N6134023R0058
Attachment J-1 SOW Rev-0
27 April 2023

STATEMENT OF WORK
FOR
Software Maintenance of Fielded Training Systems
(SWMFTS)

NAVAL AIR WARFARE CENTER
TRAINING SYSTEMS DIVISION (NAWCTSD)
12211 Science Drive
Orlando, Florida 32826-3224

Revision Number	Purpose	Date

STATEMENT OF WORK FOR
Software Maintenance of Fielded Training Systems

1. Applicable Documents.

The below documents provide guidance related to the tasking required by this Statement of Work (SOW). The SOW takes precedence in the event of conflict with the below documents; however, nothing in this SOW supersedes applicable laws and regulations. The Government will provide all necessary reference documents not generally available to the Contractor, as required. Throughout the life of the contract, if any instruction or document is replaced or superseded, the replacement or superseding instruction or document shall be applicable to the requirements defined in this SOW.

a. OMB Memorandum M-11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, 14 September 2011.

b. Chairman of the Joint Chiefs of Staff Instruction CJCSI) 3170.01I (series), Joint Capabilities Integration and Development System, 23 January 2015.

c. CJCSI 6211.02D (series), Defense Information System Network (DISN): Policy and Responsibilities, 24 January 2012, Current as of 4 August 2015.

d. CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 February 2011, Current as of 9 Jun 2015.

e. CJCSM 6510.01B, Cyber Incident Handling Program, 10 July 2012, Current as of 18 December 2014.

f. Defense Acquisition Guidebook – Chapter 7, Acquiring Information Technology, Including National Security Systems, Section 7.5, Information Assurance (IA).

g. DoD 5200.2-M, Procedures for the DoD Personnel Security Program," 3 April 2017.

h. DoDI 5205.13, Defense Industrial Base Cybersecurity Activities – Incorporating Change 2, 21 August 2019.

i. DoDI 5200.48, Controlled Unclassified Information, 6 March 2020.

j. DoDM 5200.01 Volume 1, DoD Information Security Program: Overview Classification, and Declassification – Incorporating Change 2, 28 July 2020.

k. DoDM 5200.01 Volume 2, DoD Information Security Program: Marking of Information – Incorporating Change 4, 28 July 2020.

l. DoDM 5200.01 Volume 3, DoD Information Security Program: Protection of Classified Information – Incorporating Change 4, 28 July 2020.

m. DoDD 8000.01, Management of the Department of Defense Information Enterprise, 27 March 2017.

n. 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.

o. DoDI 8500.01, Cybersecurity – Incorporating Change 1, 7 October 2019.

p. DoDD 8140.01, Cyberspace Workforce Management, 5 October 2020

q. DoDI 8140.02, Identification, Tracking, and Reporting of Cyberspace Workforce Requirements, 21 December 2021.

r. DoDI 8100.04, DoD Unified Capabilities (UC), 9 December 2010.

s. DoDI 8330.01, Interoperability of Information Technology, Including National Security Systems, 27 September 2022.

t. DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, 3 November 2017.

u. DoDI 8510.01, Risk Management Framework For DoD Systems, 19 July 2022.

v. DoDI 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011.

w. DoDI 8551.1, Ports, Protocols, and Services Management (PPSM), 28 May 2014.

x. DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 Dec 2005 (Incorporating Change 3, January 24 , 2012).

y. DoDI 8580.1, Information Assurance in the Defense Acquisition System, 9 July 2004.

z. DoDI 8582.01, Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information, 9 December 2019.

aa. DoDI 5220.22, National Industrial Security Program (NISP), 10 December 2021.

bb. 32 CFR (Code of Federal Regulations) Part 117, National Industrial Security Program Operating Manual (NISPOM), 24 February 2021.

cc. CNSS Policy No. 11, National Policy Governing The Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, 10 Jun 2013.

dd. Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems, 29 July 2022.

ee. SECNAV M-5239.3, Department of the Navy Cybersecurity Manual, 22 April 2022.

ff. SECNAVINST 5510.36B, Department of the Navy Information Security Program, 12 July 2019.

gg. SECNAVINST 5510.37A, Department of the Navy Insider Threat Program, 28 October 2019.

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

ii. SECNAVINST 5239.3C, Department of the Navy Cybersecurity Policy, 2 May 2016.

jj. SECNAVINST 5239.19A, Department of the Navy Computer Network Incident Response and Reporting Requirements, 4 September 2019.

kk. Department of Defense Information Technology Portfolio Repository- Department of the Navy (DITPR-DON) Registration Guidance, December 5, 2011.

ll. Federal Information Processing Standard Publication (FIPS Pub) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

mm. National Institute of Standards and Technology (NIST) 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations, December 2018.

nn. NIST Special Publication 800-60 Volume 1 Revision 1, Volume I: Guide to Mapping Types of Information and Information Systems to Security Categories, August 2008.

oo. NIST Special Publication 800-60 Volume 2 Revision 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.

pp. NIST 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, 10 December 2020.

qq. NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012.

rr. NIST Special Publication 800-137 Revision 1, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011.

ss. NIST Special Publication 800-59, “Guideline for Identifying an Information System as a National Security System,” August 2003.

tt. NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide, 6 August 2012.

uu. NIST Special Publication 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, 5 May 2022.

vv. NIST Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, 28 January 2021.

ww. OPNAVINST 5239.D, U.S. Navy Cybersecurity Program, 18 July 2008.

xx. USN RPG 3.3, United States Navy Risk Management Framework Process Guide, October 2021.

yy. NAVADMIN 062/21, Risk Management Framework Standard Operating Procedures, 15 March 2021.

zz. USN RMF RAG Version 1.0, United States Navy Risk Management Framework Risk Assessment Guide, 29 October 2019.

aaa. 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.

2. Scope.

This SOW establishes the requirements for Software (SW) Maintenance of Fielded Training Systems. Support includes operation, maintenance, and repair of Information Technology (IT) consisting primarily of corrective, adaptive, perfective and preventative SW maintenance; some limited modification of hardware (HW), operation, maintenance, and repair of HW; and associated minor support tasks. The trainers that will be supported on this effort simulate aviation, surface, and undersea platforms and they include: operator training systems, weapons training systems, training environments, use of sensors, and communications network systems. Locations for support are at military facilities in the continental United States (CONUS) and outside continental United States (OCONUS).

3. Requirements.

3.1 General Requirements.

The contractor shall execute the following broadly defined tasks and functional requirements as required to support the NAWCTSD In-Service Engineering Office (ISEO). The contractor shall provide primary SW Maintenance and HW operation and maintenance (O&M) tasks to fielded training systems at select United States Navy and Marine Corps installations across the United States and Japan. Minor support tasks that directly support the primary task on this effort include configuration management, technical support, engineering change proposal support (ECP), Integrated Project Team (IPT) support, Fleet Synthetic Training (FST) support, and Cyber Security support of training devices, documentation support, and supply support for the purchase and installation of incidental material, as well as the associated management and administrative support. The Contractor shall perform all applicable Cyber Security functions in Section 3.11 in association with the tasks listed below.

3.2 Detailed Requirements. (SW Maintenance Support and HW O&M Support).

The following subsections define the tasks that the Contractor shall accomplish in support of NAWCTSD SW Maintenance of Fielded Training Systems. In all of the following tasks the Contractor's role is to assist the Government with activities such as coordinating, collecting, analyzing, and reporting. The Contractor shall make recommendations to the Government, but will not make decisions.

