 IT Governance: The Contractor shall make recommendations pertaining to IT service delivery to identify opportunities to optimize the decision-making process for determining appropriate courses of action in development of the IT service delivery strategy for the Government. The Contractor shall establish, update, and maintain an IT service delivery governance structure that aligns with and supports the Government service management requirements and governance framework. The Contractor shall participate in and provide support in governance committee and/or CCB meetings. The Contractor shall establish and manage the relationships with external IT governance and management structures (e.g., DON CIO, OPNAV N2/N6) as well support the management of relationships with external (third party) IT governance and management structures (e.g., NMCI, or NGEN).
CDRL A004 Governance and Design Documents, Templates, Plans and Diagrams

3.3.18.4 Demand Management: The Contractor shall analyze and develop an understanding of end-users/processes that are utilizing or consuming IT resources, to what level, and the scheduling requirements for when IT resources must be available. The Contractor shall support activities to forecasts future IT resource Demand Management Requirements (DMR) in correlation with Capacity Management and Availability Management to synchronize high-performance, effective use of available IT capacity through asset configuration management and control.

3.3.18.5 Capacity Management: The Contractor shall provide advisory assistance to the Government for determining capacity utilization thresholds that support evolving IT mission requirements. The Contractor shall ensure that IT processing and storage capacity match the evolving demands of the Government's mission requirements in a cost effective and timely manner. The Contractor shall provide support for the three (3) Capacity Management sub-processes of mission capacity, which as defined by ITIL V3 are:
1) Business Capacity Management (BCM)
2) Service Capacity Management (SCM)
3) Resource Capacity Management (RCM)

The Contractor shall perform the forward- looking Mission Capacity Management process in conjunction with the Services Delivery Capabilities defined by Service Capacity (i.e. the current IT service delivery model defined by architecture capability, deliverable capacity, and Service Level Agreements) and provide advisory and draft documentation support for the translation of mission requirements into infrastructure demands. The Contractor shall monitor, manage and report on the RCM process of the infrastructure configuration capacity against an established set of utilization thresholds via threshold-based management reporting schemes and other techniques. The Contractor shall also monitor, manage, and report on the client-facing SCM process for Service Level Agreements (SLAs).
CDRL A008 – Capacity Report

3.3.18.6 Service Portfolio Management: The Contractor shall provide advisory assistance to the Government for determining options for the IT strategy to support its customers and in developing, maintaining and aligning the Government's service offerings and capabilities. The Contractor shall provide advisory, draft documentation, and management support for Government-approved enterprise-level IT service portfolio that provides Government end-users with pre-defined set of IT products and services that can be ordered from and provided by the Government in support of NAVAIR's IT mission.

3.3.19 Enterprise Architecture Strategy Support Services: The Contractor shall participate in and provide IT architecture design efforts and provide performance advisory service to support the Government's evolving mission objectives and ensure that all enterprise hosting systems and solutions can continue to deliver secure, fast and effective computing services while optimizing computing resource utilization and costs. The Contractor shall leverage all support areas, performance monitoring measures, capacity and demand information and problem management to advise the Government on necessary architecture changes and/or system improvements. The Contractor shall stay abreast of state of the art technologies to ensure accurate, best practice solutions are recommended to the Government as part of new implementations or modernizations of existing architectures. The Contractor shall collaborate with the Government, other

Contractors, and vendor subject matter experts to ensure recommendations evolve into executable improvements. The Contractor shall interface with various external government organizations as well as subject matter experts to ensure all solutions are Green IT centric. The Contractor shall assess, recommend, and perform system integration functions. The Contractor shall assess new technologies and develop architecture and supporting business plans and processes to adopt Government approved new technologies. The Contractor shall have the relevant expertise in the subject areas, which include but are not limited to, enterprise hosting, data storage and protection, converged networking, mobile computing solutions, and cross platform information sharing and cyber security.
CDRL A010 – Lifecycle Management and Technology Refreshment Report

3.3.19.1 Planning and Analysis: The Contractor shall research, analyze, plan, coordinate, and recommend software, system, server, storage, networking and related process options and alternatives that offer opportunities to improve efficiency and effectiveness of IT service delivery to meet the Government's mission requirements. The Contractor shall interact with the Government so that it can identify potential improvement opportunities, to analyze and solve problems, and develop draft specifications of IT processes and systems for Government consideration that are designed to meet the requirements of end-users.
CDRL A010 - Lifecycle Management and Technology Refreshment Report
CDRL A011 – Planning and Analysis Reports
CDRL A012 - Feasibility Studies

3.3.19.2 Service Continuity: The Contractor shall provide support for the development of plans and processes to ensure IT services, systems, and related infrastructure can recover and continue to operate in the event of an anomaly. This service includes both proactive and reactive measures to reduce the risk of a disaster in the first instance and optimize recovery time should a major disruption or disaster occur to any of the Government's IT applications and associated infrastructure (e.g., Central Processing Unit (CPU), servers, storage, data and output devices, End-User devices.) Government applications and associated infrastructure will receive Disaster Recovery (DR) Services according to the Government's Business Continuity Plan and SLAs. The Contractor shall review and evaluate the end-to-end operational integrity of the Government's entire mission-critical IT services and service delivery environment to identify any real and/or potential cyber vulnerability that could put the Government's mission at risk if the system or service delivery were to fail.

