STATEMENT OF WORK
SECTION C – DESCRIPTION/SPECIFICATION/WORK STATEMENT

C.1 BACKGROUND

The Naval Surface Warfare Center, Dahlgren Division (NSWCDD) Weapon Control and Integration Department (H), Unmanned & Expeditionary Weapon Systems Division (H40) has a requirement for a contractor to provide system engineering, mechanical engineering, electrical engineering, computer hardware and software engineering, software development, design and technical engineering, configuration management, mechanical and electrical engineering technician services, field service support, project management and project management support functions, and technical writing services to support the H40 Division. The systems supported include combat management systems for air, surface, and ground applications. The current specific systems include systems in the Battle Management System (BMS) portfolio, supporting such platforms as Armada, Armed Overwatch, Combatant Craft Medium (CCM), Denied Area Sprinter - Hellfire (DASH), Expeditionary Launcher Module (ELM), Unmanned Aerial Systems (UAS), Killchain Automation, Littoral Combat Ship Surface to Surface Missile Module (LCS SSMM), Precision Strike Package Precision Guided Weapon (PSP PGW), Precision Strike Package Gun Weapon System (PSP GWS), Rapid Dragon, Rotorcraft, Standoff Precision Guided Munition Development (SOPGM Dev), Surrogate, Swarm Carrier, and Tactical Visualization. BMS Sponsorship consists of Special Operations Command (SOCOM), Department of the Air Force, Air Force Special Operations Command, Department of the Navy, Naval Special Warfare PMS 340, United States Marine Corps, Tactical Airlift Program Office (PMA-207), and the United States Army.

C.2 SCOPE

The Contractor shall support all technical and engineering stages of development, test, integration, and fielding of safe and innovative weapon control systems, detection systems support, advanced weapon systems support, autonomous system support, mechanical and electrical technician support towards assembly and integration. Other duties indirectly supporting these efforts include providing business operational and financial reporting support, writing technical documentation, maintaining technical databases, and editorial support of technical publications. The services necessary to accomplish the tasks within this Statement of Work (SOW) are defined in Section

C.2.1 Applicable Documents

The following documents are applicable to this SOW. The most current versions of these documents are accessible through the internet or will be provided to the Contractor upon request.

Other Department of Defense Specifications/Standards/Other Applicable Documents may become applicable throughout the life of the Task Order and may be added to the Task Order via modification.

DRAFT

The Contractor shall ensure compliance with the most current versions of these documents throughout the life of the Task Order:

Number	Document Name
DODM 8140.03	Cyberspace Workforce Qualification and Management Program
SAE AS5553 (series)	SAE Aerospace Standard 5553
NISPOM – 32 Code of Federal Regulation Part 117	National Industrial Security Program Operating Manual (NISPOM)
NSWCDDINST 5510.4 (series)	NSWCDD Command Security Manual
SEAD-3	Security Executive Agent Directive 3 – Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position
SEAD-3 Implementation Memo	Implementation of Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position
SEAD-4 Implementation Memo	Implementation of Security Executive Agent Directive 4: National Security Adjudicative Guidelines
DODI 5200.48	Controlled Unclassified Information (CUI)
DoDM 5400.07	DoD Freedom of Information Act (FOIA) Program
SECNAVINST 5210.8 (series)	Department of Navy Records Management Program
NSWCDDINST 5100.1 (series)	Occupational Safety and Health Program
NAVADMIN 216/15	Cyber Hygiene Authorization to use Personal Wearable Fitness Devices
NAVSEA S0420-AA-RAD-010 (series)	Radiological Affairs Support Program (RASP) Manual
DODI 8510.01	Risk Management Framework for DOD Systems
CJCSI 6211.02 (series)	Defense Information Systems Network (DISN) Responsibilities
DODM 1000.13	Department of Defense Identification (ID) Cards
NAVSEAINST 4200.19 (series)	Planning, Use and Control of Services Contracting
COMUSFLTFORCOM/ COMPACFLT 6320.3 (series)	Medical Screening for U.S. Government Civilian Employees, Contractor Employees, Guests and Visitors Prior to Embarking Fleet Units
ISO/IEC 15288:2008	Systems and Software Engineering – System Life Cycle Processes
ISO/IEC 26702	Systems Engineering—Application and Management of the SE Process
ISO 16085 DoDI 8500.01	Systems and Software Engineering – Life Cycle Process – Risk Management Cybersecurity
DoDI 8510.01	Risk Management Frameworks (RMF) for DoD Information Technology (IT)