3.2.1 Primary Tasks. (SW Maintenance Support).

The Contractor shall assist the Government's ISEO with SW maintenance support efforts including corrective SW maintenance (fixing SW errors), adaptive SW maintenance (adapting SW to new environments, HW, or operating systems), perfective SW maintenance (implementing new or changed SW functionality) and preventative SW maintenance (preventing the occurrence of SW errors, code optimization, document updating, and code restructuring). The Contractor shall support the design, development, implementation, and documentation of Modeling and Simulation (M&S) systems, SW, research efforts, and related processes including system interoperability. The Contractor may also perform documentation support, integrated product team (IPT) support and configuration management support that is incidental and integral to the SW Maintenance support tasks. Specific SW Maintenance support may include but not be limited to:

a. Developing SW using high order languages that is efficient, readable, and well documented.

b. Preparing reports describing status of SW under development.

c. Suggesting solutions to problems that arise during the development or modification of simulation related real-time computational systems.

d. Analyzing requirements and preparing a SW design approach for the proposed training system(s). Provide alternative design approaches with tradeoff analyses and risk assessments.

e. Assist in reviewing SW and code reviews.

f. Monitoring and adhering to the SW configuration management practices.

g. Identifying problems encountered in SW development and providing recommendations as to how to resolve these problems.

h. Providing support in developing test plans and when needed, providing support for ISEO developed modifications.

i. Actively maintaining and enhancing job related knowledge and skills in M&S, SW development techniques, state-of-the-art computer architectures, emerging technologies, and other SW development areas.

j. Applying decision analysis techniques to ensure that the engineering approach satisfies the training objectives.

3.2.2 Primary Task HW O&M Support).

The Contractor shall assist the Government ISEO with HW development, operation, maintenance and repair efforts. These include: design, prototype, manufacture, installation, modification, and testing of training device mechanical, electrical, electronic, optical, and electro-mechanical components and systems.

3.3 Computer/Electronics Support.

The Contractor shall support computer/electronics efforts for training and simulation systems for programs as follows:

a. Developing SW and HW techniques for simulation, training, and simulation-based acquisition applications.

b. Recommend most suitable technical approach taking into consideration the proposed approach to the problem, personnel, and facilities to be used. Monitor and evaluate the progress of applied research and advanced development requiring the application of new techniques or methods. Render solutions concerning the applicability of technical methodology used, degree of conformance to requirements, and overall project performance.

c. Maintain current awareness of technological developments in the use of computer SW and HW in the technology base for simulation, modeling, and training research investigations. Evaluate technology to predict and optimize effectiveness in training systems; e.g., scene rendering SW, graphics accelerators, database modeling SW and techniques, sensor simulation integration, human animated characters, and weapon tracking systems.

3.4 Minor Support Tasks.

Minor support tasks include configuration management, technical support, Engineering Change Proposal (ECP) support for the Program Manager Air (PMA) groups, IPT support, Fleet Synthetic Training (FST) support, and Cyber Security support of training devices, documentation support, and supply support for the purchase and installation of incidental material, as well as the associated management and administrative support.

3.4.1 Documentation Development and Maintenance Support.

The Contractor shall assist the Government ISEO in:

a) Developing documentation updates for approved trainer system modification efforts.

b) Updating the content of training systems technical data affected by modification, including: Engineering documents; engineering drawings and associated lists; testing procedures; O&M manuals; instructor handbooks; SW user's handbooks; Commercial Off-the-Shelf (COTS) and vendor manuals; and diagrams, flowcharts, drawings, and other graphically-represented data.
c) Developing and maintaining quality control policies and procedures for trainer technical data changes and revisions, and update the Technical Data Package Quality Plan.
d) Supporting the development and maintenance of a relational database management application that is adaptable to rapid expansion, and provides status and cross-reference capability of the technical data.
e) Maintaining and providing physical and configuration control of documentation, data, and media in the technical library.
f) Converting documentation to portable electronic media. Updated and new documentation and drawings shall be produced using desktop publishing and drafting applications on computer systems provided.

3.4.2 Fabrication Support.

The Contractor shall assist with the building, fabrication, testing, evaluation, and operation of reduced and full-scale models, mock-ups, prototypes, and pre-production units. This includes support of fabrication and machining of trainer parts or equipment for fielded systems using traditional materials as well as new composite materials. This task is for support only and would be carried out using Government owned tools and Government purchased materials.

3.4.3 Configuration Management (CM) Support.

The Contractor shall assist the Government ISEO in applying engineering 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. This applies to Information System HW and SW items. The Contractor shall provide CM support for HW and SW Documentation baselines as follows:

a. Provide support in developing and maintaining SW, HW, and technical data configuration management policies and procedures, and perform CM planning for SW, HW, and technical data. The Contractor shall maintain Configuration Management Plans, Configuration Status Accounting (CSA) and other databases.
b. Implement the configuration management procedures established in the Government ISEO's Configuration Management Plan for identification, evaluation, documentation and control of training system modifications.
c. Use Government-developed or owned commercial SW tools to implement automated/electronic change management, configuration control, and archive procedures for trainer system and other configuration items.
d. Develop and maintain SW build procedures for each device. This includes all procedures required to edit, compile, assemble, build, and link the SW undergoing development or modification. Archive the documented procedures and maintain the sources for each program revision.

e. Support trainer SW releases by preparing cold start SW kit and the Computer SW Product End Items for each device.

3.4.4 Interoperability Support/Fleet Synthetic Training (FST) Support.

The Contractor shall provide support to FST efforts. The Contractor shall perform the following work:

a. Provide technical support to Navy Warfare Development Command (NWDC, Navy Continuous Training Environment (NCTE) and Aviation Distributed Virtual Training Environment (ADVTE) engineers to troubleshoot problems encountered with connectivity issues and new trainer capabilities.
b. Provide technical support to ensure successful integration and performance of the training device during actual FST events.

3.4.5 Supply and Provisioning Support.

The Government ISEO is responsible for decision-making pertaining to determining the supplies or services to be acquired by the Government. The Contractor shall support the Government ISEO in the procurement or requisition of equipment, parts, SW, and documentation related to trainer O&M of Platform IT or ISEO operations. This may include, but is not limited to, order processing, order tracking, inspection of goods received, and inventory management.

3.4.6 Cyber Security and Network and Computer Systems Support.

The Contractor shall assist the Government ISEO in the administration, general maintenance and Cyber Security of networks and computer systems HW and SW for assigned training devices and off-line development systems. The Contractor shall assists in collecting, organizing, and analyzing network and computer systems data.

3.4.6.1 Cyber Security and Network and Computer Systems Administration Support for Level I Computing Environments.

The Contractor shall assist the Government ISEO by providing appropriately certified personnel to support network and computer systems administration efforts as follows:

a. Perform O&M of networks, servers, and client workstations.
b. Install configure, maintain, and administer networks, network devices, client machines, and servers.
c. Answer technical queries, maintaining security posture, monitor systems security, documenting system configuration, and conduct performance tuning.
d. Procure and repair components necessary to maintain network and information technology systems.

e. Conduct systems analysis and summarize the data collected in a technical document written in a manner that is understood and usable by the decision makers.

f. Maintain system backups.

g. Recognize/Examine a potential security violation, take appropriate action to report the incident as required by regulation, and mitigate any adverse impact and preserve evidence.

h. Apply instructions and pre-established guidelines to perform Cyber Security tasks within the computing environment (CE).

i. Provide end user Cyber Security support for computer environment systems, peripherals, and applications.

j. Perform routine audits of systems and software, adding, removing, or updating user accounts information, and resetting passwords.

k. Install and operate the Network and computer systems in a test configuration manner that does not alter the program code or compromise security safeguards.

l. Develop and implement access control lists on switches and other network devices.

m. Comply with system termination procedures and incident reporting requirements related to potential CE security incidents or actual breaches.