The Contractor shall report its findings and include recommendations on course of action to be taken to eliminate or minimize any discovered cyber vulnerability, while the overarching objective is to ensure that the whole end-to-end IT environment can continue to operate should a serious incident occur.
CDRL A010– Lifecycle Management Reporting

3.3.19.3 Project Management (PM): The Contractor shall perform all project lifecycle and management activities in support of IT Project Management Services in accordance and compliance with all Government defined PM policies and procedures and utilize all tools specified by the Government in accomplishing the Government's project goals or objectives.

The Contractor shall provide advisory and draft documentation support for the development; and the Government shall review and approve project success criteria measured objectively against the achievement of goals to justify decisions to move ahead, correct, or terminate a project. The Contractor shall perform project planning, execution, and closure phases in accordance with all Government defined requirements.

The Contractor will develop IT Services project management plans, processes, and procedures that comply with the Government approved Framework (e.g. projects feasibility analysis, cost-benefit analysis Scheduling, costing, resource planning, communication planning, Procurement, risk management, and quality management). The Contractor will review and approve performance data dashboards, document milestone completions, and communicate to appropriate stakeholders.

3.3.19.4 Equipment Installation Planning and Coordination: The Contractor shall provide IT equipment installation planning and coordination services to the Government, including implementing and monitoring

compliance with enterprise-wide policies and procedures to be used for the planning and installation of new IT equipment, products, and services.

The Contractor shall coordinate inventory management of IT server and storage equipment, software, and services. The Contractor shall manage the delivery, storage, scheduling, installation, and verification testing of all hardware and software. The Contractor shall document (in draft format for Government consideration), maintain, and update configuration files, IP addressing schemas, and related business information for all IT hardware. The Contractor shall ensure that data records for all newly procured equipment and software are included in configuration management documentation.
CDRL A013 – IT Asset Database Report

3.3.19.5 Asset Management: The Contractor shall support the recording, monitoring, updating, maintaining and management all asset data records for all IT Service Areas (Table in 1.3.3) using the Government's asset management system. This includes all newly acquired IT Service Area components (e.g., hardware, software and software licenses, maintenance, etc.) and their attributes (e.g., location, costs, depreciation, contracts, vendor, serial numbers, etc).
The Contractor shall support maintenance activities and asset inventory control (including hardware and software license attributes), hardware and software asset lifecycle planning and management (e.g., timing of asset refresh, asset disposition), software version management and identify opportunities for refresh or insertion of technology.
The Contractor shall provide technology refreshment recommendations to support Government technology refreshment planning needs, including equipment order scheduling to support Government technology refreshment timelines.
The Contractor shall utilize a Government-provided centralized data repository for recording and tracking information pertaining to all IT related asset warranty agreements and maintenance contracts (vendor name, commencement and expiration date, services/assets covered, fees, etc.) needed for accurate tracking to support the ongoing operations, repair, and maintenance of Government systems.
CDRL A007 – Physical to CMDB Delta Report
CDRL A010 – Lifecycle Management and Technology Refreshment Report
CDRL A013 – IT Asset Database Report
CDRL A014 – Asset Management Report
CDRL A015 – Inventory Report

3.3.19.6 Configuration Management (CM): The Contractor shall support all lifecycle IT CM activities, which shall be performed in accordance and compliance with Government enterprise-wide CM policies and procedures. The Contractor shall use the Government's CM system to record, track, monitor and update all component configurations, all subsequent component configuration changes, licensure, and Item Unique Identifier (IUID). The Contractor shall monitor its personnel to ensure they comply with the accurate and timely recording of all IT asset parameters as specified in CM requirements. The Contractor shall include a logical model of its Service Areas' devices and their relationships by identifying, controlling, maintaining, and verifying installed hardware, software, and documentation (i.e., maintenance contracts, SLA documents, etc.). The Contractor shall use the Configuration Management System to account for all IT Assets and configurations to provide accurate information on configurations and provide a sound basis for incident, problem, change, and release management and to verify configuration records against the infrastructure and correct any exceptions.
CDRL: A016 Configuration Management Report

3.3.19.7 Change Management: The Contractor shall perform all IT change activities in accordance and compliance with Government established change management standardized process for the efficient and prompt handling of all IT Change Requests (CRs) (e.g., submitting, reviewing, prioritizing, approving, recording, managing the processes, etc.). The Contractor shall ensure that any change introduced into any production environment has been tested and verified for integration compatibility, security, functionality, and performance in order to minimize the impact upon service quality and consequently improve the day-to-day operations.

