Section C - Description/Specifications/Statement of Work

STATEMENT OF WORK

FOR

DIGITAL INFORMATION TECHNOLOGY ANALYSIS AND CYBER (DITAC) NETWORK INFRASTRUCTURE

NAVAL AIR WARFARE CENTER WEAPONS DIVISION (NAWCWD), CHINA LAKE

20 July 2021

DISTRIBUTION STATEMENT D. Distribution authorized to Department of Defense and U.S. DoD contractors only Administrative or Operational (25 August 2021). Other requests for this document shall be referred to the Naval Air Warfare Center, Weapons Division, Code DC30000, China Lake, CA 93555.

1.0 INTRODUCTION

The contractor shall provide all personnel necessary to perform the task defined in the Statement of Work (SOW).

1.1 Background

The Digital Information Technology Analysis and Cyber (DITAC) Department at the Naval Air Warfare Center Weapons Division (NAWCWD) provides facilities and laboratories with a broad spectrum of technology, capabilities, and innovative system interoperability and integration requirements with both the internal and external supports necessary to ensure an efficient and effective operating environment to meet its goals and objectives for all customers at NAWCWD. DITAC manages and operates the NAWCWD networks and computer systems providing base-wide connectivity to access Department of Defense (DoD) networks, facilities, laboratories, and ranges. DITAC provides monitoring, operations and maintenance, upgrades, and overall management for network infrastructure and planning.

The DITAC Network Infrastructure serves as a NAWCWD resource for Information Technology (IT), System Administration (SA), and Cyber Security support; and maintains expertise in DoD, Department of Navy (DoN), and subordinate command IT policy and procedures to leverage best practices for its customer base. The DITAC Network Infrastructure is composed of diverse service capabilities with the mission to provide superior customer service and to support the organizations and Product Teams at NAWCWD.

1.2 Scope

This SOW defines the services and materials required for the analysis, design, development, test, integration, deployment, and operation of IT systems and services. This effort shall meet the DITAC Department customers' needs with value added, cost effective IT, and Cyber Security solutions, with an overarching goal of maintaining a secure network.

The geographic scope of this effort includes NAWCWD China Lake, Point Mugu, Port Hueneme, San Diego North Island, San Nicholas Island; Tucson, Arizona; and Northridge, California. Contractors may be required to deploy into the field at multiple customer locations within the NAWCWD areas: China Lake (a 1.1-million-acre installation) and Point Mugu. Travel within the geographic scope for occasional efforts may be necessary to support the IT infrastructure. Contractors may be required to travel to other DoD sites in support of national enterprise architecture requirements/activities.

2.0 APPLICABLE DOCUMENTS

The following documents are applicable to this SOW to the extent specified herein. Throughout the life of the contract, the most current instruction or document shall be applicable to these requirements. The Government will provide all necessary reference documents and those not generally available to the contractor. It is the contractor's responsibility to notify the Government if it does not have access to one or more of the listed documents, and that it is the most current.

The contractor shall not purchase any IT equipment on behalf of NAVAIR in support of this contract, which reports to Program Budget Information System – Information Technology (PBIS-IT), without a NAVAIR Chief Information Officer (CIO) approved Navy Information Technology Approval System (NAV-ITAS) Information Technology Procurement Request (ITPR).

2.1 Information Technology Information.

2.1.1 Clinger-Cohen Act.

The contractor shall conduct analysis of program/project needs, acquisition strategy, and program artifacts to identify and capture specific factors required to satisfy the eleven (11) elements of Clinger-Cohen Act (CCA) compliance listed in DoDI 5000.02, Enclosure 1, Table 9. Using Microsoft Word, the contractor shall prepare a CCA compliance matrix following the organization and appearance of Table 11 with additional separate columns for the display of artifact: titles, date(s) of approval, page number(s), and paragraph or section number(s). The right-hand column shall include an embedded object permitting the reader to open unclassified artifacts. The column shall identify classified artifacts and shall describe approved channels for access of classified artifacts. The contractor shall support the DC30000 Program Manager (PM) during CCA compliance review and assist in responding to reviewer comments if and when additional supporting information or revisions are required.

Updating approved CCA compliance packages: For updates of approved CCA compliance packages, the contractor shall conduct analysis of program/project needs, acquisition strategy, and program artifacts to identify and determine if each of the Eleven (11) elements of CCA has changed; if no change has occurred, a notation

stating “no change” shall be entered in the CCA compliance matrix. If changes have been found, the contractor shall update the CCA compliance matrix to reflect the changes. The contractor shall support the DC30000 PM during CCA compliance review and assist in responding to reviewer comments if and when additional supporting information or revisions are required.

2.1.2 System Software/Application Compliance.

All IT systems or software/application development, modification, or support shall be performed in accordance with Defense Business Transformation guidance (formerly Business Management Modernization Program (BMMP)), Department of the Navy (DoN)/NAVAIR Functional Area Manager (FAM) Policies and Guidance, Network and Server Registrations, and Web Enablement mandates.

2.1.3 Websites, Web Enablement, and Application/System Development, Modification, and Maintenance Support Services.

All IT systems, software, and website development, modification or support shall be performed in accordance with all applicable Federal, DoD, DoN, and NAVAIR policy, guidance, standards, and strategies, and should be integrated within the NAVAIR Enterprise portal and collaboration environment whenever possible. Any websites or servers hosted/located in contractor facilities, or outside the NAVAIR enclave, will transition to NAVAIR architecture and infrastructure in accordance with legacy shutdown guidance. Policies include, but are not limited to:

a. Office of Management and Budget Management of Federal Information Resources, OMB CIRCULAR NO. A-130 Revised. <http://www.whitehouse.gov/omb/circulars_a130_a130trans4>

b. OMB Policies for Federal Agency Public Websites, OMB M-05-04 <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-04.pdf>

c. Section 508 Amendments to the Rehabilitation Act of 1973. <http://www.section508.gov/Section-508-Of-The-Rehabilitation-Act>

d. Department of Defense Web Policies and Guidelines. <http://www.defense.gov/webmasters>

e. Navy Information Operations Command (NIOC) Norfolk Web Risk Assessment Team Website. .public.navy.mil/fcc-c10f/niocnorfolk/Pages/AboutWRA.aspx>

f. DON Policy for Content of Publicly Accessible World Wide Web Sites SECNAVINST 5720.47B..navy.mil/navydata/internet/secnav5720-47b.pdf>

g. NAVAIR CIO Website (NAVAIR specific policy and guidelines). To request this policy contact the NAVAIR CIO office – 7.2.2 Applications Integration team – Web Manager: Shane Malamphy at 301- 342-1825.

h. Defense Information Systems Agency (DISA) Hosting of All Navy Websites (NAVADMIN 061/08).npc/reference/messages/Documents/NAVADMINS/NAV2008/NAV08061.txt>

i. Consolidation of Navy Web Sites - Reduction of IM/IT Footprint NAVADMIN 145/07. ttp://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2007/NAV07145.txt>

j. DON Web Presence Policy: The Registration, Compliance of, and Investment in, All Unclassified Web Sites and Uniform Resource Locators. .doncio.navy.mil/ContentView.aspx?ID=577>

k. Policy and Procedures for Web Risk Assessment (WRA) of Publicly Accessible Navy Sites (ALCOM 129/09).