n. Implement applicable patches including Information Assurance Vulnerability Alerts (IAVA), Information Assurance Vulnerability Bulletins (IAVB), Tenable Plugin IDs, Common Vulnerabilities and Exposures (CVE), and Execute Orders (EXORD) for CE commercial off the shelf (COTS) items.

o. Conduct the installation of security patches, remediation of vulnerabilities and reporting of patch compliance. Advise on security patches and remediation.

p. Assist in the mitigation and closure of open vulnerabilities under the system's change control process.

q. Execute Assessment and Authorization activities in coordination with the Information Systems Owner and Information Systems Security Officer/Manager.

r. Perform cybersecurity testing and vulnerability assessments using Assured Compliance Assessment Solution (ACAS), Security Compliance Checker (SCC), Security Compliance Assessment Protocol (SCAP), Security Technical Implementation Guides (STIG), Security Requirements Guides (SRG), Evaluate-STIG, and STIG Viewer, as required.

s. Assist the government in managing life cycle requirements including IAVM support, remediation, patching, vulnerability scanning utilizing tools (such as Assured Compliance Assessment Solutions (ACAS), Security Content Automation Protocol (SCAP), and RMF Automation Tools, and systems hardening through DoD Security Requirements Guides (SRGs) and DoD Security Technical Implementation Guides (STIGs) implementation.

t. Perform maintenance and cybersecurity monitoring of Endpoint Security Solution (ESS).

u. Ensure compliance with Department of the Navy Application & Database Management System (DADMS) validation requirements for COTS and Government off the shelf (GOTS) SW products used in the CE. Request a Government-sponsored DADMS access account.

v. Provide ISEO and ISSO cybersecurity support for computer environment systems, peripherals, and applications supporting ATO, ASR, and other inspection activities.

w. Assist with any security testing required as part of A&A or annual security reviews.

x. Perform vulnerability-level risk assessment, and make data entries into the eMASS record and systems POA&M consistent with implementation results Design system architectures

y. Design and document network architectures comprised of network topologies, network devices, client machines, and servers.

z. Investigate, recommend, implement, and support application packages.

aa. Recommend procurement and repair of components necessary to maintain the network and information technology systems.

bb. Conduct systems analysis and produce specific charts, graphs, databases, or other documentation that summarize the data collected in a manner that is understood and usable by the decision makers.

cc. Ensure that network device program activities are conducted for the network control devices (e.g., firewalls, routers, switches), in accordance with (IAW) DOD Cyber Security policy and organization specific guidelines, including maintaining configuration of network control devices IAW Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIGs) and National Security Agency (NSA) security guidelines to protect the network control devices from unauthorized access.

dd. Support ISEO in tracking, implementing, and assessing network(s) for changes and updates made to the network control devices, and boundary protection devices, to ensure integrity IAW the system/site Configuration Management Plan.

3.4.7 IPT Support for SW Maintenance of Fielded Platform IT Training Systems.

The Contractor shall provide IPT support for operation, maintenance, cybersecurity sustainment and, repair of identified trainer(s). Specific support may include:

a. Analyzing and assisting in identifying facility requirements such as size of buildings, air conditioning, electrical power and grounding, raised flooring, etc. to satisfy training requirements.

b. Analyzing and assessing Engineering Change Proposals (ECP), Airframe Changes (AFC), Rapid Action Maintenance/Minor Engineering Changes (RAMECs), Training Equipment Change Directives (TECDs), Training Equipment Change Requests (TECRs), and other requirement documents to determine the validity, feasibility, resource requirements, and any potential impact to training systems.

c. Providing support in engineering specifications detailing design, performance, testing, and provisions for the acceptance of the engineering changes.

d. Recommending changes to the Government for training systems contract based on revisions to military training characteristics, changes to performance characteristics, or for pre- planned product improvements.

e. Identifying problems being encountered in HW and SW development and provide recommendations as to how to resolve these problems.

f. Assisting the Government with acceptance testing. This support can range from small modifications to full complex training system with motion platforms. Assist with performing and documenting SW cold starts and other SW related system testing.

g. Analyzing potential requirements for modifications on training systems in the operational phase of the training system and provide recommendations to the Government. This involves extensive research and coordination, including direct contact with fleet activities, Government laboratories, and device/system users.

h. Assist in reviewing Contractor's data deliverable (CDRL items) and internal SW work products (e.g. System Engineering Plan, SW Development Plan, System and SW Requirement Specs, System and SW Design Descriptions, SW Test Plans/Procedures, and other Technical Reports).

i. Attend and contribute functional expertise in appropriate meetings.

j. Monitoring and evaluating SW metrics data for trends, deviations, and compliance.

k. Monitoring the SW preliminary and detailed design process and related work products generated in the training system.

l. Monitoring and participate in the SW Physical Configuration Audit.

m. Assisting in identifying problems being encountered in HW and SW development and provide recommendations as to how to resolve these problems.

n. Assisting in the analysis of potential HW and/or SW requirements for modifications on training systems in the operational phase of the training system. This involves extensive research and coordination, including direct contact with fleet activities, Government laboratories, and device/system users.

3.5 Emerging Projects.

Emerging Projects are short duration, completion support efforts consisting of Training System Modifications for specific training platforms as requirements arise. Typical Emerging Projects include but are not limited to support with: Safety modifications, Computer Operating System upgrades, Service Life Extension Programs (SLEP), Rapid Action Maintenance/Minor Engineering Change Proposals (RAMECs), Training Equipment Change Requests (TECRs), Training Equipment Change Directives (TECDs), and Airframe Changes (AFC). Emerging Projects may be required over the course of the entire contract.

4. Administration.

4.1 Contractor Management.

The Contractor shall organize, coordinate, and control all Contractor activities to ensure compliance with contract performance, cost, and schedule requirements. The Contractor shall monitor the progress of all work performed and all costs incurred under the contract. The COR or Government Project Manager may request that the Contractor provide a Plan of Action and Milestones (POA&M) for task completion. The POA&M shall define the Contractor's methods and schedule for implementing the tasks as specified in this SOW. The contractor shall furnish the POA&M as part of the Contractor's Progress, Status, and Management Report. The Contractor shall prepare the Contractor's Progress, Status, and Management Report in accordance with the Contract Data Requirements List (CDRL B001).

4.1.1 Contractor Administrative Control and Supervision.

Contractor employees shall be under the administrative control and supervision of designated contractor supervisors, site leads, and relief supervisors, and shall perform the tasks prescribed herein. The contractor shall not supervise, direct, or control the activities of NAWCTSD personnel or the employees of any other contractor. The government will not exercise any supervision or control over the contractor employees in performance of contractual services under the contract, and the contractor is accountable to the government for the actions of its contractor personnel.

4.1.2 Contractor Program Manager/On Site Supervisors.

The contractor shall designate a primary Program Manager (PM). The contractor shall identify the PM to the NAWCTSD COR during mobilization and when PM personnel changes occur. The contractor is responsible for delegating team lead and supervisory authority to its workforce members in order to manage the work and internal QA responsibilities. Contractor team leads and supervisors shall assume administrative duties and responsibilities assigned to them by the primary contractor site supervisor to include daily verification of hours worked and tasks assigned. Contractor team leads and/or supervisors shall assign and manage government tasks.

4.2 Non-Personal Services.

The Government will neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. It shall be the responsibility of the Contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the Contractor believes that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's responsibility to notify the PCO immediately. The tasks are broadly defined in the detailed support requirements in Section 3.0 of this SOW.