The Contractor shall establish standardized methods and procedures for the efficient and prompt handling of all IT CRs (e.g., submitting, reviewing, prioritizing, approving, recording, managing the processes, etc.), in order to minimize the impact of change upon Service quality and consequently improve day-to-day operations. The Contractor shall monitor and report on Contractor personnel compliance with the Change Management processes.
The Contractor shall ensure that the Change Management process incorporates ITIL best practices, processes, and procedures for managing the introduction and implementation of all IT related changes and coordinate its change management activities with all IT service providers. The Contractor shall ensure that its Change Management processes include interfaces with the Release Management, CM, and Asset Management, Incident Management, and Problem Management processes.

3.3.19.8 Release Management: The Contractor shall perform all lifecycle Release Management activities related to preparing any new or reconfigured IT equipment or software for integration and testing. The Contractor shall adhere to Release Management processes for implementing Government- approved changes to IT services, both the software and the hardware. The Contractor shall use a holistic approach in supporting the Release Management processes and methodologies to ensure that both the technical and non-technical aspects of a Release are taken into consideration in planning the introduction into production of and approved changes in software, hardware, policy and/or procedural changes.

The Contractor shall collaborate and work closely with all other relevant Release Management IT support teams/stakeholders that address support interdependencies and incorporate appropriate linkages and dependencies into the Release Management processes.
The Contractor shall incorporate a categorization methodology into the Release Management process that accommodates various levels of importance for releases and include the following release levels:
- Major software Releases and hardware upgrades or replacements, normally containing large areas of new functionality. A major upgrade or Release usually supersedes all preceding minor upgrades, Releases, and emergency fixes
- Minor software Releases and hardware upgrades, normally containing small enhancements and fixes, some of which may have already been issued as emergency fixes. A minor upgrade or Release usually supersedes all preceding emergency fixes
- Emergency software and hardware fixes, normally containing the corrections to a small number of known problems
- After Actions Review (AAR); normally review lessons learned to apply to future implementations

The Contractor shall ensure that data records for all newly procured equipment and software are included in CM documentation. The Contractor shall conduct a review and analysis of Releases that resulted in implementation of the back-out plan and develop recommendations for a Service Improvement Plan (SIP) to address and resolve failure points and implement Government-approved corrective or follow-up actions to minimize future occurrences

3.3.19.9 Documentation: The Contractor shall perform all lifecycle activities to create, revise, update, store, manage and provide all required documentation in a form and format acceptable to the Government, including obtaining Government documentation approvals and maintaining revision control. The Contractor shall ensure that all copies of documentation are provided in electronic format and are recorded and stored in a Government common documentation library (e.g., SharePoint). Documentation management shall include developing, revising, updating, maintaining, reproducing, distributing, and archiving all Service Area information and documentation in electronic and hard copy format as defined by the Government.

The Contractor shall validate the briefing and/or training of all Contractor personnel in methods and timeliness of preparing, developing, distributing, and/or complying with all Government documentation standards, security and quality requirements, review and approval processes, and documentation library usage. The Contractor shall monitor the documentation management process to ensure that all documentation is correct, up-to-date and accurately depicts or describes the as-installed IT environment, and that it contains all appropriate version information, attributions, and approvals.

The Contractor shall recommend Documentation requirements and formats. The Contractor shall document (in draft format for Government consideration) system requirements, functional and technical designs and specifications, hardware and software configurations (e.g., interconnection topology, configurations, architectural diagrams), etc. as required for all IT server and storage infrastructure for each phase of the IT service lifecycle. The Contractor shall document (in draft format for Government consideration) Standard Operating Procedures (SOPs) and (e.g., boot, failover, patch management, security scans, system backups, system event alerts and logging, event log reviews, production maintenance schedules, escalation procedures, etc.).
CDRL A017 – Requirements, Function/Technical Design, and Architecture Documentation

3.3.19.10 Quality Assurance (QA)/Quality Control (QC) Services: The Contractor shall document (in draft format for Government consideration) and implement Quality Management System (QMS) processes and procedures that comply with Government-specified QMS requirements to ensure a standard, formal, and consistently applied approach for quality management, including quality requirements and criteria, key IT processes and their sequence and interaction, and the policies, criteria, and methods for defining, detecting, correcting, and preventing non-conformity and potential quality gaps. The Contractor shall establish, maintain, and update a QA and QC documentation repository where all QA and QC records, reports, and plans are stored; and provide Government free and open access to the repository as all times. The Contractor shall conduct QA reviews and postmortem analysis of work activities and project/product deliverables to identify areas for correction and opportunities for improvement.
CDRL A018 – Quality Management Report

3.3.20 Systems Administration: The Contractor shall provide IT Services to the Government in accordance with the requirements specified in this PWS. As defined by the Government, “IT Services” are all services and activities required to provide and support the Government Service Areas defined in Table on Section 3.3.1 and subsequent sections provide a set of ITIL aligned practices for IT Service Management (ITSM) that focuses on aligning the delivery of IT services with the needs of the Government. All work as described and performed in accordance to this Section shall adhere to that established framework, as well as additions described throughout this section.