DRAFT

Number	Document Name
DoDD 8140.01	Cyberspace Workforce Management
DoD 8570.01-M	Information Assurance Workforce Improvement Program
DON CIO Memo 01-09	Information Assurance Policy for Platform Information Technology
MIL-HDBK-1568	Military Handbook Materials and Processes for Corrosion Prevention and Control in Aerospace Weapon Systems
AFSC DH 1-6	System Safety
AS50881 SAE	Aerospace Standards, Wiring Aerospace Vehicle
IPC J-STD-001	Soldering Certification
IPC-A-610E	Acceptability of Electronic Assemblies
IPC/WHMA-A-620A	Requirements & Acceptance for Cable & Wire Harness Assemblies
MIL-HDBK-454	General Guidelines for Electronic Equipment
MIL-HDBK-1587	Department of Defense Handbook Material and Process requirement for Air Force Weapon Systems
MIL-HDBK-1791	(USAF) Military Handbook Designing for Internal Aerial Delivery in Fixed Wing Aircraft
MIL-STD-130N	Identification Marking of U.S. Military Property
MIL-STD-188-220	Interface Standard for Digital Message Transfer Device (DMDT Subsystems)
MIL-STD-461	Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility
MIL-STD-462	Test Method Standard for Measurement of Electromagnetic Interference Characteristics
MIL-HDBK-61A (SE)	Configuration Management Handbook
MIL-STD-3046	Configuration Management
MIL-STD-31000A	Technical Data Packages
MIL-STD-464	Electromagnetic Environmental Effects, Requirements for Systems
MIL-STD-704	Department of Defense Interface Standard, Aircraft Electric Power Characteristics
MIL-STD-810	Department of Defense (DoD) Test Method Standard for Environmental Engineering Considerations and Laboratory Tests
MIL-STD-882	System Safety Program Requirements
MIL-STD-1553	Digital Time Division Command/Response Multiplex Data Bus
MIL-STD-1760	Department of Defense Interface Standards for Aircraft/Store Electrical Interconnection System
MIL-STD-2401	DoD World Geodetic System 1984
BMS-CHAR-26-0001	Change Control Board Charter
EXT-CMP-16-0001	Configuration Management Plan
BMS-SCMP-16-0001	Rapid Development Process
BMS-SdP-16-0001	Rapid Development Process
TBD	Software Development Plan (GFCS)
TBD	Software Development Plan (PGW)
TBD	Systems Engineering Plan
TBD	Test & Evaluation Master Plan

DRAFT

C.3 REQUIREMENTS

C.3.1 SYSTEMS ENGINEERING REQUIREMENTS AND PLANNING SUPPORT

C.3.1.1 The Contractor shall provide subject matter expertise and technical recommendations to user and peer reviews, working groups, Change Review Boards (CRB), Design Review Boards (DRB), Change Control Board (CCB), Integrated Product Teams (IPTs), and technical interchange meetings. (CDRL A001x)

C.3.1.2 The Contractor shall identify a range of technically practical engineering approaches and solutions to meet platform integration considerations, weapon systems integration, program/project timelines during engineering solution concept generation, requirements analysis, and enhancement. (CDRL A001x)

C.3.1.3 The Contractor shall develop, generate, analyze and summarize data into reports to provide safe and sound technical knowledge and subject matter expertise into: effectiveness, efficiency and appeal of designated tactical systems to include emerging and existing technologies; tradeoff assessments; studies of new systems and technologies; mission engineering; developmental schedules and timetables. (CDRL A001x)

C.3.1.4 The Contractor shall develop a system, subsystem, and component model, engineering drawing package, Bill of Materials (BOM), or architecture capturing envisioned concepts. (CDRL A00H)

C.3.1.5 The Contractor shall facilitate and document functional and interoperability requirements in Requirement Traceability Matrixes (RTM) and technical specifications. (CDRL A001x, A002x)

C.3.1.6 The Contractor shall facilitate and document the system, subsystem, or component boundaries and interfaces. (CDRL A001x, A00Bx)

C.3.1.7 The Contractor shall design, develop, refine, and provide subject matter expertise into system engineering plans. (CDRL A001x, A002x)

C.3.1.8 The Contractor shall provide subject matter expertise and recommendations to the selection of system, subsystem, or component solutions considering operational needs, system requirements, cost, schedule, test and evaluation strategy, and technology and operational integration risks. The types of systems, subsystems, and components include weapon systems, weapon controls systems, unmanned and manned systems, robotic systems, lethal and non-lethal systems, and advanced sensory systems. (CDRL A001x, A002x)

C.3.1.9 The Contractor shall develop and document reliability, availability, meantime before failure rates (MTFB), sustainability, and maintainability analyses of requirements. (CDRL A001x)

DRAFT

C.3.1.10 The Contractor shall develop and generate system and force level integration plans. (CDRL A001x)

C.3.1.11 The Contractor shall perform requirements assessments and analysis; refine specific lower level technical requirements; analyze and refine weapon system architecture; analyze and refine platform interfaces; develop system behavioral modeling; perform functional analyses and functional flows; document systems baselines; and perform system performance interface and interoperability test and analyses. (CDRL A001x, A002x)

C.3.1.12 The Contractor shall coordinate Government inputs, generate and deliver program weekly reports, monthly reports, program review presentations, and program status updates and highlights that support program management. The Contractor shall generate, update and maintain project Action Items (AIs) relative to Integrated Product Teams (IPTs) and Working Groups (WGs). The Contractor shall develop and distribute meeting minutes assigned by the designated IPT or WG lead. (CDRL A003x)

C.3.1.13 The Contractor shall generate, update, and maintain Point of Contact (POC) listings for IPT, WG, inventories, and procurements in process, procurement actions, and organizational matrices with locations. (CDRL A00Rx)

C.3.1.14 The Contractor shall prepare publication of documents through the NSWCDD public document process. The Contractor shall submit and track the release of the approval process. The Contractor shall generate, bring up to date, and maintain Integrated Master Schedules (IMSs), identifying resources, critical path items, addressing schedule conflicts and risks, and synchronizing the IMS with other project IMSs across the program's portfolio. (CDRL A002x)

C.3.1.15 The Contractor shall consolidate weekly IPT information from different projects into singular and centralized program portfolio reports. (CDRL A002x)

C.3.2 SYSTEMS ENGINEERING DESIGN SUPPORT

C.3.2.1 The Contractor shall develop and refine designs for systems, subsystems, components, and interfaces for new and existing weapons systems, manned and unmanned systems, lethal and non-lethal systems, robotic systems, and weapon control systems. (CDRL A001x, A002x, A00Cx)

C.3.2.2 For hardware designs, the Contractor shall generate design models; drawings; specifications; interface control documents; and the appropriate technical and integration data, analyses, and technical documentation to support engineering design decisions. (CDRL A001x, A002x, A00Cx)