4.3 Post Award Conference (PAC).

The first conference will be the PAC, which will be held on or about 15 days after contract award. The contractor shall coordinate the date with the COR to establish the framework for contractor and government interaction during the performance period of the contract, as well as introduce contractor and government personnel, discuss contract overview details of the upcoming effort, and resolve any concerns that may arise as a result of the discussion. Additionally, the contractor shall discuss the proposed mobilization approach with the government team. The conference will be held at a place TBD after contract award. The contractor shall prepare presentation materials and conference minutes for the PAC in contractor format. The contractor shall prepare a presentation to include:

a. Introduction.

b. Personnel assignment status and training status for each position required by the SOW.

c. Task management QA process and personnel hiring QA process.

d. Program-specific OPSEC and cybersecurity implementation plans.

e. Updated team contact list (names, IPT memberships, phone numbers, and email address).

f. Metrics collection process, analysis, and reporting.

4.4 Mobilization.

The mobilization period begins 60 days prior to the Contract Start Date (CSD). The contractor shall use this period to hire and train personnel, obtain appropriate security clearances, obtain base and building entry passes, and be prepared to begin contract execution on the CSD. All personnel shall be hired, trained, and in place by the completion of the mobilization period. Upon completion of the mobilization period, the contractor shall assume full responsibility for all tasks. During this period, as an On-The-Job Training (OJT) function, the contractor may observe all tasks being performed by the transitioning contactor, provided that observation does not interfere with ongoing services. The contractor will conduct an on-site mobilization review 30 days after contract award to discuss readiness to assume responsibility for full performance of contractual requirements. The contractor shall prepare meeting minutes for the on-site mobilization review in accordance with the Contractor Provided Meeting Minutes Format (CDRL, B002). **The contractor shall deliver personnel qualifications (including resumes) to the COR no later than 30 calendar days prior to Contract Start Date (CSD).**

4.5 Transition.

The Contractor shall ensure an orderly transition of contract responsibilities to the successor Contractor during the last 30 calendar days of contract performance and minimize impact on the Government. As an On-the-Job Training (OJT) function throughout the transition phase, the Contractor shall allow the successor contractor to observe (over-the-shoulder) the performance of all SOW efforts.

The Contractor shall keep the Government fully informed of status throughout the transition period. Throughout the transition period, it is essential that attention be given to minimize interruptions or delays to work in progress that would impact the mission. The Contractor shall cease operations and vacate all facilities by 2400 (midnight) on the last day of contract performance.

4.6 Federal Holidays.

Normally, the contractor will not provide services on the following federal holidays: New Year's Day, Martin Luther King Day, Presidents' Day, Memorial Day, Juneteenth Day, Independence Day, Labor Day, Columbus Day, Veterans' Day, Thanksgiving Day, and Christmas Day. When a holiday occurs on a Saturday, federal employees are normally granted the previous Friday as the holiday observance period. When a holiday occurs on a Sunday, federal employees are normally granted the following Monday as the holiday observance period. There are occasions when the site may reduce operations in conjunction with the following holidays: Thanksgiving Day, Christmas Day, and New Year's Day, which encompass additional non-holiday work days and weekends. When such a notice is given, the contractor shall modify the support level for the reduced operations.

4.7 Personnel Appearance & Standards of Conduct.

Contractor personnel performing on a military installations shall comply with all applicable rules, regulations, directions, and requirements pertaining to conduct of personnel on a military installation. Professional clothing similar to that of the government civilians at the site is required at all times. The Contractor shall recognize the authority of the military Commander to suspend, restrain, or restrict the activities of Contractor personnel for the protection of personnel and equipment under his military jurisdiction. Contractor personnel shall wear a Contractor-provided identification badge and a "Navy Contractor Badge" while performing work for the Navy. Contractor personnel shall identify themselves as a Contractor in all verbal and written communication means while performing work for the Navy. When attending meetings in support of the Navy, Contractor personnel shall introduce themselves as a Contractor employee working for the Navy.

4.8 Installation Closure.

In the event that an unforeseen installation closure occurs on a regular work day, the Contracting Officer's Representative (COR) will have the option to reschedule the work on any day that is mutually satisfactory to the contractor and the PCO. When a closure occurs personnel shall secure material, equipment, vehicles, and buildings, as determined by installation management.

4.8.1 Severe Weather Closure.

In the event of closings due to severe weather or other hazardous situations, the TPOC will provide notification of any action required to the contractor's designated POC.

4.9 PKI Certification.

The Government will provide PKI Certification for Contractor personnel, if necessary.

4.10 Travel and Material.

When applicable, the Contractor shall be responsible for conducting trips necessary or purchasing materials necessary to accomplish the tasks identified herein. Travel shall be reimbursed IAW Joint Travel Regulation Requirements (JTR). Contractor personnel may be required to travel on average 10% of the time up to 40%. Contractor personnel required to support travel for overseas site surveys shall obtain passports prior to required travel dates (Assumes 60 day prior to travel notification by the Government). Additionally, other travel, such as conference attendance and associated costs necessary to support the tasks identified herein may be required.

The Contractor shall obtain all other material necessary to complete scheduled work requirements via the DoD supply system to the maximum extent possible. When material and shipping cannot be provided by the DoD supply system in time to meet established scheduled requirements the Government may authorize the Contractor to purchase the required item or shipping.

4.11 Training.

SWMFTS contract personnel will be required to complete specific government or NAVAIR mandated training annually, such as Cyber Awareness training, NCIS Counter-Intelligence training, Internet Policy, etc.

5. Logistics.

5.1 Telephones, Computers, and Navy Marine Corps Intranet (NMCI) Accounts.

NMCI accounts and computers shall be the responsibility of the Government to provide, as needed. All government business shall be conducted on NMCI assets. The contractor shall be responsible for protection and care of the computer asset.

5.2 Materials and Shipping.

The Government will provide the office spaces, desks, chairs, computers, printers, paper and pens that are necessary for the performance of this contract. The Contractor shall obtain all other material necessary to complete scheduled work requirements via the DOD supply system to the maximum extent possible. When material and shipping cannot be provided by the DOD supply system in time to meet established scheduled requirements the Government may authorize the Contractor to purchase the required items or shipping. Incidental Materials and Shipping include the purchase or repair of items incidental to the Platform IT SW and HW O&M Support including, but not limited to, damaged end items, damaged components, parts, batteries, memory, repair kits, hard drives and SW licenses. The Government may provide the Contractor with authorization to utilize Federal Supply Schedules for commercial material purchases in accordance with FAR Clause 52.251-1 in support of tasking in the SOW. All incidental material and shipping purchases will be approved in accordance with **CTXT.242-9520 PROCEDURES AND APPROVALS REQUIRED PRIOR TO INCURRING DIRECT MATERIAL COSTS (APR 2022).**

5.3 Computer Proficiency.

At a minimum, all Contractor personnel shall be proficient in the use of electronic and SW tools including Microsoft Office. Contractor personnel shall rapidly learn to use any new electronic tools or SW tools provided including but not limited to: compilers and automated Configuration Management (CM) tools.

6. Reports.

6.1 Conferences and Meetings Support.

The Contractor shall attend meetings, generate minutes, and/or track action items generated using a Government approved tracking system. The Contractor shall prepare meeting minutes in accordance with the Contractor Provided Meeting Minutes Format (CDRL, B002). The Contractor shall also provide status of action items in the Contractor's Progress, Status, and Management Report (CDRL B001).

6.2 Delivered Data.

Data shall be delivered IAW the attached CDRLs, DD Forms 1423, which cite the DIDs or other appropriate reference for technical data and other information required during the performance of this contract.