2.1.4 Software Development/Server Procurement.

Any tools developed that will be hosted by the Navy Marine Corps Intranet (NMCI) or run on NMCI workstations will be certified for NMCI and comply with NMCI policy. Additionally, any servers supporting this effort will be transitioned to meet the requirements of the current NAVAIR Server Consolidation effort. All tools or servers developed by DITAC will be in compliance with Navy consolidation efforts.

2.1.5 Reserved.

2.1.6 Enterprise Architecture.

Contractor networks and connections– Contractor-owned and operated networks are prohibited on any NAVAIR facility or site in support of this contract. The contractor may access non-Government external Internet Protocol (IP) space via the NAVAIR-provided Virtual Private Network (VPN) Outreach service or NAVAIR CIO-approved IP service.

Architecture compliance– The contractor shall ensure all IT solutions, including database solutions, comply with the appropriate NAVAIR Enterprise Architect (NAE) Enterprise Architecture and are verified by the NAE prior to build out.

Disclosure of pre-existing networks, circuits, or connections– Any and all networks, circuits, or connections between the contractor and any NAVAIR site related to previous contracts shall be identified in the Memorandum of Agreement (MOA). Failure to comply and subsequent discovery of an unregistered network, circuit, or connection shall be grounds for immediate disconnection.

2.1.7 Cybersecurity.

The contractor shall conduct investigation and analysis of acquisition program artifacts, such as Initial Capabilities Document (ICD), Capability Description Document (CDD), Capability Production Document (CPD), Navy urgent operational need (UON) and Marine Corps urgent universal need statement (UUNS), joint urgent

operational needs (JUONs), threat assessments, and acquisition strategies (AS). Knowledge gained from this analysis shall be used when developing the Cybersecurity Strategy (CS) needed to steer and inform the program's development of a Security Plan (SP) in accordance with DoDI 8510.01, of 12 March 2014.

At a minimum, hardware, firmware, software, documentation (data deliverables) and/or IT services delivered by this contract shall be in compliance with the latest versions of the following references:

a. DoDI 8500.01, Cybersecurity, incorporating Change 1, dated 7 October 2019

b. DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), dated 12 March 2014, incorporating Change 3,2 dated 29 Dec 2020

c. Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, dated 27 March 2014

d. DoDD 8140.01, Cyberspace Workforce Management, Reissue, 5 Oct 2020

e. DoD 8570.01-M, Information Assurance Workforce Improvement Program, dated 15 August 2004, incorporating Change 4, dated 10 November 2015

The contractor shall conduct investigations and perform analysis, including criticality analysis, threat assessments, and vulnerability assessments. All findings and recommendations shall be reported to the Government in technical reviews and submitted as written reports or documents as listed in CDRLs. The contractor shall support Government efforts needed for information systems (IS) (enclaves or major applications), Platform Information Technology (PIT), or PIT systems to successfully categorize the system, select, implement, and test security controls, and receive an Authorization to Operate (ATO) before use or interconnection in an operating environment in accordance with references (a), (b), and (c). This includes IT that is standalone and IT that is connected to other systems, networks, or enclaves. IS enclaves or major applications, PIT, or PIT systems delivered prior to award of this contract but included in the performance of this contract may have been delivered in compliance with Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) and as such shall require transition to RMF cybersecurity compliance. Transition planning proposed or performed under this contract shall be in compliance with reference (b), Enclosure 8, Figure 2, and all hardware, firmware, and software deliverables shall be capable of receiving an ATO in accordance with reference (b).

Information technology services shall only be performed by personnel who are qualified and certified in accordance with reference (d). Personnel proposed and/or used in the performance of this contract as certified personnel shall be limited to those whose specifically assigned duties and responsibilities require certification. Continuous education must be maintained in accordance with reference (e).

All IT procured on behalf of this contract shall meet all DoD, DoN, and NAVAIR cybersecurity polices. Failure to follow these policies will result in denial of access to NMCI, One Net, Integrated Shipboard Network System (ISNS), and other DoN, DoD, and Joint networks. These cybersecurity policies are standard across the Department and ensure cybersecurity compatibility and interoperability.

IT systems and or networks operated by contractors pursuant to a NAVAIR contract, regardless of the level of data processed, shall be operated in accordance with the NISPOM.

Approved contractor-owned equipment shall be permitted connections to NAVAIR/DoD networks in order to carry out the performance of this contract. All contractor-owned hardware and/or software shall meet DoDI 8500.01, Cybersecurity, is subject to validation scanning and must be approved by the NAVAIR site Cybersecurity Manager prior to connection.

The following specific criteria must be met before the contractor can be connected to any DoD or NAVAIR network in support of this contract. Requirements include:

a. Network Vulnerability Scanning. NAVAIR Deputy CIO for Information Assurance maintains authorized auditing tools and shall provide for firewall/port scans, device discovery scan, vulnerability assessment, and other requirements as required to ensure secure interoperability with DoD networks. The contractor shall be responsible for the remediation of any equipment that fails these audits prior to the connection of the system to the networks. Results of approvals shall be documented via Memorandum of Agreement with the Facility Security officer and the Defense Security Service Representative for that contractor.

b. Extent of Validation Scanning. To prevent scanning of corporate assets, all such networks, equipment, and connections shall be physically segregated from any Government/contractor corporate networks that are not in direct support of DoD contracts.

c. Circuit Provisioning. Any circuit or connection between NAVAIR and/or DoD site and the contractor site shall be provisioned via the Defense Information Security Agency and comply with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D, Defense Information System Network (DISN): Policy and Responsibilities, 24 Jan 2012.

d. Servicing Systems from a Remote Contractor Site. Remote Access Service connections that allow off-station operation and/or administration of contractor owned systems, located at any NAVAIR facility or site, shall not be permitted, with the exception of those systems connecting to the Command via the Outreach Services identified in Section 2.3.6, Enterprise Architecture, of this SOW.

e. Memorandum of Agreement and Inter-connection Agreements. A Cybersecurity Memorandum of Agreement (MOA) between the contractor owning the equipment and AIR-7.2.6 shall be developed and signed before the equipment can be connected to NAVAIR networks. Failure to comply with the signed MOA shall be grounds for disconnection from the network.

2.1.7.1 Security Plan.

The contractor shall investigate and conduct analysis in order to provide technical reviews to make a recommendation with data supporting the development of the Security Plan. Contractor performed analysis shall include criticality analysis, threat assessment, and vulnerability assessments. The Security Plan shall be prepared for the first program/project decision point and updated for each subsequent decision point. The proposal shall include all technical data required to engage in collaboration with the security control assessor and the authorizing official (staff). In the event the collaboration results in redesign or follow-up action after collaboration requiring additional or revised documentation, the contractor shall continue to assist the collaboration process.