C.3.2.3 For software designs, the Contractor shall generate design data; specifications; interface control documents; software description documents; software version description documents; code; and the appropriate technical and integration data, analyses, and documentation to support engineering decisions. The Contractor shall derive and implement lower level requirements from system and software requirements specifications. (CDRL A001x, A002x, A00Tx, A00Ux)

DRAFT

C.3.2.4 The Contractor shall refine hardware and software designs for, weapons, manned and unmanned systems robotic systems, lethal and non-lethal systems, and weapon control systems, subsystems, and components to document the appropriate product baseline for production and resolve deficiencies discovered during the manufacturing process and user operation. The Contractor shall provide subject matter expertise and recommendations on system, subsystem, and component readiness for initial outfitting and system deployment. (CDRL A001x)

C.3.2.5 The Contractor shall provide subject matter expertise with mapping software and tactical software assurance and advanced sensory of weapon systems. The Contractor shall provide software engineering towards manipulating software control loops and tactical software assurance. (CDRL A001x)

C.3.2.6 The Contractor shall perform technical writing for technical and administrative publications. The Contractor shall conduct the configuration control and shall maintain cognizant oversight at all stages of document generation and maintenance. The Contractor shall perform technical writing for assembly procedures, system test procedures, user operation instruction manuals, and preventative maintenance and troubleshooting procedures. (CDRL A001x, A002x)

C.3.2.7 The Contractor shall perform technical editing of existing Government documents and presentations to ensure technical consistency, format consistency, and proper grammar. The Contractor shall conduct the configuration control and shall maintain cognizant oversight at all stages of document generation and maintenance. (CDRL A002x)

C.3.2.8 The Contractor shall prepare and review engineering drawings, engineering sketches, and Computer-Aided Design (CAD) systems and produce clear and technically accurate electrical and mechanical drawings based on design tolerances and specifications. The Contractor shall participate in the analysis of these technical documents. (CDRL A00Sx)

C.3.3 ENGINEERING LIFE-CYCLE SUPPORT

C .3.3.1 The Contractor shall conduct system, subsystem, component performance, and effectiveness improvement studies. (CDRL A001x, A00Bx)

C.3.3.2 The Contractor shall perform obsolescence analyses with recommendations for replacement components, parts, and systems. (CDRL A001x)

C.3.3.3 The Contractor shall provide subject matter expertise to investigate system, subsystem, and component level failures during design, integration, test, manufacture, and end-use to provide recommendations for corrective actions. (CDRL A001x)

C.3.3.4 The Contractor shall analyze deficiencies discovered during testing, outlined in production reports, maintenance reports, and user feedback trouble reports, to provide recommendations on corrective actions. (CDRL A001x)

DRAFT

C.3.3.5 The Contractor shall perform producibility trade studies and analyze production processes to: determine the most cost-effective fabrication/manufacturing process; resolve a failure observed during testing attributed to manufacture; and reduce manufacture process technology risk. (CDRL A001x)

C.3.3.6 The Contractor shall develop and generate assembly procedures and analyze approaches and generate plans to validate fabrication/manufacturing processes. (CDRL A001x, A00Ex, A00Px)

C.3.3.7 The Contractor shall develop and generate user operator manuals, preventive maintenance schedule manuals, and installation and removal procedures. (CDRL A001x, A002x, A00Ex, A00Px)

C.3.3.8 The Contractor shall develop and generate demilitarization plans. (CDRL A001x)

C.3.3.9 The Contractor shall provide subject matter expertise to develop new and modify existing Production Automated Test Equipment (ATE) hardware and software that can successfully run Factory Acceptance Tests (FAT) for USN tactical electronics hardware. (CDRL A001x, A002x, A00Ex)

C.3.4 ENGINEERING STUDIES AND ANALYSES

C.3.4.1 The Contractor shall develop and provide subject matter expertise into system analyses. (CDRL A001x, A002x)

C.3.4.2 The Contractor shall provide analysis, design, implementation, verification and documentation for new and existing shipboard combat weapons delivery and control systems. This includes: shipboard topside surveys; analyses of ships' plans and drawings; calculation of safe standoff angles from ships' structures for guns and precision guided weapons; preparation of weapons checkout forms; coordination with local Governmental and Contractor support personnel, and updating associated documentation; and design of pointing and firing cutout zones (both new and revisions to existing), including verification of weapons' performance for development of cut-out zones. (CDRL A001x)

C.3.5 MODELING AND SIMULATION SUPPORT

C.3.5.1 The Contractor shall perform and document computer solid layout modeling and simulation. (CDRL A001x, A00Ux)

C.3.5.2 The Contractor shall perform and document static and dynamic structural modeling and simulation. (CDRL A001x, A00Ux)

C.3.5.3 The Contractor shall develop, verify, validate, update, and document models and simulations to support gun and ammunition effectiveness analyses, including any associated graphical user interface. (CDRL A001x)

DRAFT

C.3.5.4 The Contractor shall document and provide source code for all models and simulations. (CDRL A001x, A002x, A00Tx, A00Ux)

C.3.6 DESIGN, PROVING AND VALIDATION ANALYSIS SUPPORT

C.3.6.1 The Contractor shall develop and generate system and force level test and exercise plans, test and exercise reports, as well as lower level test plans and reports. (CDRL A001x, A00Fx)

C.3.6.2 The Contractor shall develop test objectives, plans, and reports involving the design and analysis of test items and test fixtures. The emphasis of this work will be associated with bench level, system integration lab, computer lab and off-site testing, not including NSWCDD Range testing. (CDRL A001x, A002x, A00Fx)