Systems Administration Support for the Government Service Delivery Environment (both on premise and cloud based) encompasses all production, QA, staging, test, and development server and storage hardware and software infrastructure elements and supporting equipment, which include:

a) Unix-based servers, Windows-based servers, Linux-based servers, Load- Balancing devices, network devices, boundary security devices, converged networking devices, Public Key Infrastructure/Public Key Encryption (PKI/E) devices, and other hardware running all enterprise mission applications and services (e.g., application servers, database servers, middleware servers, web portal servers, internet/intranet servers, email/collaboration servers, file/print servers, shared drive(s), DNS servers, proxy servers, etc.). This includes all supporting equipment and system software (e.g., operating systems, virtualization software, authentication software, utilities, schedulers, etc.)
b) data storage hardware and software for all computing environments (e.g., SAN/NAS storage arrays, etc.)
c) all server and storage management tools and utilities (e.g., command consoles; authentication, automation, and optimization tools; security monitoring; protocol analysis; system and data backup, recovery, and archiving, etc.)
d) all server and storage physical equipment racks and patch panels, Keyboard, Video, Mouse (KVM) switches and monitoring consoles, intra-cabinet wiring/cabling, etc.)
e) use of all tools required to monitor, patch, maintain, and sustain the operating environment.

The Contractor shall provide and perform all services in accordance with the conditions and support parameters stated in all sections of this PWS. In support of this tasking, the Contractor may be required to:

a) Install, upgrade, and configure operating systems, system software, hardware and peripherals.
b) Install, configure, tune, maintain, administer, upgrade, backup and restore software, including third-party applications as applicable. Ensure data is protected.

c) Troubleshoot, diagnose, resolve issues and/or make suggestions on solutions for the operating system, system software, hardware, peripherals, user access, and connectivity.
d) Monitor system operability and performance (e.g., CPU/memory utilization, file system space) on a daily basis and make recommendations as applicable.
e) Evaluate, apply, and respond to Information Assurance Vulnerability Alert (IAVA) Certification (CERTS), Bulletins, Chief Technology Officers (CTOs), and Advisories.
f) Establish and maintain system security posture in compliance with DoD Security Technical Implementation Guidelines.
g) In coordination with application administrators, provide advisory and draft documentation support for the development of mitigation plans, Information
Assurance Vulnerability Management (IAVMs), and vulnerabilities that cannot be resolved due to functionality requirements
h) Respond to cyber threats and cyber vulnerabilities, as required.
i) Develop scripts to automate the administration process for all systems.
j) Monitor growth and equipment needs and advise the Government of potential issues for consideration.
k) Manage, maintain, and administer systems management/utility servers
l) Maintain facsimile solutions.
m) Maintain and administer directory services.
n) Apply best practices for tuning the operating system for overall system performance.
o) Evaluate, install, configure, and support High Availability systems.
p) Install, develop, maintain, and monitor SAN environment ensuring SAN services are available as applicable.
q) Coordinate and/or work with other teams and/or vendors to assist with hardware and software installations and updates.
r) Provide technical assistance to other teams, customers, and vendors regarding the operation systems, system software, hardware and peripherals.
s) Support DOD, DON, and NAVAIR directives to reduce and consolidate the IT environment. Participate in transition and migration activities.
t) Support access solutions by performing tasks to include, but not limited to, user account administration, password resets, account auditing, etc.
u) Request and track all NMCI CLIN27 server connections following the NMCI CLIN27 process.
v) Maintain System Configuration documentation and operational instructions, including software installation instructions, operating system installation and system configuration documentation.
w) Create and provide monthly metrics (e.g., percentage of server up time, amount of data archived via back-up routines, available data storage capacity, and storage area network utilization and available capacity, equipment growth, power consumption, etc.).
x) Perform project management duties.
y) Provide technical, design, and integration support of Voice Over Internet Protocol (VOIP), Voice and Video Over Internet Protocol (VVOIP), and/or data services in support of DOD/DON Unified Capabilities Plan.
z) Provide monthly status report.

CDRL A001 – Monthly Status Report
CDRL A009 – Operational Reporting

3.3.20.1 Operations & Administration Services: The Contractor shall manage all aspects of all classes of servers and supporting equipment as described in Part 3.3, including all hardware and software systems and tools used to monitor, maintain, optimize, and report on environment health and status. The Contractor shall support all servers and other hardware running all enterprise mission applications and services. The Contractor shall support all physical servers, as well as all logical servers (i.e., virtualized). The Contractor shall provide support for all supporting equipment and system software (e.g., Operating Systems (OS), virtualization software, authentication software, utilities, schedulers, etc.).
The Contractor shall provide advisory and draft documentation support to establish, document, and implement enterprise-wide operations and administration policies, procedures, and standard tools to be used by all IT Service Areas for providing and maintaining a stable IT infrastructure capable of providing IT Service Delivery that meets or exceeds SLA performance threshold targets and requirements. The

Contractor shall ensure that all SDMs perform their respective operations and administration tasks and activities in accordance with the Government-approved requirements and in cooperation and collaboration with all other IT service providers involved with or impacted by these support activities.