All Cybersecurity shall be in compliance with the following listed instructions:

a. DoDI 8582.01, Security Of Unclassified DoD Information On Non-DoD Information Systems, 06 May 2012, incorporating Change 3, 9 Dec 2019.

b. CJCSI 3170.01I (series), Joint Capabilities Integration and Development System (JCIDS), 23 Jan 2015.

c. CJCSI 6211.02D, DISN: Policy and Responsibilities, 24 Jan 2012 (Current as of 04 Aug 2015).

d. CJCSI 6251.01D, Narrowband Satellite Communications Requirements, 30 Nov 2012.

e. CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 09 Feb 2011, certified current 09 Jun 2015.

f. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Cyber Incident Handling Program, 10 July 2012 (Current as of 18 Dec 2014).

g. Navy Ports Protocols, and Services (NPPS) Manual, Version 1.5, 16 Nov 2010.

h. Defense Acquisition Guidebook – Chapter 7, Acquiring Information Technology, Including National Security Systems, Section 7.5, IA.

i. DoD 5220.22-M,National Industrial Security Program Operating Manual, 28 Feb 2006 (NISPOM) Incorporating Change 2, 18 May 2016.

j. DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 Dec 2005, incorporating Change 3, dated 24 Jan 2012.

k. DoDD 8000.01, Management of the Department of Defense Information Enterprise, 17 March 2016.

l. DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004, Certified Current, 23 April 2007.

m. DoDD 8140.01, Cyberspace Workforce Management, 11 Aug 2015, Certified Current, 5 Oct 2020.

n. DoDI 8330.01, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 21 May 2014, incorporating Change 2, 11 Dec 2019.

o. DoDI 8500.01,Cybersecurity, 14 March 2014, incorporating Change 1, 7 Oct 2019.

p. DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011.

q. DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), 28 May 2014, incorporating Change 1, 27 Jul 2017.

r. DoDI 8580.1, IA in the Defense Acquisition System, 09 July 2004.

s. DoDI 8581.01, IA Policy for Space Systems Used by the Department of Defense, 08 June 2010.

t. DON CIO Memo 02-10, Department of the Navy Chief Information Officer Memorandum 02-10 Information Assurance Policy Update for Platform Information Technology, 26 April 2010.

u. DON letter 5239NAVAIR 726/2322 of 18 Feb 09, NAVAIR Data at Rest Policy.

v. Federal Information Processing Standards Publications (FIPS PUB)-199, Feb 2004.

w. Committee on National Security Systems Policy (CNSSP) No.11, 10 June 2013.

x. Office of the Chief of Naval Operations Instruction (OPNAVINST) 5239.1C, Navy IA Program, 20 Aug 2008.

y. SECNAV M-5239.1,Department of the Navy Information Assurance Program; Information Assurance Manual, Nov 2005.

z. SECNAVINST 5230.15, Information Management/Information Technology Policy for Fielding of Commercial Off the Shelf Software, 10 April 2009.

aa. SECNAVINST 5239.3C,Department of the Navy Cybersecurity Policy, 02 May 2016.

bb. SECNAVINST 5239.19, Department of the Navy Computer Network Incident Response and Reporting Requirements, 18 March 2008.

cc. The National Security Act of 1947.

dd. Title40/Clinger-Cohen Act.

ee. Title44/ Federal Information Security Management Act.

ff. National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013 (Updated 22 Jan 2015).

2.2 Government Documents

The following Government Documents are referenced for information and contractor guidance:

a. National Industrial Security Program Operating Manual (NISPOM)

b. Rules of the Road, A Guide for Leading Successful Integrated Product Teams, Revision 1, October 1999

c. DoD Office of General Counsel, Ethics Issues in Government-Contractor Teambuilding, 15 July 1999

d. DoDM 5200.01, Information Security Program Manual (Volume 4)

e. DoDD 5205.02E, National Security Decision Directive 298

f. OPNAVINST 3432.1A, Operations Security

3.0 REQUIREMENTS

The contractor shall ensure all personnel understand and follow statutory and regulatory restrictions and standards of conduct issues faced when close working relationships, such as Integrated Product Teams (IPTs), are required. All team members shall have the authority, knowledge, and expertise to participate in problem solving and decision-making (except for Government functions normally referred to as inherently Governmental, such as the act of governing, i.e., the discretionary exercise of Government authority, and monetary transactions and entitlements), and the implementation of team decisions.

The contractor shall utilize the current work request tracking system and the current IT/Customer Service (CS) billing system to obtain requirements of DITAC customers. Access to the system will be provided through Government resources. The Government Technical Point of Contact (TPOC), Security team, or Lab Manager will estimate applicable labor hours and identify changes in priorities to the daily customer requirements, needs, or projects in an e-mail, database, or a daily meeting which require the contractor to perform tasking as stated within the SOW and defined by any DoD directives.

The contractor shall provide qualified personnel who possess the training, qualifications, experience, equipment, clearances, and certifications to meet the requirements of this SOW. These qualifications include the ability to verify and validate the solution sets and protocols while assisting the user with all aspects of IT acquisition. All required certifications and training shall be obtained by the contractor employee within 60 days of assignment. Contractor employees shall remain current in their functional areas of expertise and evolving technologies as well as maintaining certifications and training throughout the task order. The contractor shall have working knowledge of BICSI and TIA/EIA Industry Standards.

3.1 System Administration in compliance with Information Assurance/Security

3.1.1 The contractor shall perform tasks to support all aspects of the DITAC Department, such as database and application administration; integration support; workstation management of hardware repair, upgrades, and/or enhancements; software license management upgrades and/or enhancements; requirements analysis; identifying and improving technical solutions; securing and managing operating systems; validating backups; on-site and remote troubleshooting and repair; CND; identification of cyber security threats to include remediation of identified vulnerabilities and risk mitigation; and technical advice and assistance.

3.1.2 The contractor shall perform operational support, including backups, system tuning, file conversions, information handling, data entry, and data management.

3.1.3 The contractor shall analyze systems security log files, monitor system firewall log files, and take appropriate information security action should an intrusion or threat be detected. The contractor shall respond to Information Assurance Vulnerability Alert (IAVA) or Information Assurance Vulnerability Bulletin (IAVB) and report back to the Information Security Division through the internal DC3 Code Information System Security Officer (ISSO) task-team leaders. The contractor shall perform vulnerability scanning and harden systems to meet DoD requirements to meet accreditation standards in accordance with Risk Management Framework. The contractor shall perform and complete technical network diagrams depicting network and computer components and their appropriate security controls, hardware lists, software lists, and user lists that are required to maintain and create accreditation boundaries.

3.1.4 The contractor shall analyze and document information assurance compliance strategies for specific D/EC3 Infrastructure customers and determine their IA maturity and security posture, compared to NAWCWD and DoD/ DoN standards. The contractor shall provide Cyber Security recommendations based on Cyber Security policies and procedures outlined in the DoDI 8510.01. The contractor shall provide the required documentation for Government approval to complete the certification and accreditation process in accordance with the DIACAP, Risk Management Framework (RMF), or the subsequent processes as defined by the DoD 8510 series of instructions.

