STATEMENT OF WORK
NAVAL AIR WARFARE CENTER WEAPONS DIVISION (NAWCWD), China Lake
RDT&E INFRASTRUCTURE DIVISION CONTRACTOR SERVICE

1. DESCRIPTION OF SERVICES / INTRODUCTION

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

1.1 Background

The RDT&E Infrastructure Divisions at the Naval Air Warfare Center Weapons Division (NAWCWD) provides unique facilities and laboratories with a broad spectrum of technology, capabilities, and innovative system interoperability and integration requirements with both internal/external supports necessary to ensure an efficient and effective operating environment to meet our goals and objectives for all customers at NAWCWD. The RDT&E Infrastructure Branches manage and operate the NAWCWD networks and computer systems providing cost effective, base-wide connectivity to access Department of Defense (DoD) networks, facilities, laboratories and ranges. These services provide operations, maintenance, upgrades and management for network infrastructure and planning.

The RDT&E Infrastructure serves as a NAWCWD resource for Information Technology (IT), System Administration (SA) and Cyber Security support and maintains expertise in Department of Defense (DoD), Department of Navy (DoN) and subordinate command IT policy and procedures to leverage best practices for our customer base. The RDT&E Infrastructure is composed of diverse service capabilities whose mission is to provide superior customer service and support to the organization within NAWCWD. Providing this support, the RDT&E Infrastructure Division enables the organization to focus their resources on the mission at hand which is to support the United States Warfighter.

1.2 Scope

The scope of this SOW is to encompass the services and materials necessary for the analysis, design, development, test, integration, deployment and operation of Information Technology (IT) systems and services to meet the RDT&E Infrastructure Division customers by providing NAWCWD, NAVAIR and the user community with value added, cost effective IT and Cyber Security solutions with an overarching goal of maintaining a secure network.

The place of performance for this effort is NAWCWD China Lake, Point Mugu and Tucson Arizona. The following sites are for future work possibilities at Port Hueneme and San Nicholas Island. Contractors may be required to deploy into the field at multiple customer locations within the China Lake installation (a 1.1 million acreage installation).

APPLICABLE DOCUMENTS

The following documents are applicable to this SOW to the extent specified herein.

2.1 Websites, Web Enablement and Application/System Development, Modification, and Maintenance Capability

All IT systems, software, and website development, or modification 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/servers hosted/located in contractor facilities, or outside NAVAIR enclave, will transition to NAVAIR architecture and infrastructure in accordance with Legacy Shutdown guidance. Policies include, but are not limited to the following:

a. Office of Management and Budget (OMB) 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, Rehabilitation Act of 1973, http://www.section508.gov/
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, https://www.nioc-norfolk.navy.mil/wra/index.html
f. DON Policy for Content of Publicly Accessible World Wide Web Sites, SECNAVINST 5720.47B, http://www.doncio.navy.mil/PolicyView.aspx?ID=421
g. NAVAIR CIO Website (NAVAIR specific policy and guidelines), https://mynavair.navair.navy.mil/portal/server.pt/community/dcio_applications_integration___business_intelligence_%287_2_2%29/1491/web_enablement/57583
h. Defense Information Systems Agency (DISA) Hosting of All Navy Websites (Naval Administrative (NAVADMIN) 061/08), http://www.npc.navy.mil/NR/rdonlyres/A4E463D0-02AF-4094-A054-BB1D807F631B/0/NAV08061.txt
i. Consolidation of Navy Websites – Reduction of IM/IT Footprint, NAVADMIN 145/07, http://www.npc.navy.mil/NR/rdonlyres/787908B8-55E8-4A6F-9BD8-A74B3C0824F0/0/NAV07145.txt
j. DON Web Presence Policy: The Registration, Compliance of, and Investment in, All Unclassified Web Sites and Uniform Resource Locators, http://www.doncio.navy.mil/PolicyView.aspx?ID=577

2.2 Information Assurance

NAVAIR's IA Program is a unified approach to protect unclassified, sensitive, or classified information, and is established to consolidate and focus efforts in securing that information, including its associated systems and resources. IA is required operationally throughout the DON. The DON CIO is responsible for IT within the Navy, as mandated by the CCA, and is the lead for Departmental compliance with the Federal Information Security Management Act of 2002.