C.3.6.3 The Contractor shall perform requirements analyses including the review of Design Agent requirements traceability documentation to ensure the traceability of hardware and software requirements to test events and test procedures. The Contractor shall develop recommended supplemental documentation for functional and cost analysis. (CDRL A001x, A00Fx)

C.3.6.4 The Contractor shall perform software code review and analyses in support of design engineering and perform software testing for design verification analyses. (CDRL A001x, A00Gx)

C.3.6.5 The Contractor shall perform tests and analyses to verify that the system, subsystem, and component either meet the functional, allocated, and product baseline or satisfy other requirements documentation. The Contractor shall provide subject matter expertise into the reduction of system, subsystem, and component-level risk. (CDRL A001x, A00Fx)

C.3.6.6 The Contractor shall analyze test and evaluation data and perform trade off analysis of alternatives assessments. The Contractor shall provide subject matter expertise and recommendations on reduction of design and technology risk and assess compliance with weapon and platform system requirements. (CDRL A001x)

C.3.6.7 The Contractor shall participate in off-site system, subsystem, and component testing by performing test planning and set up, execution, data collection, and test data analysis functions. (CDRL A001x, A00Fx)

C.3.6.8 The Contractor shall prepare test documentation to include: test requirements, test plans, test reports, test schedules, Mission Control Panel briefings, tactical mission briefings, Mission Readiness Reviews, Test Readiness Reviews, Standard Operating Procedures (SOP), flight cards, safety requirements and presentations to safety review. (CDRL A001x, A002x, A00Fx)

C.3.6.9 The Contractor shall perform test data collection, reduction and analysis for completion of tests relating to gun, system (gun mount and other associated equipment), ammunition, and ammunition feed testing. (CDRL A001x)

DRAFT

C.3.6.10 The Contractor shall provide system software testing and analysis of software-based weapon systems. The Contractor shall develop test procedures from the documented requirements and software trouble reports; perform unit, module, end-to-end, and endurance testing including the development of test procedures and test execution; perform white and black box testing; participate in and conduct independent verification and validation testing; prepare test reports and conduct analysis of test results to develop recommendations for mitigation or correction. (CDRL A001x, A00Tx)

C.3.6.11 The Contractor shall develop and give technical recommendations to test documentation such as test requirements, test plans, test reports, test schedules, Standard Operating Procedures (SOP), flight cards, countdown checklists and problem reports. (CDRL A001x, A00Fx)

C.3.6.12 The Contractor shall participate in test and evaluation events by performing test planning and setup of test equipment and systems, execution, data collection, and test data analysis functions and development of problem reports discovered during testing. (CDRL A00Fx)

C.3.6.13 The Contractor shall build and setup test equipment, collect, analyze and sample data, and produce mechanical and electrical engineering drawings and documentation. (CDRL A001x)

C.3.7 CONFIGURATION MANAGEMENT SUPPORT

C.3.7.1 The Contractor shall provide configuration management (CM) support performed at the program, project, system, and subsystem levels. The Contractor shall attend Change Review Boards (CRB), Change Control Boards (CCB), and Design Reviews.

C.3.7.2 The Contractor shall attend and provide technical subject matter expertise to Configuration Control Boards (CCBs) to evaluate proposed changes for system, subsystem, and component level impact and other associated system applicability. (CDRL A001, A00Q)

C.3.7.3 The Contractor shall generate and maintain formal Configuration Management Plans and related documentation. (CDRL A001, A002, A00Q)

C.3.7.4 The Contractor shall generate and review configuration item change documentation including Class I and Class II Engineering Change Proposals (ECPs), Requests for Deviations (RFDs), Request for Waivers (RFWs), Specification Change Notices (SCNs), and Notice of Revisions (NORs). (CDRL A001, A002, A00H, A00J, A00K, A00L, A00M, A00R)

C.3.7.5 The Contractor shall organize program, project, and IPT level documentation into repositories, including web-based repositories, and maintain the repository to facilitate documentation storage and retrieval. The Contractor shall convert program documents, weapons data and records to include video and microfiche into digital format for digital access, distribution, and archiving using electronic means including CDs and DVDs. (CDRL A002, A00S, A00U)

DRAFT

C.3.7.6 The Contractor shall generate, maintain, and revise drawings associated with components, sub-assemblies, and systems. The Contractor shall participate in the configuration management process by maintaining controlled and versioned documentation in accordance with the program or project CM plan. The Contractor shall provide process improvement suggestions towards the program or project CM plan. The Contractor shall participate in drawing and program reviews to baseline and revise documentation. (CDRL A002, A00H, A021, A00S)

C.3.8 TECHNICAL ADMINISTRATIVE SUPPORT

C.3.8.1 The Contractor shall identify and facilitate security requirements for conducting meetings. The Contractor shall organize and facilitate meetings by scheduling conference rooms at the Government and Contractor facility, generating agendas and invitations, disseminating invitations, and printing/binding presentation materials. (CDRL A006)

C.3.8.2 The Contactor shall attend meetings to generate attendee's lists, meeting minutes, and Action Items (AIs). The Contractor shall track meeting action items and maintain records reflecting both open and closed action items. The Contactor shall make real-time edits to documentation during meetings. The Contractor shall contact open action item Points of Contact (POCs) for status updates and document any updates prior to recurring meetings. (CDRL A007)

C.3.8.3 The Contractor shall provide support for requirement gathering from engineers, development of documentation for Government review/submission, entering data into systems, tracking procurements, and receiving and organizing information for delivery micro-purchase procurements. The Contractor is not authorized to receive any items that require NSWCDD plant accounting. (CDRL A002, A003)

C.3.8.4 The Contractor shall generate, update, and maintain program, project, and budget estimates, tracking budget execution by appropriation type, addressing budget issues, and recommending responses to budget data calls. (CDRL A002)

C.3.8.5 The Contractor shall generate, update and maintain Work Breakdown Structures (WBS). A WBS provides the necessary framework for detailed cost estimating and control along with providing guidance for schedule development and control. (CDRL A002, A00N)

C.3.8.6 The Contractor shall analyze and document the Government's market research, research alternatives for obsolete parts, and provide the Government recommendations on meeting technical specifications from the Government's analysis.