3.1.5 The contractor shall ensure physical security requirements are met and maintained, including open storage certifications, TEMPEST access control systems, combination locks, and keycard systems. The contractor shall ensure cyber threat avoidance, Defensive Cyber Operations (DCO), and perform threat assessments. This requirement shall include integrating innovative cyber technologies to enable cyber superiority and the facilitation of technology transition.

3.1.6 The contractor shall ensure Communications Security (COMSEC) requirements are met for the handling, storage, and operations of COMSEC hardware and material in accordance with Electronic Key Management System (EKMS)-1.

3.1.7 The contractor shall assist the Government by providing recommendations to mitigate and remediate risk while balancing customer functional requirements. The contractor shall submit all required supporting and risk assessment documentation through the use of Enterprise Mission Assurance Support Service (eMASS) prior to the deadlines determined by the D/EC3 Command Information System Security Managers (CISSMs). The contractor is notified of deadlines during biweekly meetings.

3.1.8 The contractor shall perform Information Assurance Vulnerability Management (IAVM), Information Assurance (IA), and cyber security compliance support by responding to vulnerability notifications which require action, tracking compliance, and reporting to DITAC customers and performing compliance checks.

3.1.9 The contractor shall protect unclassified, sensitive, and classified information. The contractor shall develop and assist, submit and maintain Certification and

Accreditation (C&A) documentation in accordance with National Institute of Standards and Technology (NIST) 800 series. The contractor shall ensure all IT resources procured, installed, and maintained in support of this SOW meet security requirements while maintaining the most current versions of approved host based security tools. The contractor shall interface with individual lab managers for adherence to security requirements and compliancy. The contractor shall respond to vulnerability notifications that require action, track compliance and reporting, and perform compliance checks as directed by the CISSMs and ISSOs responsible for the accreditation boundaries.

3.1.10 The contractor shall provide Information Assurance/Security/System Administration services in accordance with the following criteria:

a. Allocate sufficient resources to adequately protect organizational information systems.

b. Ensure the program development, implementation, and maintenance of IT security performance measures.

c. Employ system development life cycle processes that incorporate information security considerations.

d. Employ software usage and installation restrictions.

e. Ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

f. Provide pre-operation setup, power-up, diagnostics, interfaces, and all system checks shall be set up, fully tested, and operationally ready.

3.2 Network Security

3.2.1 The contractor shall provide recommendations, including creation of metrics and dashboard aids; development of scripting to support automation of CND functions; and development and presentation of status and progress briefings to persons responsible for the accreditation boundaries security on Security Technical Implementation Guide (STIG) and Computer Tasking Order (CTO) development, implementation, and reporting on the results of vulnerability scanning and remediation actions per DoDD 5000.01, The Defense Acquisition System. The contractor shall follow the approval of recommendations and implement approved recommendations. The contractor shall conduct status and progress reporting via Government scheduled briefings.

3.2.2 The contractor shall analyze and provide recommendations for the update and sustainment of the cyber readiness of the systems and processes providing CND services, and incorporate CND best practices into planned recommendations for workflow and process improvement.

3.2.3 The contractor shall assist the Government in preparing and sustaining the network infrastructure to meet and maintain compliance of DoD and DoN cyber security requirements with respect to IAVAs, CTOs, and STIGs. The DITAC Department employs multiple systems in multiple configurations, including but not limited to the following:

Network Security Stack:

a. Firewalls

b. Network Intrusion Detection Systems (IDS)

c. Intrusion Protection Systems (IPS)

d. Proxy server with antivirus content scanning

e. Reverse Proxy

f. Traffic Profiling Systems

g. Routers

Network Core:

a. Radius, Message Authentication Code (MAC) authentication

b. Network Access Controller (NAC)

c. Domain Host Configuration Protocol (DHCP)

d. Domain Name System (DNS)

e. Active Directory

f. PKI/Public Key Enablement (PKE)/Cryptographic Log On (CLO)

g. Network monitoring, reporting and configuration management

h. Network event correlation

i. Syslog

j. Exchange

k. Switched Infrastructure

CND tools:

a. Vulnerability scanning and remediation

b. Patching - Windows Server Update Services (WSUS) or any other systems

c. Host Based Security System (HBSS)

d. Mobile asset protection/Data at Rest (DAR)

e. Asset management

f. Application Whitelisting

g. Forensics

h. Incident Response (i.e., Computer Emergency Response Team (CERT))

i. Penetration testing

j. Shavlik

k. Assured Compliance Assessment Solution (ACAS)

In the course of maintaining these systems, network technicians shall perform the following tasks:

a. Operating system upgrades

b. Patch application

c. Firmware upgrades

d. Hardware upgrades in support of the IT Infrastructure

e. Troubleshooting

3.2.4 The contractor shall perform engineering design, development, installation, integration, testing, upgrade, analysis, and maintenance of the NAWCWD DITAC network.

3.2.5 The contractor shall provide network security support services in accordance with the following criteria:

a. Monitor information system security alerts and advisories and take appropriate actions in response.

b. Respond in real time to all mission requirements.

c. Protect information systems against environmental hazards.

d. Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals.

e. Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.

3.3 Configuration Management (CM)

3.3.1 The contractor shall apply logistics and analytical disciplines to identify, document, and verify the function, performance and physical characteristics of systems, to control changes and non-conformance, and to track actual configurations of systems and platforms. Contractor responsibilities shall include the definition, accounting, documenting, controlling, storing, and reporting of data and information concerning hardware, software, systems, components, and processes over their life cycle. The contractor shall also ensure software compliance with the DON Application and Database Management System (DADMS). The CM process facilitates orderly management of system information and system changes for such beneficial purposes as to revise capability; improve performance, reliability, or maintainability; extend life; reduce cost; reduce risk and liability; or correct defects. All configuration management work shall conform to DODD5000.01, The Defense Acquisition System.

3.3.2 The contractor shall perform property management tasks, such as bar coding equipment, provide data to support the Property Management System, maintain data, keep data current and accurate, and print reports. The contractor shall track and report all equipment/materials to the appropriate NAWCWD property administrator.

3.3.3 The contractor shall implement and maintain a billing and work tracking system, including entering all pertinent financial data for all work performed, including logging, transferring, and tracking. The contractor shall utilize the Government-owned Billing Tracking System (BTS) database to input and track all

contractor labor hours on a weekly basis. The Government will provide the contractor with access to this BTS database.

3.3.4 The contractor shall perform CM tasks in accordance with the following criteria:

a. Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

b. Establish and enforce security configuration settings for IT products employed in organizational information systems.

c. Identify, report, and correct information and information system flaws in a timely manner.

d. Provide protection from malicious code at appropriate locations within organizational information systems.

3.4 Material Purchasing

3.4.1 The contractor shall track, process, and procure materials necessary to support DITAC customer requirements. The contractor shall provide oversight and expertise on all contractor support services; maintain communication with leadership and the contracting officer's representative (COR) while meeting cost, performance, and schedule requirements. The contractor shall maintain all necessary documentation, paperwork, and procurement paperwork packages. Procurements may include classified and unclassified materials. Any purchased material shall remain the property of the Government. Typical procurements may include hardware, software, switches, routers, crypto, security, and network analysis software. The contractor shall provide receipts for all items purchased. The contractor is responsible for managing all procurements by soliciting quotes from vendors. The contractor shall follow directions included in contract clause H-TXT-16.