The Contractor shall develop, document, and maintain in the Standard Process and Procedures Manual, Operations, and Administration procedures that meet requirements and adhere to defined policies. The Contractor shall perform day-to-day server and storage operations and administration activities. The Contractor shall maintain and provide audit information including access, general logs, application logs in accordance with the Government's security policies.
CDRL A009 – Operational Reporting
CDRL A017 – Requirements, Function/Technical Design, and Architecture Documentation
CDRL A023 – Desktop Guides

3.3.20.2 Maintenance and Break/Fix Actions: The Contractor shall collaborate with other IT service providers for the delivery of all IT Service Area deliverables supporting the activities associated with the maintenance and repair of all IT hardware and software to include all "Break/Fix" Services.
The Contractor shall coordinate with NAVAIR National Helpdesk (NNHD), the Government's customers, and all other IT service providers on planning and scheduling maintenance downtime on all server and storage systems, including identifying maintenance to be performed, the systems impacted, and coordinating scheduling to minimize potential downtime conflicts with other services. The Contractor shall ensure appropriate maintenance coverage for all Service Area components. The Contractor shall replace defective parts including preventive maintenance, according to the manufacturer's published mean-time-between failure rates. The Contractor shall conduct investigations and produce After Action Reports as required.
CDRL A017 – Requirements, Function/Technical Design, and Architecture Documentation

3.3.20.3 Storage Management/Backup and Recovery Services: The Contractor shall manage all aspects of all tiers of storage resources located as described in Part 3.3, including all hardware and software systems and tools used to monitor, maintain, optimize, and report on storage environment health and status.
The Contractor shall provide support for types of data storage resources including, SAN, NAS, Redundant Array of Independent Disks (RAID) arrays, storage virtualization, data de-duplication, archival/tape backup, etc., and any future implemented storage technology as defined by the Government.
The Contractor shall provide advisory and draft documentation support to recommend, define, document and implement, enterprise- wide server and storage system backup and recovery processes and procedures to ensure consistent compliance and performance of the required backup and recovery activities for all respective IT Service Areas. The Contractor shall monitor all storage backup activities on all IT systems in accordance with Government-designated backup schedules and periodically conduct tests to ensure that the backup media can be read and data restored from magnetic storage media in accordance with Government defined schedules and requirements.
The Contractor shall develop, document, and maintain in the Standards and Process and Procedures Manual all Backup and Recovery schedules and procedures that adhere to Government requirements and policies for IT services. The Contractor shall test backup media to ensure incremental and full recovery of data is possible and ensure Service Area component integrity.

3.3.21 IT Resource, Training, and Knowledge Transfer Management: The Contractor shall maintain a competent IT workforce to ensure the delivery of IT services. The Contractor shall identify key personnel and promptly fill any key personnel position vacancies.
The Contractor shall identify key personnel and inform the Government of any potential key personnel staffing changes and of any new personnel assignments planned for new projects and services. The Contractor shall obtain appropriate security clearances for all Contractor personnel and all sub-contractor personnel based upon the required security level for the work that each person will be performing within the specified timeframe. The Contractor shall take expedient actions regarding job changes, especially job terminations, including arranging knowledge transfer, reassigning responsibilities, and removing access rights.

3.3.22 Service Level Monitoring: The Contractor shall manage, monitor, measure and report on the ongoing service delivery and performance management across all services provided to Government end-users. Reports shall provide performance analysis and assessment of each individual IT Service Area's (defined in Section Table 1.3.3) performance achievements against contractual SLAs.

The Contractor shall generate and provide reports on system management information (e.g., performance metrics, system accounting information, etc.) on a monthly basis to the designated Government representatives in a format approved by the Government.

The Contractor shall cooperate and coordinate with the Government in managing, configuring, maintaining, and updating electronic reporting system tools to provide real-time, near real-time, snapshot, and historical reporting of IT service performance and progress information related to IT service level achievement objectives. Reporting capabilities shall be segmented by various Government management viewpoints and presented as a "dashboard" and "scorecard" which include:

a) Government command management view
b) Component management view
c) IT service management view
d) IT service operations view

The Contractor shall review the set of IT performance tools currently in use by the Government and identify any gaps in capability to fulfill the requisite monitoring, modeling, measurement, management, analysis, and reporting requirements. The Contractor shall document and report their recommendations to the Government, which shall include potential alternative courses of action to resolve the gaps. The Contractor shall provide general health of environments reports (e.g., system performance response times and trend lines, patches not yet applied) as well as reports that represent demand fulfillment.
CDRL A009 – Operational Reporting

3.3.23 Incident Management: The Contractor shall perform the following IT incident management activities and tasks in to restore normal service operation as quickly as possible in order to minimize any adverse impacts to customers, thus ensuring maintenance of the best possible enterprise-wide levels of service quality and availability.
The Contractor shall respond to and closely coordinate incident resolution and ongoing resolution status of all support requests escalated to the Contractor by the government, customer, and NNHD.