7. Security.

7.1 Security Requirements for Classified Programs.

The contractor is required to possess a Top Secret (TS) Facility Clearance (FCL) in accordance with the National Industrial Security Program Operating Manual (NISPOM) Chapter II at proposal time (see https://www.dss.mil/ma/ctp/io/fcb/nisp/). The contractor shall safeguard classified information and meet the security requirements identified in the DD Form 254. The contractor shall enforce these safeguards throughout the life of the contract including the transport and delivery phases. Most of the position/labor category equivalents require a Secret Security clearance at a minimum. Historically, Whidbey Island has had TS requirements and it is anticipated that TS personnel requirements will be needed at NAS Jacksonville and other sites. Some positions/ labor categories in the future may require a Top Secret Security clearance that personnel shall attain prior to reporting on-site for work.

The Contractor shall have a Department of Defense (DoD) Top Secret clearance with Director, Central Intelligence Directorate (DCID) 6/4 eligibility for SCI to fulfill the requirements specified in the contract. A Top Secret Facility Clearance is required at the time of proposal submittal.

Distribution of program documentation provided to the Contractor is authorized only with written approval from both the originating activity, and the platform Program Office. The Contractor shall not publicly release any unclassified documentation without written approval from the COR. The Contractor shall provide internal distribution of unclassified documents only to those personnel with a need-to-know. The Contractor shall not release documentation related to the platform to any foreign nationals. At the completion of the contract, the Contractor shall properly dispose of all documentation in accordance with the Contractor's facility security guidelines and Government Standard Operation Procedures (SOP).

The Contractor shall control all classified documents, SW, or HW received, or generated as part of this contract in accordance with current National Industrial Security Program (NISP) guidelines.

7.2 Operations Security (OPSEC).

The contractor shall develop, implement, and maintain an OPSEC program to protect controlled unclassified and classified activities, information, equipment, and material used or developed by the contractor and any subcontractor during performance of the contract. Guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring are provided in NIST SP 800-37. This program may include Cybersecurity and Communications Security (COMSEC). The OPSEC program shall be in accordance with National Security Decision Directive (NSDD) 298. If the contractor does not have an established OPSEC Plan that addresses the protection of classified information, critical information, sensitive, proprietary, or controlled unclassified information, the Government will provide a template for the Contractor's internal development of an OPSEC Plan. Additional OPSEC program planning guidance can be found in DI-MGMT-80934C, OPERATIONS SECURITY (OPSEC) PLAN and NAVAIR OPERATIONS SECURITY (OPSEC) REQUIREMENTS (attachment). The OPSEC program, at a minimum, shall include:

a. Assignment of responsibility for OPSEC direction and implementation

b. Issuance of procedures and planning guidance for the use of OPSEC techniques to identify vulnerabilities and apply applicable countermeasures

c. Establishment of OPSEC education and awareness training to include Basic OPSEC training, produced by the Interagency OPSEC Support Staff (IOSS), which can be found at https://www.iad.gov/ioss/department/opsec-fundamentals-course-opse1300-opse1301-opse1300e-10045.cfm (OPSE1301 OPSEC Fundamentals)

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

e. Flow down of OPSEC requirements to subcontractors when applicable

7.3 Unclassified Contractor-Owned Network Security - Safeguarding of Unclassified Controlled Technical Information (CTI).

The safeguarding of Unclassified CTI applies to prime contractors and their subcontractors (if applicable) for information resident on or transiting through contractor unclassified information systems. The contractor shall provide security to safeguard controlled unclassified technical information on their unclassified information systems from unauthorized access and disclosure. The contractor shall take means (defense-in-depth measures) necessary to protect the confidentiality, integrity, and availability of Government Unclassified CTI.

a. The contractor shall manage and maintain contractor-owned unclassified IT network assets used to process U.S. Government controlled unclassified information (sensitive information) IAW FAR 252.204-7012.

b. The Contractor shall prevent U.S. Government Unclassified CTI from being placed or stored on peer-to-peer applications or social media applications on Contractor owned networks, including IT assets provided to Contractors in a Teleworker status.

c. The Contractor shall manage and control networks (which contain U.S. Government Unclassified CTI serving in a Continuity of Operations (COOP) capacity to meet the same personnel and security requirements identified in this SOW.

1) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or

2) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and

a. Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of FAR 252.204-7012, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

b. Minimum required security controls for Unclassified CTI requiring safeguarding. (A description of the security controls is in the NIST SP 800-53.

Table 1 - Minimum Security Controls for Safeguarding

Access Control	Audit & Accountability	Identification and Authentication	Media Protection	System & Comm Protection
AC-2	AU-2	IA-2	MP-4	SC-2
AC-3(4)	AU-3	IA-4	MP-6	SC-4
AC-4	AU-6(1)			

AC-6
AC-7
AC-11(1)
AC-17(2)
AC-18(1)
AC-19
AC-20(1)
AC-20(2)
AC-22
	AU-7
	AU-8
	AU-9
		IA-5(1)	Physical and Environmental Protection
			PE-2
			PE-3
			PE-5
				SC-7
				SC-8(1)
				SC-13
				SC-15
				SC-28

	Configuration Management CM-2 CM-6 CM-7 CM-8	Incident Response IR-2 IR-4 IR-5 IR-6	Program Management PM-10	System & Information Integrity SI-2 SI-3 SI-4
Awareness & Training AT-2	Contingency Planning CP-9	Maintenance MA-4(6) MA-5 MA-6	Risk Assessment RA-5	

c.

Legend:	
AC: Access Control	MA: Maintenance
AT: Awareness and Training	MP: Media Protection
AU: Auditing and Accountability	PE: Physical & Environmental Protection
CM: Configuration Management	PM: Program Management
CP: Contingency Planning	RA: Risk Assessment
IA: Identification and Authentication	SC: System & Communications Protection
IR: Incident Response	SI: System & Information Integrity

7.4 Cyber Incident and Compromise Reporting.

The contractor shall report to DoD certain cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems set forth IAW FAR 252.204-7012. The contractor shall also provide the report to the NAWCTSD Contracting Officer, NAWCTSD Security Manager, and the NAWCTSD Information Systems Security Manager (ISSM).

7.4.1 Reportable Cyber Incidents.

Reportable cyber incidents include the following:

a. A cyber incident involving possible exfiltration, manipulation, or other loss or compromise of unclassified controlled technical information resident on or transiting through Contractor's, or its Subcontractors', unclassified information systems.
b. Activities that allow unauthorized access to the Contractor's unclassified information system on which unclassified controlled technical information is resident on or transiting.

7.4.2 Contractor actions to support DoD damage assessment.

In response to the reported cyber incident, the Contractor shall:

a. Conduct further review of its unclassified network for evidence of compromise resulting from a cyber-incident to include, but is not limited to, identifying compromised computers, servers, specific data and users accounts. This includes analyzing information systems that were part of the compromise and other information systems on the network that were accessed as a result of the compromise;

b. Review the data accessed during the cyber incident to identify specific unclassified controlled technical information associated with DoD programs, systems or contracts, including military programs, systems and technology; and

c. Preserve and protect images of known affected information systems and all relevant monitoring and packet capture data for no less than 90 days from the cyber incident to allow DoD to request information or decline interest.

7.4.3 DoD damage assessment activities.

If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor point of contact identified in the incident report provide all of the damage assessment information gathered in accordance with DFARS 252.204-7012. The Contractor shall comply with damage assessment information requests. The requirement to share files and images exists unless there are legal restrictions that limit a company's ability to share digital media. The Contractor shall inform the Contracting Officer of the source, nature, and prescription of such limitations and the authority responsible.

7.4.4 Protection of reported information.

Except to the extent that such information is lawfully publicly available without restrictions, the Government will protect information reported or otherwise provided to DoD in accordance with applicable statutes, regulations, and policies. The Contractor shall identify and mark attribution information reported or otherwise provided to the DoD. The Government may use information, including attribution information and disclose it only to authorized persons for purposes and activities consistent with DFARS 252.204-7012.