3.4.2 The contractor shall develop a procurement management plan documenting all processes and that is consistent with FAR 52.245-1.

3.4.3 The contractor shall perform maintenance of material purchasing in accordance with the following criteria:

a. The contractor shall document the quantity, documentation, classification of operations supported, projects supported, issues or problems encountered, type of data processed, products prepared and delivered to DITAC customers or DITAC personnel, labor hours to produce a data product, and number of re-runs.

3.5 Program Management

3.5.1 The Program Manager shall:

a. Ensure all business activities and task order operational requirements are satisfied, including completion of any travel and overtime request documents.

b. Perform oversight on contractor personnel training and certification activities.

c. Provide managerial guidance and technical leadership, as well as perform overall task order execution.

d. Attend scheduled Government meetings and produce a report detailing the proceedings of meetings. All meeting reports shall include action items, action taken/status, and issues discussed. The Government will provide a meeting schedule(CDRL A002).

e. Provide a monthly status and financial report. The report shall contain an accurate, up-to-date summary of work performed/completed during the month, issues encountered and solved. (CDRL A003)

3.5.2 The Program Manager shall perform in accordance with the following criteria:

a. Ensure that contractor personnel within the contractor's organization are adequately trained to carry out their assigned information security-related duties and responsibilities.

b. Ensure managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems.

3.6 Help Desk and Network Operations Support

3.6.1 The contractor shall maintain current task status in the existing Government status tracking system or any subsequent replacement system. This system may require direct entry or coordination for entry within the DITAC Department, along with national organizations providing Help Desk and Network Operations support services. The contractor shall enter and maintain accurate data in the furnished database as well as establish a method to know there is an action. The contractor shall triage and track deficiencies using the status tracking database.

3.6.2 The contractor shall perform maintenance of the Help Desk in accordance with the following criteria:

a. The contractor shall maintain 100% accuracy in the Help Desk security processes, meaning that 100% of data products are delivered, entered, and maintained within approved security guidelines found within the Section 2.0 Applicable Documents.

3.7 Security

3.7.1 This contract may involve classified information up to the level of SECRET with SSBI. All personnel shall possess a secret clearance. T5 clearance is needed for Network and Computer System Administrator, Computer Network Architect and Information Security Analyst. The Government will specify the need for a higher specification as the work requires. The attached DoD Contract Security Classification Specification (DD Form 254) identifies the anticipated security access and

performance requirements for this contract.

3.7.2 Personnel Security. The contractor shall provide personnel with the appropriate personnel security clearance levels for the work to be performed. Access to Secret information is required in the performance of this contract and shall be in accordance with the DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), incorporating change 2, 18 May 2016, applicable DoD personnel security regulations, and DoD Contract Security Classification Specification (DD Form 254). The contractor shall maintain sufficiently cleared personnel to perform the tasks required by this SOW IAW the DD Form 254 and the contract. All contractor personnel shall possess the requisite security clearance, accesses, and need-to-know commensurate with the requirements of their positions.

All contractor personnel with access to unclassified information systems, including e-mail, shall have at a minimum a favorable Tier 3 (T3) investigation.

3.7.3 Information Security. Direct Support contractor personnel working under the purview of a DoN Commanding Officer/Commander shall comply with the local security provisions and the requirements of SECNAV M-5510.36B (series). The contractor shall implement and maintain security procedures and controls to prevent unauthorized disclosure of controlled unclassified information and to control distribution of controlled unclassified information in accordance with DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), and SECNAV M-5510.36B

Controlled Unclassified Information (CUI) information generated and/or provided under this contract shall be marked and safeguarded as specified in DoDI 5200.48, CUI. Contractor shall not store or transmit CUI on personal information technology systems or via personal e-mail. Unclassified e-mail containing any DoD CUI shall be encrypted. Prior to sending CUI to any non-Navy Marine Corps Internet (NMCI) addressees, the sender must first positively verify all recipients are authorized access to CUI and have need-to-know. Non-NMCI recipients must have a DoD compliant Private Key Infrastructure (PKI) certificate that enables electronic transmission via unclassified networks while protecting the CUI with a digital signature and encryption.

3.7.3.1 The contractor shall support the DC30000 ISSO in the performance of cybersecurity requirements, including reporting, managing, and securing IT assets and data under the scope of this SOW. The contractor shall provide support for the sustainment and evolution of system and application security compliance. The supporting personnel require knowledge of STIGs and must maintain IT certifications in accordance with SECNAV M-5239.2. The contractor shall report IT certification status when providing a personnel roster to the COR.

3.7.4 Communications Security (COMSEC). The contractor will require access to COMSEC at Government/contractor locations. U.S. cryptographic equipment inventory information, as well as the systems and manner in which each particular equipment is used, is for official use only. Publication or release of any related COMSEC information by any means, by the contractor, without prior written approval of the contracting officer is prohibited. The contractor must be a U.S. citizen, have a final Government security clearance with the appropriate personnel security background investigation for the level of classification involved, have strict need-to-know, have the appropriate COMSEC briefing before access is granted, and granted access only in conformance with procedures established for the particular type of COMSEC information involved. The contractor shall adhere to the DD Form 254 COMSEC security requirements, facility COMSEC material control and operating procedures, and all applicable COMSEC regulations, instructions, and policies. Prior approval from the Government Contracting Activity is required in order for a prime contractor to grant COMSEC access to a subcontractor.

3.7.5 Operations Security (OPSEC). The contractor shall comply with the OPSEC requirements outlined in the DD Form 254.

The contractor shall develop, implement, and maintain an OPSEC program to protect controlled unclassified activities, information, equipment, and material used or developed by the contractor and any subcontractor during performance of the contract. The contractor shall be responsible for the subcontractor implementation of OPSEC requirements. The OPSEC program shall be in accordance with DoD and DoN OPSEC requirements, to include:

1. Assignment of responsibility for OPSEC direction and implementation.

2. Planning guidance for the use of OPSEC Process to identify vulnerabilities and apply applicable countermeasures (Contact NAWCWD Industrial Security Office for a current OPSEC Annex and Counterintelligence CI Guide).

3. Establishment of OPSEC education and awareness training.

4. Provisions for management, annual review, and evaluation of OPSEC programs.

5. Oversight for accountability of OPSEC requirements to subcontractors.

3.7.6 Public Release. Disclosure of information is covered by DFARS 252.204-7000 Disclosure of Information, incorporated in Section I of the contract. Concerning subsection (a)(2), “information otherwise in the public domain” is information officially released into the public domain, e.g. via Distribution Statement A, and does not include information in the public domain that has not been officially released. For disclosure of unclassified information that has not been officially released, the contractor must seek specific approval from the Contracting Officer, with approval from the NAWCWD Public Affairs Office (PAO).

3.7.7 The Government retains the right to request removal of contractor personnel from work on this contract, regardless of prior clearance or adjudication status, whose actions while assigned to this contract conflict with the interests of the Government.