The Contractor shall establish criteria for Incident Management support requirements, including equipment and services to be covered, Priority-levels, definitions and characteristics, incident classification and prioritization schema, escalation requirements, communication requirements with Government IT personnel and end-users, etc. The Contractor shall ensure incident resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual. The Contractor shall accurately record, update, and close Incident Management system records and capturing the resolution actions and knowledge in the NNHD's IT knowledge management database. The Contractor shall provide unrestricted read access by the Government- authorized staff and other Government and third-party personnel to all current and historical Contractor- maintained Incident records and knowledgebase data and read/write access for a limited number of Government- authorized personnel. The Contractor shall monitor all Government IT systems for automatically generated and/or logged Incident alerts and events.
CDRL A020 – Incident/Problem Management Report

3.3.24 Problem Management: The Contractor shall perform the problem management lifecycle activities associated to identify and resolve the underlying root cause of an IT problem. The Contractor shall perform Root Cause Analysis (RCA) for analyzing and determining the underlying cause or event that generated or created one or more incidents, identify appropriate problem resolution and provide recommendations to prevent recurrence of the problem.
The Contractor shall coordinate problem management activities with the Incident Management, Change Management, and Release Management processes. The Contractor shall minimize the adverse impact of incidents and problems to the Government's mission caused by errors within the Government's IT

environment, application or service delivery environment and shall perform the following Problem Management processes:

a) Problem detection
b) Problem logging
c) Problem categorization
d) Problem prioritization
e) Problem investigation and diagnosis
f) Workarounds
g) Raising known error records
h) Problem resolution
i) Problem closure
j) Performing major problem review

3.3.25 Monitoring and Reporting Services: The Contractor shall develop requirements and policies (in draft format for Government consideration) for IT monitoring and problem management. The Contractor shall implement measures that provide proactive monitoring and self- healing capabilities to limit server and storage outages. The Contractor shall identify server and storage problems and resolve in accordance with Incident and Problem Management Services, policies and procedures. The Contractor shall coordinate resolution of server and storage problems with third party IT service providers (e.g., NMCI, or NGEN), other governmental entities, and non-governmental entities having access and/or providing connectivity to the IT resources.

3.3.26 Technology Performance Management Services: The Contractor shall recommend and adhere to Government approved policies, procedures, measurement, and evaluation practices and monitoring and reporting requirements for managing the enterprise-wide IT server and storage infrastructure and software to obtain optimal performance. The Contractor shall perform all technology performance management tasks and activities in cooperation, collaboration, and coordination with all other IT service providers to ensure ongoing compliance with all performance management optimization requirements and objectives.

3.3.26.1 The Contractor shall perform Service Area component tuning to maintain optimum performance in accordance with Change Management, Release Management, and Configuration Management procedures. The Contractor shall provide regular monitoring and reporting of Service Area component performance, utilization, and efficiency. The Contractor shall perform trending studies and analyses on various IT parameters (e.g., usage patterns, incident/problem event correlations, operations efficiency, etc.) to identify potential problem areas and provide reports on recommendations. The Contractor shall provide technical advice and support to the application maintenance and development staffs as required.
CDRL A009 – Operational Reporting

3.3.27 Environment and Facilities: The Contractor shall coordinate all facilities-related work in coordination with the Government and any applicable base-level facilities management requirements, as well as, in coordination and collaboration with on-site facility management personnel and all other affected IT service providers. This shall include but is not limited to LAN cabling infrastructure and coding requirements, component identification marking systems, equipment racks, and rack layout. Heating, Ventilation, and Air Conditioning (HVAC), power, Uninterruptable Power System (UPS), IT security systems, fire suppression system, and environmental issues related to the Data Center or network communications equipment spaces will be addressed via close coordination and collaboration with existing facility management personnel.
CDRL A017 – Requirements, Function/Technical Design, and Architecture Documentation

3.3.28 Information Assurance (IA) Coordination: The Contractor shall implement and adhere to all Government IA policies, procedures, and documentation pertaining to IT server and storage computing systems and services for which it has management responsibility. The Contractor shall work with the Government IA Division to ensure that appropriate IA controls and reporting are in place for all facets of its IT Service Areas. The Contractor shall monitor the work performed by all of the Contractor personnel to ensure that they comply with, and have incorporated all, appropriate IA requirements and implemented all

required safeguards for securing and managing Government IT computing systems and related IT infrastructure environments.