C.3.8.7 The Contactor shall populate and maintain acquisition database repositories to enable execution and tracking of procurements throughout their respective Life-Cycles.

C.3.8.7.1 The Contractor shall match end user material requests to various databases (technical screening and Information Technology Approval System).

C.3.8.7.2 The Contractor shall work with technical departments to answer questions or concerns relating to material management and general supply assistance.

DRAFT

C.3.9 TACTICAL SYSTEM SOFTWARE COMPLIANCE

C.3.9.1 The Contractor shall provide software compliance support to the programs supported under this Task Order. The Contractor shall assure all tactical Government systems managed under this requirement adhere to and are authorized in accordance with DODI 8500.01 and DODI 8510.01. The Contractor shall provide technical assistance to the Government in assuring compliance with all policies, guidance, and recommendations stipulated by higher authorities.

C.3.9.2 The Contractor shall prepare and develop certification and accreditation documentation that complies with known (e.g. Authorization & Accreditation (A&A), Platform Information Technology (PIT)) and future) requirements for tactical systems.

C.3.9.3 The Contractor shall perform testing and risk assessment of the Government tactical systems and provide results and reports.

C.3.9.4 The Contractor shall analyze software and hardware vulnerabilities and assess the likelihood of exploitation and impact those vulnerabilities have to Government tactical systems.

C.3.9.5 The Contractor shall assess and provide recommendations for the lifecycle of network threats, attack vectors and method of exploitation.

C.3.9.6 The Contractor shall prepare and update documentation for certification and accreditation of Government tactical systems. (CDRL A00H)

C.3.9.7 The Contractor shall recommend and implement Government approved and cost effective countermeasures to protect Government IT components.

C.3.10 SOFTWARE DEVELOPMENT

C.3.10.1 The Contractor shall provide software engineering and DevSecOps capability to weapon systems that shall be in compliance with Battle Management Open Architecture requirements. The Contractor shall, in collaboration with the Government and modeled after the ISO/IEC/IEEE 12207 standard, develop and maintain Software Development Plans (SDP), Software Requirements Specification (SRS), Interface Requirements Specification; test plans; engineering change proposals for the analysis and review of performance characteristics; test and evaluation documentation; evaluation modifications and upgrades as a result of maintenance efforts, technology refresh, analysis of alternatives, redesign/re-engineering, and obsolescence management; recommendations for the development and/or procurement of systems and subsystems. All developed products shall be owned by the Government.

C.3.10.2 The Contractor shall design, write and deliver software (all source code, files required for building/compiling, and executables) for use on mobile Android and/or Apple iOS platforms to meet operational and emerging requirements.

C.3.10.3 The Contractor shall provide technical development in the areas of intelligent automation, machine learning, and artificial intelligence for military applications. This includes the automation of all phases of the weapon system kill chain as well as Intelligence, Surveillance, and Reconnaissance (ISR) applications.

C.3.11 TESTING

C.3.11.1 The Contractor shall provide assigned portions of various engineering studies, plans, and related documents to include trade-off assignments, test or exercise plans and reports, and performance and effectiveness improvement studies. (CDRL A002, A00A)

C.3.11.2 The Contractor shall provide on-site and off-site testing support including the design and analy1sis of test items, systems, and test fixtures. (CDRL A002)

C.3.11.3 The Contractor shall participate in on-site and off-site testing by performing test planning and setup, execution, data collection, and test data analysis functions. (CDRL A00A)

C.3.11.4 The Contractor shall prepare test documentation such as test requirements, test plans, test reports, test schedules, Mission Control Panel briefings, Mission Readiness Reviews, Test Readiness Reviews, Standard Operating Procedures (SOP), flight cards, countdown checklists, safety requirements and presentations for safety review. (CDRL A002, A003, A00A)

C.3.11.5 The Contractor shall perform test data collection and reduction and analysis for completion of tests relating to gun, system (gun mount and other associated equipment), and ammunition testing.

C.3.12 DATA MANAGEMENT

C.3.12.1 The Contractor shall provide data management support for engineering efforts including system requirements tracing from high-level specifications through design, code, and test. Requirements tracing shall be performed on-site in Government facilities in the computer application designated by the Government.

C.3.12.2 The Contractor shall support the design, development, and maintenance databases and tools to facilitate the maintenance and tracking of systems engineering and program management activities. The Contractor shall also support the administration and implementation of Commercial Off-the-Shelf (COTS) databases and work-management systems based on the government infrastructure and tool selection. These databases and tools, developed in Government-specified or agreed-upon applications, shall be used to produce reports of systems engineering, configuration management, and program status.

C.3.12.3 The Contractor shall assist in the development of configuration management and quality assurance plans and procedures.

C.3.12.4 The Contractor shall provide status accounting and shall maintain the databases for platform or system configuration files, system builds, and deliveries. (CDRL A002)

DRAFT

C.3.12.5 The Contractor shall support software build and release management. The Contractor shall generate, update and maintain environment and software build procedure documentation; maintain the release schedule for all core services and ensure alignment across internal business and clients; and maintain a release repository and manage key information such as build and release procedures, dependencies, and notification lists.