All IA shall be in compliance with the following listed instructions to include those referenced within the below listing:

a. Assistant Secretary of Defense (ASD) Networks and Information Integration (NII) Directive-Type Memorandum (DTM) 08-027 – Security of Unclassified DoD Information on Non-DoD Information Systems, 31 July 2009
b. OPNAVINST 2201.2, Navy and Marine Corps Computer Network Incident Response
c. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170. 01H (series) – Joint Capabilities Integration and Development System, 10 January 2012
d. CJCSI 6211.02D – Defense Information System Network (DISN): Responsibilities, 24 January 2012
e. CJCSI 6212.01E (series) – Interoperability and Supportability of Information Technology and National Security Systems, 15 December 2008
f. CJCSI 6212.01F (series) – "Net Ready Key Performance Parameter (NR KPP)," March 21, 2012.
g. CJCSI 6251.01D (series) – Narrowband Satellite Communications Requirements, 30 November 2012
h. CJCSI 6510.01F – Information Assurance (IA) and Computer Network Defense (CND), 9 February 2011
i. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01A – Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program), 24 June 2009
j. Chief of Naval Operations/Headquarters, United States Marine Corps (CNO) N614/HQMC C4 – Navy-Marine Corps Unclassified Trusted Network Protection (UTN-Protect) Policy, Version 1.0, 31 October 2002
k. Defense Acquisition Guidebook – Chapter 7, Acquiring Information Technology, Including National Security Systems; and Section 7.5, Information Assurance (IA)
l. DoD 5200.1-R, Information Security Program
m. DoD 5205.02-M, dated November 3, 2008,
n. DoD Directive 5230.09, dated August 22, 2008.
o. DoD 5220.22-R, the DoD Industrial Security Regulation
p. DoD 5220.22-M – National Industrial Security Program Operating Manual, 28 February 2006 (NISPOM)
q. DoD 8570.01-M – Information Assurance Workforce Improvement Program, 19 December 2005 (Incorporating Change 3, 24 January 2012)

r. DoDD 8000.01 – Management of the Department of Defense Information Enterprise, 10 February 2009
s. DoD 8100.1--Global Information Grid (GIG) Overarching Policy
t. 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 as of 23 April 2007
u. DoD 8500.1--Information Assurance
v. DoDD 8500.01E (series) – Information Assurance (IA), 24 October 2002; Certified Current as of 23 April 2007
w. DoDI 8510.01 "DoD Risk Management Framework (RMF)," 12 March 2014
x. DoDI 8551.01, "Ports, Protocols, and Services Management (PPSM)," May 28, 2014.
y. DoDD 8140.01 – Cyberspace Workforce Management 11 August 2015
z. DoDI 4630.8 – Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004
aa. DoDI 8510.01 – DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007
bb. DoDI 8520.02 – Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011
cc. DoDI 8551.1 – Ports, Protocols, and Services Management (PPSM), 13 August 2004
dd. DoDI 8580.1 – Information Assurance in the Defense Acquisition System, 9 July 2004
ee. DoDI 8581.01 – Information Assurance (IA) Policy for Space Systems Used by the Department of Defense, 8 June 2010
ff. 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
gg. DON letter 5239 NAVAIR 726/2322, 18 February 2009 – NAVAIR Data at Rest Policy
hh. Federal Information Processing Standards Publications (FIPS PUB), http://www.itl.nist.gov/fipspubs/by-num.htm
ii. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 – Revised Fact Sheet National Information Assurance Acquisition Policy, July 2003
jj. Office of the Chief of Naval Operations (OPNAVINST) 5239.1C – Navy Information Assurance (IA) Program, 20 August 2008
kk. SECNAV M-5239.1 – Department of the Navy Information Assurance Program; Information Assurance Manual, November 2005
ll. SECNAVINST 5230.15 – Information Management/Information Technology Policy for Fielding of Commercial Off the Shelf Software, 10 April 2009
mm. SECNAVINST 5239.3B – Department of the Navy Information Assurance Policy, 17 June 2009
nn. SECNAVINST 5239.19 – Department of the Navy Computer Network Incident Response and Reporting Requirements, 18 March 2008
oo. SECNAV M-5239.2 Cyberspace Information Technology And Cybersecurity Workforce Management And Qualification Manual, June 2016
pp. NTISSD 600, Communications Security (COMSEC) Monitoring
qq. The National Security Act of 1947
rr. Title 40/Clinger-Cohen Act
ss. National Institute of Standards and Technology (NIST) 800 series
tt. Electronic Key Management System (EKMS)-1
uu. DOD Directive 5000.01 The Defense Acquisition System

All IT procured on behalf of this contract shall meet all DoD/DON and NAVAIR IA policies. Failure to follow these policies will result in denied access to NMCI, and other DON, DoD, and Joint Networks. These IA policies are standard across the Department and ensure IA compatibility and interoperability.