The Contractor shall ensure all IT elements within any environment comply with the following IA guidelines:

a) Incorporate security as part of the design
b) Assume a hostile environment
c) Use open standards as much as possible
d) Minimize and protect trusted system elements
e) Protect data at the source (i.e., in process, transit, and storage)
f) Limit access to need-to-know
g) Authenticate
h) Do not subvert in-place security protections
i) Fail securely
j) Log, monitor, and audit

The Contractor shall monitor and verify that all server and storage systems and associated hardware and software components are tested and deployed within the Government's environment in compliance with all appropriate IA requirements. The Contractor shall ensure incorporation of IA management processes within each of the following processes for all IT hardware and software elements introduced into the Government's IT environment:

a) System or service design
b) System or service build/development
c) System or service testing
d) System or service implementing
e) System or service updating
f) System or service managing
g) System or service maintaining

The Contractor shall provide all server and storage IA management information (e.g., system vulnerabilities, security incidents, and intrusion detection) in accordance with IA reporting policies and shall be correctly documented and reported to designated Government representatives in accordance with IA reporting requirements and in a format approved by the Government.

The contractor shall have an organic understanding of FedRAMP/DoD Impact Level (IL) implications, and how IL 4/5 rules may impact design and cost. The Contractor shall assist with outlining cloud environment continuous monitoring strategy. The Contractor shall educate and develop an organic understanding of the cloud first policy, and how to best utilize that to the Government's advantage, to reduce time to Approval To Operate (ATO). Interaction with Navy Cyber Defense Operations Command (NCDOC) to understand their requirements regarding sensor data and feeds from Intrusion Detection Service/Intrusion Protection Service (IDS/IPS), web application firewall (WAF), firewalls, etc. is required.

3.3.29 General Information Assurance Services: The Contractor shall perform General Information Assurance Services in conformance with Government regulations and IA policies and standards. The Contractor shall implement and adhere to all Government IA policies (DIACAP and Risk Management Framework (RMF)), procedures and documentation pertaining to IT server and storage computing systems and services for which it has management responsibility. The Contractor shall monitor and verify that all server and storage systems and associated hardware and software components are tested and deployed within the Government's environment in compliance with all appropriate DoD/DON IA requirements. The Contractor shall provide all server and storage IA management information (e.g., system vulnerabilities, security incidents, and intrusion detection) in accordance with IA reporting policies and shall provide results to designated Government representatives. The Contractor shall provide technical expertise in the support of the assessment and authorization (A&A) activities for all Data Center and Cloud IT infrastructure elements to ensure accurate, complete and timely performance of all activities associated with RMF and continuous monitoring. The Contractor shall consult with AD 7.2 team members, including those assigned collateral IA duties, to ensure their use of enterprise hosting systems and assets is conducted

in accordance with governing IA program policies, processes, and requirements. The Contractor shall ensure Assured Compliance Assessment Solution (ACAS) benchmarks and scans, Security Technical Information Guides (STIGs) and Checklists, DISA Security Compliance Checker (SCC) Security Content Automation Protocol (SCAP) Scanning Utilities and all A&A artifacts are provided at the agreed upon schedule. The Contractor shall utilize analytical findings to identify appropriate and operationally effective security countermeasures, and to resolve existing or potential IA security problems. The Contractor shall write supporting mitigation statements. The Contractor shall ensure security metrics for the operating systems and supporting services meet the 'passing requirements' for Command Cyber Security Readiness Inspections.
CDRL A021 – System Defense and Anomaly Report

3.3.30 Intrusion Detection Services (IDS): The Contractor shall operate and maintain Intrusion Detection and Prevention Services (IDS/IPS) in conformance with Government regulations and IA policies and standards.
The Contractor shall Provide Host-based Intrusion Detection and Prevention Services (HIDS/IPS & HIPS) and reporting for managed systems and devices. The Contractor shall allow for third party IDS (e.g., Inspector General (IG), Defense Information Systems Agency (DISA), DOD, or other contracted services. The Contractor shall develop, document, and provide recommendations for improvement in IT security.

3.3.31 Security Compliance and Management Services: The Contractor shall perform IT security compliance and management services in conformance with Government regulations and IA policies and standards.
The Contractor shall ensure compliance with all established Government and other governmental entities (e.g., DISA, DOD, etc.) regulations and systems and software development guidelines and policies at all times. The Contractor shall adhere to all applicable policies and procedures concerning the destruction of classified and sensitive but unclassified information. The Contractor shall establish and maintain an Information Security Plan in accordance with then-current National Institute of Standards and Technology (NIST) Special Publication 800-18R1 to respond to, analyze, and mitigate both internal and external threats to the Government's high value assets, as part of the C&A process. Include in the security plan: logical access controls, access control monitoring including firewall and IDS/IPS monitoring and response plan, assurances, operational practices, and training processes.