C.3.13 SYSTEM TRAINING

C.3.13.1 The Contractor shall support the development of a training curriculum (e.g. software and documentation) and train end users how to operate NSWCDD developed systems. The Contractor shall provide review, analysis, and development support for training software. The Contractor shall participate in technical meetings to address training issues and architecture as they are related to the overall training program. The Contractor shall provide troubleshooting support on-site for deployed systems. The Contractor shall investigate problems and recommend architectural and systems solutions to enhance system operations within the training environment. (CDRL A002, A003)

C.3.13.2 The Contractor shall support the development and delivery of training on the operation of specific engagement systems, subsystems and/or components. The Contractor shall prepare course syllabi, classroom training, training aids and exams to measure achievement of learning objectives. (CDRL A002, A003)

C.3.14 LABORATORY SUPPORT

C.3.14.1 The Contractor shall provide laboratory maintenance for the supported programs, including identifying necessary tools and materials to effectively maintain the laboratory equipment on a daily basis. The Contractor shall perform troubleshooting of failed equipment; reporting to the facility manager the status and health of the equipment.

C.3.14.2 The Contractor shall maintain and troubleshoot the BMS Weapon System hardware as well as hardware from related systems.

C.3.14.3 The Contractor shall support and maintain electromechanical assembly projects in support of program requirements in accordance with Government best practices.

C.3.14.4 The Contractor shall work in an agile development environment to assist Government personnel in the design, build, and testing of hardware assembly projects.

C.3.14.5 The Contractor shall support and maintain virtual reality projects in support of program requirements in accordance with Government best practices.

C.3.15 FACILITY LOCATION/UNCLASSIFIED MEETING FACILITY

C.3.15.1 The Offeror's primary facility providing support under this contract must be located within 60 miles of NSWCDD, Dahlgren, VA.

DRAFT

C.3.15.2 The Contractor shall have a facility providing support to this requirement located within 60 miles of NSWC Dahlgren, Virginia, including conference facilities.

C.3.15.3 The Contractor shall provide an unclassified facility to hold meetings for technical discussions or design reviews for Government programs supported by this Task Order. The facility should accommodate up to 25 people and will be used up to once a month. The Government will provide 5 business days' notice prior to scheduled meeting.

C.3.15.4 The Contractor shall provide additional unclassified meeting space for 25-100 people for meetings or reviews for Government programs supported by this Task Order, when Government or Contractor facilities are not available or large enough for periodic program events. It is estimated that such large meeting space may be required up to two times per year. Government will provide 4 weeks' notice prior to a scheduled meeting.

C.4 TASK ORDER MANAGEMENT

The Contractor shall provide sufficient supervision to ensure all personnel work instructions and schedules originate with the Contractor rather than with the Government technical office. This supervision shall ensure that the Contractor's personnel are not assigned work instructions and schedules outside this SOW. Any perceived conflicts with the SOW shall be directed to the Contracting Officer and Contracting Officer's Representative (COR).

C.4.1 Progress Report

The Contractor shall submit a Contracting Officer's Management Report. (**CDRL A001x, A00Bx, A00Cx, A00Dx**) The Contractor shall maintain and provide a list of all personnel assigned to the Task Order. The Contractor shall provide copies of invoices received from Sub-contractors and consultants as well as evidence of its review to ensure that all invoiced costs represent services that have been performed and deliverable items. In accordance with G-232-H005, Supplemental Instructions Regarding Invoicing, and FAR 52.216-7(DEVIATION 2026-O0045), Allowable Cost and Payment, the Contractor shall provide the COR supporting documentation, including receipts, for all travel and material purchases with each invoice submission.

C.4.2 In Progress Reviews (IPRs)

The Contractor shall participate in both formal and informal In Progress Reviews (IPRs) of work being performed. IPRs may be conducted at the overall Task Order level or for specific projects/work areas. Reviews will be scheduled by the Government. An initial formal IPR is planned within 90 days of the Task Order award date and will follow the agenda agreed to by the COR. Subsequent formal IPRs shall be held approximately every six (6) months thereafter unless waived by the Government. The IPRs shall be conducted at a location mutually agreed upon by the Contractor and the Government. At the time the review is scheduled, the Government will communicate the specific purpose of the review and advise the Contractor as to the desired content of the presentation. (**CDRL A001x, A007x, A009x**)

C.4.3 Task Prioritization Meetings

The Contractor shall participate in periodic Task Prioritization Meetings with the COR and Subject Matter Experts (SMEs). The purpose of these meetings is to convey the Government's technical program schedules and priorities and to identify corresponding task priorities for this Task Order. The Contractor shall document meeting minutes of the meetings. (**CDRL A007x**)

C.4.4 Telework

In accordance with H-216-H002 Level of Effort -- Alternate I (NAVSEA) teleworking at an alternative worksite is permitted. Telework is also dependent upon the type of work being performed. The Contractor shall track all Government Furnished Property, listing personnel, asset tag numbers and serial numbers for all Navy Marine Corps Intranet (NMCI) computer equipment in the Contractor's possession for telework. All equipment shall be returned to the Government by the end of the Task Order or when equipment is no longer in use, whichever comes first.

C.5 SKILLS AND TRAINING

C.5.1 The Contractor shall provide capable personnel with qualifications, experience levels, security clearances, and necessary licenses, certifications, and training required by Federal, State, and Local laws and regulations. Information assurance functions require certifications specified in DOD Manual (DoDM) 8140.03 Cyberspace Workforce Qualification and Management Program.