7.4.5 Information Security Requirements for Protection of Unclassified DoD Information On Non-DoD Systems.

The Contractor shall safeguard unclassified DoD information stored on non-DoD information systems to prevent the loss, misuse, and unauthorized access to or modification of this information. Protection of unclassified DoD information not approved for public release on non-DoD Information Systems will be protected IAW DoDI 8582.01, Security of Unclassified DoD Information on non-DoD Information Systems. The Contractor shall:

a. Not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

b. Protect information by no less than one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

c. Sanitize media (e.g., overwrite) before external release or disposal.

d. Encrypt the information that has been identified as Controlled Unclassified Information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media, compact disks, using the best available encryption technology.

e. Limit information transfer to Subcontractors or teaming partners with a need to know and a commitment to the same level of protection.

f. Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS).

g. Encrypt organizational wireless connections and use encrypted wireless connection, where available, when traveling. When encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using no less than application-provided password protection level encryption.

h. Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

i. Not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

j. Provide protection against computer network intrusions and data exfiltration, including no less than the following:

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

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

    (3) Prompt application of security-relevant SW patches, service packs, and hot fixes.

k. Comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., critical program information, Personally Identifiable Information (PII), export controlled information) IAW the requirements of the contract.

7.5 Access to DoD Installations, Government Information, and Information Technology (IT) Systems. Personnel Security Background Checks and DBIDS.

a. The Common Access Card (CAC) shall be the principal identity credential for supporting interoperable access to DoD installations and access to U.S. Government information systems IAW FAR 52.204-9. The Defense Biometric Identification System (DBIDS) shall be used for contractors and vendors who do not have a CAC, but only requires access to a base/installation Navy command. The Contractor shall first coordinate with the appropriate NAWCTSD Contracting Officer Representative /Technical Point of Contact or government sponsor to request an application to be processed through the specific site Security Office Trusted Agents for issuance of the CAC or via the Trusted Associate Sponsorship System. The base Visitor Control Center representative will process request for installation access using the DBIDS. More information for obtaining the CAC can be found at http://www.cac.mil/common-access-card/getting-your-cac/for-contractors/ and for DBIDS at https://www.cnic.navy.mil/Operations-and-Management/Administrative-Services/Common-Access-Card-Program/

b. Contractor personnel who do not need a security clearance, but require a CAC in performance of their duties (including access to controlled unclassified information, but not access to classified information), shall coordinate with the COR and contractor Facility Security Officer (FSO) to complete a TIER- 3 (T3) background investigation, which includes submission of fingerprints and the Standard Form SF-86 (Questionnaire for National Security Positions). The contractor FSO shall submit the SF-86 to the COR for processing with NAWCTSD or any of the SWMFTS Site Security Offices as required. There shall be no additional T3 submissions for contractors holding a valid national security clearance. The Government may issue the credential upon favorable return of the Federal Bureau of Investigations (FBI) fingerprint check, pending final favorable completion of the T3 investigation.

c. Contractor personnel who require Privileged Access to Fielded Training Device IT root systems in performance of their sensitive duties (including access to Unclassified CTI), shall coordinate with the COR and contractor FSO to complete a TIER- 5 (T5) background investigation. There shall be no additional T5 submissions for contractors holding a valid national security clearance. The Government may issue the credential upon favorable return of the Federal Bureau of Investigations (FBI) fingerprint check, pending final favorable completion of the T5.

d. A T5 background investigation is conducted on each military, civilian, and contractor occupying a Special Sensitive (SS) or Critical Sensitive (CS) position or requiring continued national security eligibility at an equivalent level will undergo a T5 review every five years. The T5 review is also required to support personnel security determinations on personnel with continued assignment to NATO billets requiring TS Constellation Observing System for Meteorology, Ionosphere, and Climate (COSMIC) access, Nuclear Weapons PRP, privileged access IT supporting domain/root level administrator positions (See SOW Section 7.5.3), Presidential Support Activities (PSA), access to INC-2, and for Limited Access Authorizations (LAAs) for non-U.S. citizens employees. The T5 investigative elements include: a National Agency Check (NAC) (except that a technical fingerprint check of FBI files is not conducted), a subject interview, a credit check, an employment check, neighborhood interviews, local agency checks, interviews of employers and developed character references, an ex-spouse interview, and additional investigation when warranted by the facts of the case.

e. Access to restricted areas, controlled unclassified information or Government Information Technology by contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a T3 investigation for Secret Restricted areas, T5 for Top Secret Restricted areas or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a T3/T5 as applicable shall be initiated by the contractor FSO and favorably reviewed by the appropriate DoD component, agency, or activity prior to permitting such access.

f. The contractor shall comply with the Cybersecurity and personnel security requirements for accessing U.S. Government IT systems specified in the contract. The contractor shall review and become familiar with the credentialing standards presented in OPM Memorandum for Issuing Personal Identity Verification cards to use as an aid in their employee selection process. The site Security Office will apply the credentialing standards and execute the credentialing process for individual contractors.

7.5.1 Access to restricted areas, controlled unclassified information (sensitive information), or Government Information Technology.

Access to restricted areas, controlled unclassified information (sensitive information), or Government Information Technology by Contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a T3/T5 as appropriate or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a T3/T5 as applicable shall be initiated by the contractor's FSO and favorably reviewed by the DoD component, agency, or activity prior to permitting such access.

7.5.2 Contractor access to controlled unclassified information

For Contractor personnel performing sensitive duties including access to controlled unclassified information, but do not have a clearance to access classified information, the Contractor shall use the Standard Form 86 (Questionnaire for National Security Positions) in order to obtain the CAC. The Contractor shall submit the SF 86 to the COR for processing into the Trusted Associate Sponsorship System (TASS) to initiate the CAC issuance process.

7.5.3 Privileged User/Access

A Privileged User is an individual that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform (See reference (t)). Privileged Users operate IT within the authorities vested in them according to DON Cybersecurity policies and procedures, and usually has the following system controls:

- Access to the control functions of the IS/network, administration of user accounts, etc.

- Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key IS/network equipment or software

- Ability and authority to control and change program files, and other users' access to data

- Direct access to OS level functions that permit system controls to be bypassed or changed

- Access and authority for installing, configuring, and monitoring security monitoring functions of Information systems/networks (e.g., network/systems analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operations

- Responsible for the upkeep, configuration, and reliable and secure operations of computers, networks, and information systems

- Responsible for Core Intrusion Detection Systems/Intrusion Prevention Systems functions may also be applicable

7.5.3.1 IT Level-1 positions

IAW DON CIO, and NAVAIR guidance, IT Level-1 positions are defined as users with privileged access. Contractor employees assigned to an IT Level-I designated position with SECRET access will be required to have a favorably adjudicated T5/T5R completed every 5 years. Contractor employees that require a SECRET Clearance as part of their job duties, with IT Level-I designation, will be initiated by the contractor FSO, and will be at the contractors expense. Contractor employees that require a Top Secret Clearance as part of their job duties, with IT Level-I designation, shall be initiated by the Contracting Company.

Any Contractor employee, who has a final clearance and submitted T5/T5R that is accepted by OPM along with a favorable fingerprint check (SAC), is eligible for IT-1 designation. The Command Security Office will review all SF-86 paperwork for all Contractor employees nominated for IT Level-I designations if the T5/T5R is not completed.

Contractor employees that do not have a final clearance investigation within DISS are ineligible for IT Level-I designation until the T5/T5R has been favorably adjudicated and shall not be assigned to a contract position requiring IT Level-I designation.