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

2.3 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. Department of Defense Office of General Counsel, Ethics Issues in Government-Contractor Teambuilding
d. DoDM 5200.01, Information Security Program Manual (Volume 4)
e. National Security Decision Directive 298, DoDD 5205.02E
f. OPNAVINST 3432.1A Operations Security

2.4 Other Standards

The following Industry Standards apply to contractor performance of all aspects of the contract:

a. Building Industry Consulting Service International (BICSI)
b. Telecommunications Industry Association (TIA)/Electrical Industry Alliance (EIA)

2. 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 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 Government Status Tracking system to obtain requirements of Infrastructure Division customers. Access to the system will be provided through government resources. The Government 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. This includes the verification and validation of solution sets and protocols while assisting user with all aspects of IT acquisition. All required certifications and training shall be obtained 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, TIA/EIA Industry Standards.

3.1 Information Assurance/Security

3.1.1 The contractor shall perform tasks to support all aspects of the 5.4.1 Infrastructure Division 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; Computer Network Defense (CND); identification of cyber security threats to include remediation of identified vulnerabilities and risk mitigation; 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, monitored 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 5.4.1 Code IA 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 5.4.1 Infrastructure customers and determine their IA maturity and security posture, compared to NAWCWD and DoD/Department of Navy (DoN) standards. The contractor shall provide Cyber Security recommendations based on Cyber Security policies and procedures outlined in the Department of Defense Issuances (DoDI) 8510.01. The contractor shall provide the required documentation for government approval to complete the certification and accreditation process in accordance with Department Of Defense Information Technology Security Certification and Accreditation Process (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 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/or 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 5.4.1 customers.

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

3.1.9 The contractor shall protect unclassified, sensitive and classified information. The contractor shall develop and or 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 information technology 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 required by organization responsible for the accreditation boundary.

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

(a) Allocate sufficient resources to adequately protect organizational information systems
(b) Ensures 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) The contractor shall 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 which may include the creation of metrics and dashboard aids; development of scripting to support automation of CND functions; 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 DOD Directive 5000.01 The Defenses Acquisition System. The contractor shall follow 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 plan recommendations for workflow and process improvement.

3.2.3 The contractor shall assist the government in preparing and sustaining the RDT&E network infrastructure to meet and maintain compliance of DoD and DoN cyber security requirements with respect to IAVAs, CTOs and STIGs. The RDT&E network infrastructure 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. Public Key Infrastructure (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

In the course of maintaining these systems, network technicians are expected to perform the following tasks but not limited to:

a. operating system upgrades
b. patch application
c. firmware upgrades
d. hardware upgrades in support of the IT Infrastructure.

3.2.4 The contractor shall perform engineering design, development, installation, integration, testing, upgrade, analysis, and maintenance of the NAWCWD RDT&E 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) The contractor shall 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

3.3.1 The contractor shall apply logistics and analytical disciplines to identify, document, and verify the functional, 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, but not be limited to, 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 DOD Directive 5000.01, The Defenses 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, maintaining 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. Contractor shall utilize the government owned Business Tracking System (BTS) database to weekly 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 configuration Management 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 information technology 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 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/or unclassified materials. Any purchased material shall remain the property of the Government. Typical procurements may include but not limited to: 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 to 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 and FAR 52.244-1.

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

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

3.5 Program Management

3.5.1 The Program Manager is responsible for the following:

a. Ensure all business activities and task order operational requirements are satisfied, including completion of any travel and/or 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. Shall 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. (A001). See Section 6, Deliverables in this SOW.

e. Shall 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. (A002). See Section 6, Deliverables in this SOW.

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

3.6.1 The Contractor shall maintain current task status in the existing Government status tracking system or any subsequent replacement system. This may require direct entry or coordination for entry with the Information Technology / Information Management (IT/IM) Department and the National Help Desk provider. This task requires the contractor to enter and maintain accurate data in the furnished database as well as establish a method for the contractor to know they have an action. The contractor shall triage and track deficiencies using the status tracking database.

3.6.2 The contractor shall perform maintenance of 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 The contractor shall comply with the security requirements contained in the attached DoD Contract Security Classification Specification, DD 254. All personnel assigned to work included in this SOW shall be United States citizens. The Contractor shall ensure compliance with applicable DoD, DoN and Command Directives and Instructions to eensure security requirements are met and maintained. The contractor shall provide new employee clearances within 30 days prior to starting work under this contract. This task shall require the contractor to interface with local security representatives on security issues; process all media and documentation movement within controlled spaces; and maintain the status of all tracked items from creation to destruction.