C.5.2 Per the requirements set forth in DODM 8140.03 as a condition of meeting requirements, personnel performing Information Assurance (IA) functions outlined in the manual will be tracked for compliance, designated in writing from the Local Command Authority as Cyberspace Workforce (CWF), shall already be in possession of an approved commercial certification for their environment at time of performance start, and shall satisfy both preparatory and sustaining DOD IA training and certification requirements as outlined in DODM 8140.03. Additionally, personnel with Privileged Access must sign acknowledging duties on a "Privileged Access Agreement", be able to maintain the appropriate investigation type, sign a System Authorization Access Request-Navy (SAAR-N) with "privileged" indicated, complete applicable Operating System/Computer Environment (OS/CE) training to Navy's standards, and maintain a valid commercial certification that meets outlined designations. Failure to maintain all requirements at the appropriate level may result in the removal of elevated access and removal from tasks being performed. Non-privileged Information Assurance Workforce (IAWF) members may be removed from tasks being performed. In both situations, access will be returned once the failure(s) are corrected.

C.5.3 Training necessary to ensure that personnel performing under this Task Order maintain the knowledge and skills to successfully perform the required functions is the responsibility of the Contractor. Training necessary to maintain professional certification is the responsibility of the Contractor. The Contractor shall provide training opportunities to maintain Contractor

capabilities and/skills to coincide with changing technology environments. All costs for DODM 8140.03 certification shall be borne by the Contractor for new employees on this Task Order.

C.5.4 Training on non-commercial and department-specific tools and procedures will be provided by the Government.

C.5.5 Notwithstanding the above, it is understood that the Government may require services requiring knowledge and skills of a newly emergent technology. The Contracting Officer may, on a case-by-case basis, authorize the expenditure of Government funds for the training of Contractor personnel. Advance approval is required. The Contractor is encouraged to suggest a cost-sharing arrangement that addresses registration, tuition, travel, and labor costs.

C.5.6 The Contractor shall complete all mandatory training as prescribed by the Government. These training requirements are accessed through Government web-based training (WBT), classroom training, or combination of both.

C.5.7 Mandatory Training Completion Log - The Contractor shall submit a CWF report (CDRL A00xx). The CWF report shall address required CWF training including annual continuous learning training requirements. The Contractor shall also submit Mandatory Training Completion Log (CDRL AOOVx). The Mandatory Training Completion Log shall address all mandatory training completed as directed by the COR.

Commented [K1]: Suggested DID DI-MGMT-82160

C.6 OTHER DIRECT COSTS

During the performance of this Task Order the Contractor will have to travel and procure material and consumables to perform the tasking of the SOW.

C.6.1 Travel

The Contractor shall be required to travel in performance of this Task Order. The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements and shall be requested of and authorized in advance by the COR by email. All requests shall show the appropriate Task Order number, the number of people traveling, the number of days for the trip, the reason for the travel, an estimated cost (with G&A separate), and any high cost or unusual costs expected. The Contractor is not authorized to perform any travel that is not in conjunction with this effort. All travel shall be conducted in accordance with Class Deviation 2026-O0032 Revolutionary FAR Overhaul (RFO) 31.205-46 Travel Costs. Locations will be determined by the Government and are subject to change.

Representative travel locations may include: Naval Surface Warfare Center Dahlgren Division Dahlgren VA, United States Special Operations Command Detachment 1 Eglin AFB FL, Special Operations Squadron (SOS) Hurlburt Field FL, Robins Air Force Base Robins GA, Cannon Air Force Base Cannon NM, White Sands Missile Range White Sands NM, Fort Eustis Army Base Eustis VA, Peterson Space Force Base Colorado Springs CO, Aberdeen Proving Ground Aberdeen MD, Naval Station Mayport Mayport FL, Surface Combat Systems Center Wallops Island VA, Redstone Arsenal Arsenal AL, Naval Air Station Patuxent River Patuxent River MD,

Naval Surface Warfare Center Carderock West Bethesda MD, Naval Surface Warfare Center Corona Norco CA, Naval Surface Warfare Center Crane Crane IN, Naval Surface Warfare Center Indian Head Indian Head MD, Picatinny Arsenal Morris County NJ, Naval Surface Warfare Center Keyport Keyport WA, Naval Undersea Warfare Center Division Newport Newport RI, Naval Surface Warfare Center Panama City Panama City FL, Naval Surface Warfare Center Philadelphia Philadelphia PA, Naval Surface Warfare Center Port Hueneme Port Hueneme CA, Hickam Air Force Base Pearl Harbor HI, Naval Air Weapons Station China Lake China Lake CA, Joint Base Andrews Andrews MD, Fort Liberty Fayetteville NC, Fort Moore Columbus GA, Naval Base Ventura County Point Mugu Ventura County CA, San Diego CA, Portsmouth ME, Savannah GA, Norfolk VA, Moss Point MS, Huntsville AL, Denver CO, Fort Walton Beach FL, Clovis NM, Corona CA, Jacksonville FL, El Centro CA, Lexington Park MD, Fayetteville NC, Austin TX, Everett WA, and all other NSWC Warfare Centers. OCONUS: Guantanamo Bay Cuba, Singapore, Bahrain, Japan, Israel, Philippines, Africa, Korea, Guam, Italy, Thailand, United Kingdom, Vietnam, Spain, Brunei, Indonesia, Malaysia, Taiwan, Hong Kong, Djibouti, Greece, Turkey, Seychelles, Diego Garcia, Caribbean Panama, Australia, Guyana, Palau, and the Netherlands

The Contractor shall submit trip reports following any travel under this effort. (**CDRL A00Wx**)

C.6.2 Direct Charge of Materials

(a) During the performance of this Task Order it may be necessary for the Contractor to procure materials to respond to the mission requirements listed in the SOW. This Task Order is issued under a services contract and the procurement of materials of any kind that are not directly related to and necessary for performance may be determined to be unallowable costs pursuant to Class Deviation 2026-O0032 RFO Part 31. Any material provided by the Contractor is subject to the requirements of the FAR, Defense Federal Acquisition Regulation Supplement (DFARS), and the applicable Department of Navy regulations and instructions. Charges related to materials costs may include general and administrative (G&A) expenses but shall not include fee or profit.