7.6 Personnel Security - Background Checks.

Contractor personnel shall undergo the company internal vetting process prior to gaining access to U.S. Government controlled unclassified information. To comply with immigration law, the contractor shall use the Employment Eligibility Verification Program (E-Verify) IAW FAR 52.222-54.

7.7 International Traffic and Arms Regulation (ITAR).

The contractor shall ensure that foreign persons, as defined under section 120.16 of the ITAR (22 CFR, Parts 120 – 130), are not given access to U.S. Government controlled unclassified information, sensitive information, defense articles, defense services, or technical data, as defined in the ITAR, Part 120, without proper issuance of an export license from the U.S. Government authority.

7.8 Personnel Security - Reporting of Adverse or Derogatory Information related to Contractors.

The Contractor shall report to the NAWCTSD Security Office adverse or derogatory information pertaining to on-site CSS personnel (when applicable) or contractor personnel in direct support of this contract. Information reported to the Government Contracting Agency shall be integrated and reported in Contractor Performance Assessment Reporting System (CPARS) on contractor performance of Personnel Security (PERSEC) related aspects of contractor performance.

a. Adverse or derogatory information reporting of contractor personnel. Example: Domestic Violence arrest, or other violent or sexual crime arrest or self-report.

b. When contractor personnel receive a revocation of an Interim or denial for the issuance of a CAC until final adjudication

c. When a denial or suspension of clearance occurs for a contractor employee

d. When contractor employee receives a final denial of eligibility for a security clearance.

7.9 Government-Issued Personal Identification Credentials.

The contractor shall account for all forms of U.S. Government-provided identification credentials (CAC or U.S. Government-issued identification badges) issued to the contractor (or their employees in connection with performance) under the contract. The contractor shall return such identification credentials to the issuing agency at the earliest of any of the circumstances listed below, unless otherwise determined by the U.S. Government. The contracting officer may delay final payment under the contract if the contractor or subcontractor fails to comply with these requirements.

a. When no longer needed for contract performance.

b. Upon completion of the contractor employee’s employment.

c. Upon contract completion or termination.

7.10 Contractor “Out-processing” Policy.

The contractor shall have in place (established and enforced) an “out-processing” policy for employees that leave the company, including suspension of account access, return of all PCs, laptops, smartphones, and other electronic devices (Government-furnished IT equipment and contractor-issued IT equipment) that contain U.S. Government Controlled Unclassified Information. The contractor shall also ensure that out-processed employees receive debriefings on the need to maintain confidentiality of U.S. Government Controlled Unclassified Information.

7.11 Supply Chain Risk Management (SCRM) For National Security Systems.

The Contractor shall mitigate supply chain risk in the provision of supplies and services to the Government per FAR 252.239-7018, Supply Chain Risk, and CNSSD -505, Supply Chain Risk Management (SCRM). The contractor shall, implement a process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal.

7.12 Transmission of Controlled Unclassified Information (CUI) via e-mail.

The Contractor shall use approved encryption to safeguard the electronic transmission of all Controlled Unclassified Information. The Contractor shall ensure that when transmitting CUI over non- secure e-mail (e.g. not connected to the Navy Marine Corps Intranet through Broadband Unclassified Remote Access System / Virtual Private network), those transmissions are encrypted using Department of Defense Public Key Infrastructure (PKI), or an approved DoD External Certificate Authority, in accordance with Public Key Infrastructure & Public Key Enabling, DoDI 8520.02, 24 May 2011.

7.13 Transmission of Controlled Unclassified Information (CUI) via S.A.F.E. Safe Access File Exchange (SAFE). SAFE is designed to provide an alternative way to send encrypted files other than email. Information regarding the use of SAFE can be found at https://safe.apps.mil.

The contractor shall ensure the following:

- All files transferred via SAFE shall be for official US Government related business.
- All files transferred via SAFE shall be UNCLASSIFIED.
- SAFE CANNOT be used to transmit classified information
- All files shall be encrypted+

7.14 Privacy Act Compliance.

The Contractor may be in contact with data subject to the Privacy Act (Title 5 of the U.S. Code, Section 552.a). The Contractor shall ensure that employees assigned to this effort understand and adhere to the Privacy Act of 1974. The Contractor shall identify and safeguard reports and data accordingly. The Contractor shall follow agency procedures in compliance with the Privacy Act.

The Contractor shall ensure that Contractor employees assigned to the TO are briefed annually on properly identifying and handling privacy act data and information.

8. Cyber Security (CS).

The Contractor shall comply with DoDI 8500.1, Cybersecurity and Department of the Navy (DON) Cybersecurity (CS) Policy, NAVINST 5239.3C.

8.1 Cybersecurity and Personnel Security Requirements for Accessing Government Information Technology (IT) Systems - Credentialing Standards.

The Contractor shall comply with the Cyber Security and personnel security requirements for accessing U.S. Government IT systems specified in the contract. Contractors requiring access to U.S. Government IT systems will be subject to a background check. The Contractor shall review and become familiar with the credentialing standards presented in OPM Memorandum for Issuing Personal Identity Verification Cards to use as an aid in their employee selection process. The NAWCTSD Security Office will apply the credentialing standards and execute the credentialing process for individual contractors.

Contracted Personnel shall (when required):

a. Complete a System Access Authorization Request-Navy (SAAR-N), Privileged Access Authorization Training (PAA) and complete a PAA Agreement before receiving access to a DOD IT system.

b. For new personnel, provide the Personnel Security information required to the NAWCTSD Security Manager Office in order to validate the SAAR-N application. SAAR-N form shall be submitted to NAWCTSD ISSM for final authorization.

c. Complete the current version of DoD Cyber Awareness Challenge training and the NACWTSD Cybersecurity Training Supplement before requesting access to DoD IT system and each year thereafter. DoD Cyber Awareness Challenge training is available at: https://iase.disa.mil/Pages/index.aspx. The NACWTSD Cybersecurity Training Supplement is provided as GFE.

d. Ensure all media and data storage is properly marked and labeled per lab project manager’s policy and guidance documents (i.e., SECNAV M-5510.36 series).

e. Report cybersecurity incidents and violations to the ISSM.

f. Ensure security of all communications and transmissions of sensitive information in accordance with Navy-approved means and process.

9. Appendix A

The below Labor Categories for services comport to those of the Office of Management and Budget's (OMB) 2018 Standard Occupational Classifications (SOC) published by the Bureau of Labor Statistics (BLS) and the Department of Labor (DOL) Service Contract Act (SCA) Directory of Occupations, Fifth Edition.

Experience and Education Deviations: Any acceptable deviation to the Experience and Education requirements for services is noted in the specific labor category paragraph descriptions.

Personnel Resumes: The contractor is responsible for providing fully qualified and competent employees to perform the scope of the effort set forth herein. The government reserves the right to review the resumes of prospective or current contractor employees to confirm they meet the below work, certification, and education requirements. Accordingly, the contractor shall furnish such resumes upon request by the COR.

NOTE: All education requirements must be from an accredited school or program. To determine if a school or program is accredited, refer to the U.S. Department of Education's Institutional Accreditation System (http:// https://ope.ed.gov/dapip/#/home), which contains information reported directly by recognized accrediting agencies and state approval agencies.

A post-secondary certificate program must have been completed at a qualifying educational institution equivalent to at least one academic year of full-time study that is part of an accredited college-level, technical, trade, vocational, or business school curriculum.