3.3.32 Critical Incident Response: The Contractor shall support the incident response process for critical incidents (extraordinary events) as explained below.
Critical incidents are those incidents that have moderate to significant impact to operations and pose a significant threat to DoD data or service delivery such as major malware incidents, TOP SECRET and above level spillages, and response to repair services after an environmental event, such as fire or severe water damage impacting numerous services. Invocation of the IT/CS Data Center Contingency Plan that requires support outside core business would be categorized under this section. Thus, if a critical incident materializes during the normal operating day resource prioritization shall be utilized to support the response activity. Critical incident response activities occur outside of core hours. Critical incident response events have clearly defined project begin and project end criteria. Critical incidents are not considered a part of the daily routine and may require significant engineering and recovery support that is difficult to forecast based on today's operating environment and threat landscape. Activities shall be documented in the monthly status report.
CDRL A001 – Monthly Status Report

3.3.33 Status Reporting: The Contractor shall provide a monthly status report to summarize accomplishments during the reporting period and clearly demonstrates that the Performance Requirements Summary (PRS) objectives were satisfied for the reporting period. The report shall also include planned vs. actual task completion to include any milestones, anticipated activity (including anticipated CDRL deliveries) for the next reporting period, lessons learned, risks, outstanding issues and recommendations. The Contractor shall provide monthly financial/resource reporting by CLIN and/or Sub-CLIN as follows:
1. Cost Reimbursable CLINs: The Contractor shall provide information to include, but not limited to cost details (i.e., Traveler's Name(s), Dates of Travel, Destination, & Purpose for travel;

2. Item/Name, Description, Unit Cost, Number of Units, & Extended Costs for ODC's/Material, etc.), financial status of cost CLINs/SLINs (i.e., funding applied, expenses incurred during current reporting period, total expenses to date, amount remaining, etc.) and forecast of funds depletion by CLIN/SLIN type based on known requirements.

3. Cost Plus Fixed Fee CLINs: The Contractor shall provide information to include, but not limited to cost details (i.e., Employee Name, Labor Category, Rate, Current and Cumulative Hours & Costs etc.), financial status of cost CLINs/SLINs (i.e., funding applied, expenses incurred during current reporting period, total expenses to date, amount remaining, etc.) and forecast of funds depletion by CLIN/SLIN type based on known requirements.

4. Status and financial reporting will be in accordance with each CLIN/SLIN.

CDRL A001 – Monthly Status Report

3.4 Labor Category Definition: Standard labor category definitions can be found in the base General Services Administration Alliant/Alliant 2 GWAC contract. Additionally, SECNAV M-5239.2 establishes mandatory procedures for the uniform identification, management, and qualification of the Cyberspace IT/Cybersecurity Workforce (Cyber IT/CSWF). All Cyber IT/CSWF personnel must meet and maintain the minimum qualification standards of their assigned Specialty Area and proficiency level.

Labor Categories; Security Clearance/Certification Requirements Table:

Labor Categories	**Security Requirement**	**Certification Requirement**
Senior Computer and Information Research Scientist	Requires personnel to have a favorably adjudicated Secret clearance	
Senior Computer and Information Research Scientist	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Junior Computer Hardware Engineer	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Journeyman Computer Hardware Engineer	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
*Senior Computer Hardware Engineer (Key Position)	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved

Journeyman Computer Network Support Specialist	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Senior Computer Network Support Specialist	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Journey Computer Operator	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Senior Computer Operator	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Senior Computer Programmer	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
SME-Computer Systems Analyst	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
*Senior Computer Systems Engineer/Architect (Key Position)	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
SME-Computer Systems Engineer	Requires personnel to have a favorably adjudicated SSBI with Secret clearance	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved

	Top Secret Clearance is required for Critical Incidents as required by the Government	
Journeyman Computer User Support Specialist	Requires personnel to have a favorably adjudicated Secret clearance	
Junior Information Security Analyst	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Junior Information Security Analyst	Requires personnel to have a favorably adjudicated Secret clearance	
Journeyman Information Security Analyst	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Journeyman Information Security Analyst	Requires personnel to have a favorably adjudicated Secret clearance	
Senior Information Security Analyst	Requires personnel to have a favorably adjudicated Secret clearance	
Senior Information Security Analyst	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Senior Information Technology Project Manager	Requires personnel to have a favorably adjudicated Secret clearance	
*SME-Information Technology Project Manager (Key Position)	Requires personnel to have a favorably adjudicated Secret clearance	
Junior Management Analyst	Requires personnel to have a favorably adjudicated Secret clearance	
Journeyman Management Analyst	Requires personnel to have a favorably adjudicated Secret clearance	

Senior Management Analyst	Requires personnel to have a favorably adjudicated Secret clearance	
Senior Management Analyst	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
*SME-Management Analyst (Key Position)	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
SME-Management Analyst	Requires personnel to have a favorably adjudicated Secret clearance	
Junior Network and Computer Systems Admin	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
Journeyman Network and Computer System Admin	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
*Senior Network and Computer System Admin (Key Position)	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved
*SME-Network and Computer Systems Admin (Key Position)	Requires personnel to have a favorably adjudicated SSBI with Secret clearance Top Secret Clearance is required for Critical Incidents as required by the Government	Requirement for privileged access includes: One of the following IA certifications: CCNA Security, CySA+ **, GICSP, GSEC, Security+ CE, SSCPAND an OS/CE Certification/Qualification Achieved

*** Denotes Key labor category**

A022 – Compliance Report