3.7.8 The contractor shall perform tasking in secure spaces after obtaining written authorization from a NAWCWD security representative.

3.8 Reserved

3.9 Phase In

3.9.1 The contractor shall establish and provide a transition plan (CDRL A004). The contractor shall facilitate the accomplishment of a seamless transition from the incumbent to the contractor. Phase-In services shall begin on the effective date of the award and shall be complete thirty (30) days after the effective date when the contractor will assume full responsibility.

3.9.2 The contractor shall identify points of contact (POCs) for liaison between the Government, the prime contractor, and other contracted industry partners to

ensure a proper and orderly transition, and transfer of services and assets between the parties cited. In addition, the contractor shall ensure minimum disruption to vital Government business. The contractor shall ensure there is no service degradation during or after transition.

3.9.3 The contractor shall obtain the following information from contractor and Government personnel to minimize performance reduction:

a. Transition knowledge and information regarding risk or problem areas;

b. program and project management processes;

c. points of contact;

d. location of technical, program, and project management documentation;

e. status of ongoing technical initiatives;

f. appropriate contractor-to-contractor coordination to ensure a seamless transition;

g. transition of management personnel;

h. identification of schedules and milestones; and

i. technical approach/methods and processes in support of NAWCWD Cybersecurity.

3.10 Phase Out

3.10.1 The contractor shall develop and execute a Phase-Out Plan that shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor personnel at the expiration of the contract. The Phase-Out Plan shall be submitted to the Government sixty (60) days prior to expiration of this contract (CDRL A005). The plan shall identify how the contractor shall coordinate with the incoming contractor and Government personnel to transfer knowledge regarding the following:

a. Program and project management processes;

b. points of contact;

c. location of technical, program, and project management documentation;

d. status of ongoing technical initiatives;

e. appropriate contractor-to-contractor coordination to ensure a seamless transition;

f. transition of management personnel;

g. identification of schedules and milestones;

h. identification of actions required of the Government; and

i. establishment and maintenance of effective communication with the incoming contractor personnel for the period of the transition via weekly status meetings.

3.10.2 The Phase-Out Plan shall include the following:

a. Coordination with Government representatives;

b. review, evaluation, and transition of current support services;

c. transition of historic data to new contractor systems;

d. Government-approved training and certification processes;

e. transfer of hardware warranties and software licenses (if applicable);

f. transfer of all necessary business and/or technical documentation;

g. orientation phase and program to introduce Government personnel, programs, and users to the contractor's team, tools, methodologies, and business processes;

h. disposition of contractor-purchased Government-owned assets, including facilities, equipment, furniture, phone lines, computer equipment;

i. transfer of Government-Furnished Equipment (GFE), Government-Furnished Information (GFI), and GFE inventory management assistance; and

j. personnel out-processing procedures, turn-in of all Government keys and Identification (ID) access cards.

3.11 Work Hours/Compressed Work Schedule

Workhours are defined as 0600 to 1800, Pacific Time Monday through Friday, excluding flex Fridays and US Federal holidays. NAWCWD China Lake, CA, and Pt. Mugu, CA, installations work a flex schedule of forty-four (44) hours worked one week and thirty-six (36) hours worked the other week to equate to two (2) weeks of eighty (80) hours total. Individual contractor employee work schedules, individual customer work requests, or customer agreements may define alternate work schedules, with TPOC approval. Critical functions or events may require overtime to be performed during non-core work hours.

4.0 FACILITIES AND EQUIPMENT

Government facilities and associated equipment are jointly utilized and are not provided for the exclusive use of the contractor, but on-site availability is permitted to support the performance of the requirements in this SOW.

4.1 Office Space

The Government will provide on-site facilities access, phone (land-line), computer, desk, chair, copier, scanner, administrative support, access to necessary software, Large Area Network (LAN), Wide Area Network (WAN), file stores, internet access, applicable databases, and pertinent documents.

4.2 Physical Office Space

The contractor will need the ability to respond to Government issues in person at China Lake, CA, within 30 minutes. The contractor shall establish and maintain a facility located within 15 miles of the NAWCWD main gate at China Lake to house the administrative functions necessary to ensure compliance with the contract requirements.

4.3 Government-Owned Vehicles

The contractor shall provide all vehicles required for the performance of this contract unless shared access is authorized by the Government. Contractor personnel may use Government Owned Government Operated (GOGO) vehicles managed through the Transportation Office, NAVFAC Southwest, Code 270, under the following conditions: COR concurrence with the contractor's need to use GOGO vehicle(s); COR oversight to ensure compliance with DoD 4500.36-R; clause 5252.228-9501, Liability Insurance, is included in this contract and applies to the use of GOGO vehicles; all training and licensing requirements to operate the GOGO vehicles and equipment, as defined in NAVFAC P-300, is met by the contractor; the contractor need for GOGO vehicles and equipment must be less than full time and shall not interfere with Government use of those vehicles and equipment; and use of GOGO vehicles is for work on a Government site and is for official use only for specific TO requirements.

Contractor employees that work primarily at non-Government-provided work spaces (off-site spaces) shall provide their own vehicles and equipment. Transportation Office, NAVFAC Southwest, Code 270, can only issue vehicles and equipment to Government employees. The Government remains responsible for the vehicles and equipment. The Government will only provide vehicle and equipment access to the contractor on an as-available basis.

5.0 TRAVEL

5.1. Travel will be required to Government and contractor sites to support the work required under this SOW. Travel shall be approved by the COR in writing prior to actual travel. The contractor shall travel to other Government facilities, both local and long distance, in support of this SOW. Travel may include various contractor facilities, Navy facilities, DoD facilities, Other Government Agency (OGA) offices, which may include Federal Aviation Administration (FAA), test ranges, operational activities, project or program offices, and intelligence & support activities, conferences, and seminars.

5.2 Costs associated with travel and lodging shall be reimbursed in accordance with the Joint Travel Regulations (JTR) and Federal Travel Regulations (FTR). The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements and shall be coordinated with the TPOC.

6.0 DELIVERABLES

CDRL	Title
A001	Reserved
A002	Report, Record of Meeting/Minutes
A003	Contractor's Progress, Status and Management Report
A004	Phase In Transition Plan
A005	Phase Out Transition Plan

CDRL A001 - Reserved.

CDRL A002 - Provide minutes for all meetings and include action items, action taken/status, and issues discussed. The government will provide the contractor with a meeting schedule. During these meetings, the contractor shall brief the status to other project personnel, contractor and government, and identify impediments to the successful accomplishment of the project.

CDRL A003 - The contractor shall provide a Monthly Status and Financial Report. The reports shall contain an accurate, up-to-date summary of work performed/completed during the month; issues encountered and solved. The report shall include an actual versus planned task expenditures, technical progress made, schedule status, travel conducted, meetings attended, issues, and recommendations. The report shall identify cost, schedule, and performance against task order requirements and maintain personnel certification status. The report shall identify procurements status and expenditures. The report shall identify funding compared to

ceiling, planned versus actual expenditures, technical progress made and schedule status. The report format and due date shall be mutually agreed upon by the contractor and TPOC. These reports shall be no longer than three pages.