Appendix #	Labor Category	SLC SOC
A.1	Technical Writer III	27-3042
A.2	Technical Writer II	27-3042
A.3	Electronics Technician, Maintenance, III	17-3023
A.4	Drafter/CAD Operator	17-3010
A.5	Documentation Specialist	43-9022
A.6	Software Engineer, Senior	15-1252
A.7	Software Engineer, Journeyman	15-1252
A.8	Software Engineer, Junior	15-1252
A.9	System Administrator, Senior	15-1244
A.10	System Administrator, Junior	15-1244
A.11	Computer Systems Analyst, Senior	15-1211
A.12	Computer Systems Analyst, Journeyman	15-1211

A.13	Computer Scientist, Journeyman	15-1221
A.14	Network Engineer, Journeyman	15-1244
A.15	Engineer/Scientist, Senior	17-2041
A.16	Engineer/Scientist, Journeyman	17-2041
A.17	Engineer/Scientist, Junior	17-2041
A.18	Supply Technician	43-5061
A.19	Information Assurance Analyst, Senior	15-1122
A.20	Information Assurance Analyst, Journeyman	15-1122

A.1 Technical Writer III

a. EDUCATION – Minimum of High School diploma or GED; Vocational training commensurate with Department of Labor functional description as follows: develops, writes, and edits material for reports, manuals, briefs, proposals, instruction books, catalogs, and related technical and administrative publications concerned with work methods and procedures, and installation, operation, and maintenance of machinery and other equipment.

b. EXPERIENCE – Minimum of five (5) years of experience in developing technical manuals, such as system design documents, configuration drawings, operation manuals, maintenance manuals, and training manuals.

A.2 Technical Writer II

c. EDUCATION – Minimum of High School diploma or GED; Vocational training commensurate with Department of Labor functional description as follows: develops, writes, and edits material for reports, manuals, briefs, proposals, instruction books, catalogs, and related technical and administrative publications concerned with work methods and procedures, and installation, operation, and maintenance of machinery and other equipment.

d. EXPERIENCE – Minimum of two (2) years of experience in developing technical manuals, such as system design documents, configuration drawings, operation manuals, maintenance manuals, and training manuals.

A.3 Electronics Technician, Maintenance, III

a. EDUCATION - At a minimum shall be a graduate of an accredited technical or computer school, with related vendor sponsored training classes. May substitute additional four (4) years of relevant work experience for the "graduate of an accredited technical or computer school" requirement.

b. EXPERIENCE - Minimum of seven (7) years relevant work experience in installation, troubleshooting, and maintenance of electronics equipment, and computers in a networked environment.

c. CERTIFICATIONS – Minimum of A+ (ce) or Network+ (ce) (formerly IAT-I certification) in accordance SOW paragraph 3.2.2.

A.4 Drafter/CAD Operator

a. EDUCATION – Minimum of High School diploma or GED.

b. EXPERIENCE - Minimum of five (5) years of relevant progressive work experience in drafting with a professional working knowledge of drafting methods, procedures, and techniques, and use of computer aided design (CAD).

A.5 Documentation Specialist, BLS SOC 43-9022

a. EDUCATION – Minimum of High School diploma or GED.

b. EXPERIENCE – Minimum of 2 years general clerical experience and experience with MS Office, including Excel, Access, Power Point, and Word.

A.6 Software Engineer, Senior

a. EDUCATION - Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, mechanical engineering, or computer science.

b. EXPERIENCE - At least seven (7) years of practical experience in software development.

c. CERTIFICATIONS - Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.7 Software Engineer, Journeyman

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, mechanical engineering, or computer science.

b. EXPERIENCE - At least three (3) years of practical experience in software development.

c. CERTIFICATIONS - Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.8 Software Engineer, Junior

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, mechanical engineering, or computer science.

b. EXPERIENCE- Experience in software development.

c. CERTIFICATIONS – Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.9 System Administrator, Senior

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, computer information systems, computer science, or a B.A. degree in Management Information Sciences. An additional three (3) of related work experience may be substituted for education requirement.
b. EXPERIENCE – Minimum of five (5) years of experience as a network and computer systems administrator.
c. CERTIFICATIONS - Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.10 System Administrator, Junior

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, computer information systems, computer science, or a B.A. degree in Management Information Sciences. An additional three (3) years of related work experience may be substituted for education requirement.
b. EXPERIENCE – Minimum of one (1) year of experience as a network and computer systems administrator.
c. CERTIFICATIONS - Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.11 Computer Systems Analyst, Senior

a. EDUCATION – Minimum of M.S./M.A. degree in electronics engineering, electrical engineering, computer engineering, computer science, mathematics, or physics. A B.S./B.A. degree and an additional four (4) years of experience can be substituted for a M.S. or M.A. degree.
b. EXPERIENCE – A minimum of ten (10) years of experience in the design, integration, and test of systems.
c. CERTIFICATIONS – Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.12 Computer Systems Analyst, Journeyman

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, computer science, mathematics, or physics.
b. EXPERIENCE – A minimum of six (6) years of experience in the design, integration, and test of systems.
c. CERTIFICATIONS - Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.13 Computer Scientist, Journeyman

a. EDUCATION – Minimum of B.S. in Computer Science.
b. EXPERIENCE – At least three (3) years of experience in the application of computer science principles to develop new software and computer hardware solutions.

c. CERTIFICATIONS – Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.14 Network Engineer, Journeyman

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, computer science, computer information systems, or mathematics. An additional three (3) years of related work experience may be substituted for education requirement.

b. EXPERIENCE – Minimum of five (5) years of engineering or network/computer systems administrator experience with at least 1 year of Cyber Security experience.

c. CERTIFICATIONS – Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M and SOW paragraph 3.11.

A.15 Engineer /Scientist, Senior (Hardware Engineer, Senior)

a. EDUCATION – Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, or mechanical engineering.

b. EXPERIENCE - At least six (6) years of hardware design and integration experience.

c. CERTIFICATIONS – Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.16 Engineer/Scientist, Journeyman (Hardware Engineer)

a. EDUCATION - Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, or mechanical engineering.

b. EXPERIENCE - At least three (3) years of hardware design and integration experience.

c. CERTIFICATIONS – Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.17 Engineer /Scientist, Junior (Hardware Engineer, Junior)

a. EDUCATION - Minimum of B.S. in electronics engineering, electrical engineering, computer engineering, aeronautical engineering, aerospace engineering, or mechanical engineering.

b. EXPERIENCE – Experience in hardware design and integration.

c. CERTIFICATIONS – Minimum of Information Assurance Technician (IAT) I IAW DOD 8570.01-M.

A.18 Supply Technician

a. EDUCATION - Minimum of High School Graduate or equivalent.

b. EXPERIENCE – Minimum of five (5) years of experience IAW SOW Paragraph 3.10.

A.19 Information Assurance Analyst, Senior

a. EDUCATION - Minimum of B.S. or B.A. degree in Computer Science, Information Systems or a relevant technical discipline. An A.S. or A.A. degree and an additional three (3) years of experience can be substituted for degree requirement.

b. EXPERIENCE - At least seven (7) years of cyber security experience in secure network and system design, analysis, procedure/test generation, test execution and implementation of computer/network security mechanisms.

c. CERTIFICATIONS – Minimum of DoD Approved Baseline Certification as Information Assurance Technical (IAT) Level II IAW DOD 8570.01-M and SOW paragraph 3.11.

A.20 Information Assurance Analyst, Journeyman

a. EDUCATION - Minimum of B.S. or B.A. degree in Computer Science, Information Systems or a "Relevant Technical Discipline". An A.S. or A.A. degree and an additional three (3) years of experience can be substituted for degree requirement.

b. EXPERIENCE - At least four (4) years of cyber security experience in secure network and system design, analysis, procedure/test generation, test execution and implementation of computer/network security mechanisms.

c. CERTIFICATIONS – Minimum of DoD Approved Baseline Certification as Information Assurance Technical (IAT) Level II IAW DOD 8570.01-M and SOW paragraph 3.11.