3.7.2 The minimum clearance level required to perform this task order is an active SECRET and is required on the first day of performance. All specialists shall be required to obtain a Single Scope Background Investigation (SSBI) with a Secret clearance level. Personnel must hold this designated clearance level when they start work as indicated by the Government. Some programs supported by the RDT&E Infrastructure Division have security requirements above Secret and may require a Top Secret, SCI Special Access Program (SAP), or Special access required (SAR) clearances for access and support. Additional security requirements for F-35 Joint Program Office special projects will be provided to the contractor employee on a case-by-case basis as required in performance of the contracted services. Cognizant SAP security office will provide the contractor with program security guide and program classification guide. Access to or knowledge of that portion of the work will be restricted to those individuals who have a need-to-know, a U.S. government clearance at the appropriate level and a special briefing. Contractors may need to be COMSEC briefed. The Government anticipates that access to classified data/information up to and including TS, SAP/SAR, and North Atlantic Treaty Organization (NATO) will be required for both facility and personnel in the performance of this work.

3.7.3 Communications Security (COMSEC): The contractor will require access to COMSEC for the work being performed under this contract. 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.

3.7.4 For Official Use Only information generated and/or provided under this contract shall be marked and safeguarded as specified in DoDM 5200.01, Information Security Program Manual (Volume 4) available at http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf . Contractor shall not store or transmit Controlled Unclassified Information (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.

3.7.5 Operations Security: The contractor shall adhere to all Operations Security (OPSEC) requirements specified in the DD Form 254. While performing work at NAVAIR or NAVAIR sites, the contractor shall comply with the provisions of all Department of Defense (DoD) and Department of Navy (DoN) OPSEC requirements per the National Security Decision Directive 298, DoDD 5205.02E, DoD 5205.02-M, OPNAVINST 3432.1A, and the local command/facility instruction series for OPSEC as well as any procedures identified in program-specific operations security plans and program protection plans as applicable. The contractor shall be responsible for subcontractor implementation of the OPSEC program requirements for this contract, as applicable.

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, notwithstanding subsection (a)(2) of [the clause], the contractor must seek specific approval for disclosure of controlled unclassified information even if the information already exists within the public domain.

3.8 Reserved

3.9 Phase In / Phase Out

PHASE IN:

3.9.1 The contractor shall establish and provide a transition plan. (A003) See section 6, Deliverables in this SOW. 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 In order to minimize performance reduction, the contractor shall obtain the following from contractor personnel and/ or Government personnel in the areas of:

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. Identify schedules and milestones
i. Technical approach/methods and processes in support of NAWCWD Cybersecurity

PHASE OUT:

3.9.4 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/Government personnel at the expiration of the contract. The Phase-Out Plan shall be submitted to the Government sixty (60) days prior to expiration this contract. (A003) The plan shall identify how the contractor shall coordinate with the incoming contractor and or 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. Identify schedules and milestones
h. Identify actions required of the Government
i. Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings

3.9.5 Phase Out Plan shall include, but is not limited to:

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 process
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, etc.
i. Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
j. Personnel out-processing procedures, turn-in of all Government keys and ID/access cards.

3.10 Work Hours

3.10.1 Work hours 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.

4.1 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.

4.2 Office Space

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

4.3 Physical Office Space

Contractor shall have a physical designated office space, not a P.O. Box address, located within a ten (10) mile radius of the city of Ridgecrest, CA to provide a 30 minute response time by contractor to conduct official government to contractor business.

4.4 Government Owned Vehicles

The contractor shall be required to utilize Government owned vehicles (when available) on and off Center, while performing tasks under this SOW. Potential uses of Government owned United States Navy (USN) vehicles may include the transport of data, equipment, and material between Government locations. The contractor shall only use Government vehicles for required contract performance. The contractor and Government personnel may rideshare to remote sites and customer facilities on the NAWCWD installation when performance of official duties are necessary. Ridesharing to remote sites and customer facilities outside

the NAWCWD installation shall be on a case-by-case basis and approved by the Contracting Officer. Ridesharing includes the use of Government-owned, Government-operated (GOGO) code-owned vehicles. The following shall be required of all contractor drivers:

a. Comply with all state and federal laws pertaining to operating motor vehicles.
b. Comply with NAVAIR command policies when operating a vehicle (i.e. no cell phone use).
c. Have a valid California driver's license
d. Have vehicle insurance coverage for contractor employees driving designated vehicles, FAR 52.228-7.
e. Meet all requirements of FAR Part 45 Government Property while operating Government vehicles.
f. Use the most cost-effective (economical) means to fuel vehicles.
g. Use valid property passes when transporting Government inventory.

5. 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, but is not limited to, 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 IAW 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. DELIVERABLES

(CDRL A001) 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 A002) 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 A003) Phase In/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.