CDRL A004 - Phase In Plan: The contractor shall establish and provide a transition plan describing the activities to transition, which shall include a schedule with milestones by activity.

CDRL A005 - Phase Out Plan: The contractor shall establish and provide a transition plan describing the activities to transition, which shall include a schedule with milestones by activity.

7.0 LABOR CATEGORIES AND QUALIFICATIONS

7.1 The Contractor shall be responsible for employing personnel having at least the minimum level of education, training, and experience, and security clearance as stated under each labor category specified herein.

7.1.2 **College Degree:** All college degrees shall be obtained from an "accredited college or university" as recognized by the U.S. Department of Education. This includes Associate's, Bachelor's, Master's, and Doctorate degrees.

7.1.3 **Professional employee Experience and Education Level definitions:**

JUNIOR: A Junior level person within a labor category has less than 3 years' experience and a BA/BS degree. A Junior level person is responsible for assisting more senior positions and/or performing functional duties under the oversight of more senior positions.

JOURNEYMAN: A Journeyman level person within a labor category has 3 to 10 years' of experience and a BA/BS degree. A Journeyman level person typically performs all functional duties independently.

SENIOR: A Senior level person within a labor category has more than 10 years' of experience and an MA/MS degree. A Senior level person typically works on high-visibility or mission critical aspects of a given program and performs all functional duties independently. A Senior level person may oversee the efforts of less senior staff and/or be responsible for the efforts of all staff assigned to a specific job.

Bachelor's Degree	6 years' additional work experience may be substituted for a Bachelor's Degree	Associate's Degree plus 4 years' additional work experience may be substituted for a Bachelor's Degree
Master's Degree	Bachelor's Degree plus 4 years' additional work experience may be substituted for a Master's	

"Years of experience" shall mean full, productive years of participation.

"Productive years" shall mean 52 weeks of work reduced by reasonable amounts of time for holidays, annual and sick leave.

If participation was part-time, or if less than one-half of the standard work week was spent performing qualifying functions, the actual time spent performing qualifying functions may be accumulated to arrive at full years of experience.

7.1.4 **Labor Qualifications:** The following lists the minimum labor category, education and experience requirements, and the functional descriptions for each labor category:

Labor Category	Level	BLS SOC Code	Functional Description
Manager	Journeyman	11-1021	Acts as the overall lead, manager and administrator for the contracted effort. Serves as the primary interface and point of contact with Government program authorities on technical and program/project issues. Oversees contractor execution of the contract requirements. Manages acquisition and employment of program/project resources.

General Clerk	General Clerk I (SCA 01111) General Clerk II (SCA 01112)	43-6011	Follows clearly detailed procedures in performing simple repetitive tasks in the same sequence. Responsibilities would include filing pre-coded documents in a chronological file, or operating office equipment, (e.g., mimeograph, photocopy, addressograph or mailing machine). This position uses some subject-matter knowledge and judgment to complete assignments consisting of numerous steps varying in nature and sequence.
Configuration Management Analyst	Journeyman	13-1111	Collects, organizes and interprets data relating to aircraft and product programs. Maintains configuration control of acquisition products and data. Tracks configuration changes. Coordinates and supports development of Engineering Change Proposals. Applies government-instituted processes for documentation, change control management and data management.
Network and Computer Systems Administrators	Junior, Journeyman and Senior	15-1244	Install, configure, and maintain an organization's local area network (LAN), wide area network (WAN), data communications network, operating systems, and physical and virtual servers. Perform system monitoring and verify the integrity and availability of hardware, network, and server resources and systems. Review system and application logs and verify completion of scheduled jobs, including system backups. Analyze network and server resource consumption and control user access. Install and upgrade software and maintain software licenses. May assist in network modeling, analysis, planning, and coordination between network and data communications hardware and software. Excludes "Information Security Analysts"(15-1212), "Computer User Support Specialists" (15-1232), and "Computer Network Support Specialists" (15-1231).
Computer Network Architects	Senior	15-1241	Design and implement computer and information networks, such as local area networks (LAN), wide area networks (WAN), intranets, extranets, and other data communications networks. Perform network modeling, analysis, and planning, including analysis of capacity needs for network infrastructures. May also design

			network and computer security measures. May research and recommend network and data communications hardware and software. Excludes "Information Security Analysts" (15-1212), "Network and Computer Systems Administrators" (15-1244), and "Computer Network Support Specialists" (15-1231)
Information Security Analyst	Junior, Journeyman and Senior	15-1212	Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. Assess system vulnerabilities for security risks and propose and implement risk mitigation strategies. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses. Excludes "Computer Network Architects" (15-1241).
Computer User Support Specialist	Senior	15-1232	Provide technical assistance to computer users. Answer questions or resolve computer problems for clients in person, or via telephone or electronically. May provide assistance concerning the use of computer hardware and software, including printing, installation, word processing, electronic mail, and operating systems. Excludes "Network and Computer Systems Administrators" (15-1244).

7.1.5 The DITAC Endpoint Systems Administration Branch, provides IT and expertise in direct support of DITAC and NAWCWD laboratories. The Endpoint Systems Branch provides DITAC, NAWCWD, and Product Teams' laboratories critical information technology professionals and solutions required to perform their mission objectives.

The Contractor shall provide System Administrators (SA) support for the DITAC mission. The SAs shall:

- Have training and certification in accordance with DoD standard (DoD 8570/8140).

- Implement new technologies, as directed by DITAC engineering project plans

- Troubleshoot systems for firewall, Host-based Intrusion Prevention System (HIPS), and Network-based Intrusion Prevention System (NIPS) problems and provide corrective action directly or with the assistance of the HBSS administrator.

- Troubleshoot all network and server errors/malfunctions and provide resolution.

- Install software only after verifying it is approved in DADMS and is licensed.

- Upgrade systems in accordance with vendor supportability maintenance and documentation (i.e., video cards, hard drives or Solid State Drives (SSD's), printers).

- Troubleshoot systems and software; and shall provide resolution.

- Manage users, groups and access lists.

- Utilize the latest technologies to rapidly produce "ready information systems" (e.g., virtualization, hard disk cloning software, operating system utilities).

- Work with vendors and appropriate infrastructure teams to implement, operate, and maintain various technologies, including:

o Virtualization systems

o High Performance Computing (HPC) environments

o Storage arrays

o Dedicated WAN connections

- Support the operation and maintenance of Lab environments, including:

o Windows operating environments

o Linux operating environments

o MAC operating environments

o Server environments

- Work with the ISSO to establish, secure, and maintain accreditation boundaries. In conjunction with the ISSO, the SA shall ensure the information system is adequately safeguarded against cyber security threats and is operationally sound to meet the organization's mission requirements.

- Satisfy all roles and responsibilities defined in their formal appointment letter, as designated by the CISSM.

The contractor shall perform tasks to support all aspects of the DITAC digital infrastructure, such as: database and application administration; integration support; workstation management of hardware repair, upgrades and/or enhancements; software license upgrades and/or enhancements; requirements analysis; identifying and improving technical solutions; securing and managing operating systems; validating backups; on-site and remote troubleshooting and repair.

The contractor shall perform operational support including backups; system tuning, file conversions, information handling; data entry, data migration, and data management.

The contractor shall analyze systems security log files, monitor system firewall log files, and take appropriate information security action should an intrusion or threat be detected. The contractor shall respond to IAVM and report back to the appropriate Cybersecurity Team. The contractor shall perform vulnerability scanning and harden systems to meet DoD requirements to meet accreditation standards in accordance with Risk Management Framework.

7.1.6 Approved Baseline Certifications

Computer Network Architect and Network Computer Systems Administrator.

IAT Level I	IAT Level II	IAT Level III
A+ CE CCNA-Security CND Network+ CE SSCP	CCNA Security CySA+ ** GICSP GSEC Security+ CE CND SSCP	CASP+ CE CCNP Security CISA CISSP (or Associate) GCED GCIH CCSP

Information Security Analyst.

IAM Level I	IAM Level II	IAM Level III
CAP CND Cloud+ GSLC Security+ CE HCISPP	CAP CASP+ CE CISM CISSP (or Associate) GSLC CCISO HCISPP	CISM CISSP (or Associate) GSLC CCISO

8.0 ACRONYMS

ACAS Assured Compliance Assessment Solution

AS	Acquisition Strategy
ATO	Authorization to Operate
BICSI	Building Industry Consulting Service International
BMMP	Business Management Modernization Program
BTS	Business Tracking System
C&A	Certification and Accreditation
CCA	Clinger-Cohen Act
CDD	Capability Description Document
CDRL	Contract Data Requirement Lists
CERT	Computer Emergency Response Team
CI	Counterintelligence
CIO	Chief Information Officer
CISSM	Command Information System Security Manager
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLO	Cryptographic Log On
CM	Configuration Management
CND	Computer Network Defense
CNO	Computer Network Operations
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
COR	Contracting Officer's Representative
CPD	Capability Production Document
CPI	Critical Program Information
CS	Cybersecurity Strategy
CTO	Computer Tasking Order
CUI	Controlled Unclassified Information
DADMS	DON Application and Database Management System
DAR	Data at Rest
DCO	Defensive Cyber Operations
DHCP	Domain Host Configuration Protocol
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITAC	Digital Information Technology Analysis and Cyber
DNS	Domain Name System

DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Issuance
DoDM	DoD Manual
DoN	Department of Navy
EIA	Electronics Industries Association
	Electrical Industry Alliance
EKMS	Electronic Key Management System
eMASS	Enterprise Mission Assurance Support Service
FAM	Functional Area Manager
FIPS PUB	Federal Information Processing Standards Publications
FTR	Federal Travel Regulations
GFE	Government-Furnished Equipment
GFI	Government-Furnished Information
GFP	Government-Furnished Property
GOGO	Government-Owned, Government-Operated
HBSS	Host Based Security System
HIPS	Host-based Intrusion Prevention System
HPC	High Performance Computing
HUMINT	Human Intelligence
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
ICD	Initial Capabilities Document
ID	Identification
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical & Electronics Engineers
IM	Information
IMINT	Imagery Intelligence
IP	Internet Protocol
IPS	Intrusion Protection Systems
IPT	Integrated Product Team
IS	Information System
ISNS	Integrated Shipboard Network System
ISSO	Information System Security Officer

IT	Information Technology
ITPR	Information Technology Procurement Request
JTR	Joint Travel Regulations
JUON	Joint Urgent Operational Need
LAN	Large Area Network
MAC	Message Authentication Code
MOA	Memorandum of Agreement
NAC	Network Access Controller
NAE	NAVAIR Enterprise Architect
NAVAIR	Naval Air Systems Command
NAV-ITAS	Navy Information Technology Approval System
NAWCWD	Naval Air Warfare Center Weapons Division
NIOC	Navy Information Operations Command
NIPS	Network-based Intrusion Prevention System
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NMCI	Navy Marine Corps Intranet
NPPS	Navy Ports Protocols, and Services
NSS	National Security Systems
OMB	Office of Management and Budget
OPNAVINST	Office of the Chief of Naval Operations Instruction
OPSEC	Operations Security
OSINT	Open Source Intelligence
PAO	Public Affairs Office
PBIS-IT	Program Budget Information System – Information Technology
PIT	Platform Information Technology
PKE	Public Key Enablement
PKI	Public Key Infrastructure
PM	Program Manager
POC	Points of Contact
PPIP	Program Protection Implementation Plan
PPL	Parts Provisioning List
PPSM	Ports, Protocols, and Services Management
PRS	Provisioning Requirements Statement
RMF	Risk Management Framework
SA	System Administration

	System Administrator
SDP	Software Development Plan
SECNAVINST	Secretary of the Navy Instruction
SIGINT	Signals Intelligence
SOW	Statement of Work
SP	Security Plan
SSD	Solid State Drive
STIG	Security Technical Implementation Guide
T3	Tier 3
TIA	Telecommunications Industry Association
TPOC	Technical Point of Contact
UON	Urgent Operational Need
USN	United States Navy
UUNS	Urgent Universal Need Statement
VPN	Virtual Private Network
WAN	Wide Area Network
WRA	Web Risk Assessment
WSUS	Windows Server Update Services

Note: All provisions and clauses of Section C of the basic contract apply to this task order, unless otherwise specified in the task order, in addition to the following:

CLAUSES INCORPORATED BY FULL TEXT

5252.204-9502 REQUIREMENTS FOR LOCAL SECURITY SYSTEM (NAVAIR) (OCT 2005)

The contractor agrees to provide locator information regarding all employees requiring a permanent badge for authorized entrance to the Naval Air Station China Lake. Entrance is authorized by this contract as a result of tasks associated with performance of the Section C - Statement of Work only. Initial information shall be provided as each individual is assigned to this contract by using the Locator Form provided as an attachment to this contract. Thereafter, quarterly reports (due at the beginning of each quarter by the fifth day of the month) will be provided with gains/losses (identification of new and replaced or added individuals) and any changes to current personnel (such as telephone number, building number and room number). A point of contact is to be named on each quarterly report for any questions/additional information needed by the Government recipient. The quarterly reports are to be addressed to COR. All losses are to have the permanent badges returned to COR on the last day of the individual’s task requirement.

5252.211-9509 INCORPORATION OF THE CONTRACTOR'S TECHNICAL PROPOSAL (NAVAIR)(OCT 2005)

The Contractor's Technical Proposal Number: 8122-501, dated 22 March 2022 , and any amendments/addendums thereof, is incorporated herein by reference, unless otherwise specified, with the same force and effect as if set forth in full text. Nothing in the Contractor's proposal shall constitute a waiver of any of the provisions of the contract, including the Statement(s) of Work and Specification. For purposes of FAR Clause 52.215-8, “Order of Precedence”, the Contractor's technical proposal shall be considered a “Specification” but the Government's Specification shall take precedence over the Contractor's technical proposal.