(b) The materials listed in paragraph (e) below shall be the only ones approved for purchase under this Task Order. The numbers of, and types of, material purchases shall be limited to the minimum required to accomplish work requirements and shall be coordinated with the COR. Splitting purchase requirements to defeat purchasing thresholds shall not be approved. If the Contractor (or Sub-contractor) possesses a Defense Contract Management Agency (DCMA) approved purchasing system, individual item purchases greater than $3,000 but less than $10,000 shall be approved by the COR; individual item purchases equal to or over $10,000 shall not be executed until the COR reviews the requested purchase and approval is obtained from the Contracting Officer. If the Contractor does not possess an approved purchasing system, individual item purchases less than $3,000 shall be approved by the COR. For purchase of materials equal to or over $3,000 shall not be executed until the COR reviews the requested purchase and approval is obtained from the Contracting Officer. No purchases of any amount shall be executed by a Sub-contractor if they do not have a Defense Contract Audit Agency (DCAA) approved accounting system.

(c) Information Technology (IT) Resources shall not be purchased unless DOD and Navy purchasing procedures (including Information Technology Procurement Request (ITPR) approval) have been satisfied and approvals obtained. IT Resources include personal computers (PCs), laptops, printers, software, servers, hubs, routers, phones, fax machines, and any related maintenance, telecommunications, training, or other support services. All IT Resource Other Direct Cost (ODC) purchases require COR approval regardless of the dollar value associated with the purchase.

(d) The costs of general purpose business expenses required for the conduct of normal business operations will not be considered allowable direct costs in the performance of the Task Order - unless supported by DCMA as a procedure of the Contractor's accounting procedures. General purpose business expenses include the costs for items such as telephones (including cell phones) and telephone charges, copy machines, word processing equipment, personal computers, and other office equipment and supplies.

(e) The materials and equipment contained in the following list are authorized for purchase once the Contractor has complied with approval requirements stated in paragraph (b) above and paragraph (f) below:

- Incidental material and logistics costs (shipping/packaging/storage) in direct support of SOW tasking and in quantities appropriate for prototype or R&D efforts.
- Fasteners and miscellaneous hardware
- Connectors and miscellaneous electrical hardware
- Systems Integration Laboratory (SIL) Materials and Equipment required to replace system applications for development, testing, and demonstrations.
- Special tools and tooling (such as dial calipers, measurement gauges, torque wrenches, depth micrometers, multimeter, etc.)
- Limited quantities of miscellaneous hardware and fixtures
- Limited quantities of miscellaneous electrical cabling and enclosures
- Limited quantities of circuit boards and electrical hardware
- Specific IT tools that are required to support SOW tasking for particular project requirements
- Emergency response asset protection equipment such as portable pumps, generators, dehumidifiers, and air conditioners to be utilized in the event a laboratory is compromised therefore placing Government and Government Sponsor owned equipment at risk of being damaged.
- Additional ODCs include communication costs, supplies, reproduction, and materials directly associated with the Task Order. Examples of additional ODCs are:
- Occupancy costs for subcontractors working in Contractor facilities
- Communications (cellular services if required and authorized, internet hosted meetings, remote training services and conference calling services)
- Reproduction/Printing/Binding
- Delivery costs (i.e., FedEx)

DRAFT

- Insurance for OCONUS travel should this become required at anytime
- Documents and related items for OCONUS travel should it become necessary
- Safety Supplies and miscellaneous items as needed such as hardhats, goggles, flight suits, boots, safety shoes, safety harnesses lanyard.

Materials not fitting the descriptions listed in this section may not be purchased unless mutually agreed to by both the Government and Contractor and subsequently added to the contract by Task Order modification.

(f) Procedure for obtaining COR and/or Contracting Officer approval, the Contractor shall submit a request for purchase of materials to the COR through email. The COR will review the request, if it is in accordance with paragraph (b) above and requires Contracting Officer approval, the COR will submit the request via the Contract Specialist to the Contracting Officer for review and approval. Minimum requirements for a written request for purchase are as follows:
(1) Description of the material to be purchased;
(2) Quantity;
(3) Unit and total cost;
(4) Delivery/freight charges;
(5) Any associated service charges such as assembly, configuration, packing, etc.;
(6) An explanation of the need for the material;
(7) Copy of the competitive quotes received from potential suppliers;
(8) The basis for the selection of the selected supplier;
(9) Explanation of the determination of price reasonableness regarding the selected supplier costs;
(10) If the procurement is sole sourced to a particular supplier or manufacturer, include the rationale for limiting the procurement to that supplier or manufacturer;
(11) ITPR request date, and if granted, approval date and tracking number (if applicable);

Once the COR and/or Contracting Officer have reviewed the request, the Government will notify the Contractor of the outcome. Issues or details may be discussed with the Contract Specialist acting on behalf of the Contracting Officer until a final Government determination is made as to whether to approve, modify, or reject the purchase.

(g) The Contractor is required to possess and maintain an adequate property management system. The system must track all materials/ODCs associated with this Task Order. Equipment purchased by the Contractor and delivered to the Government must be delivered via electronic Material Inspection and Receiving Report (DD Form 250) within the Wide Area Workflow (WAWF) system. Upon completion of the Task Order Period of Performance, all material associated with this Task Order that were purchased by the Contractor and not depleted or previously delivered to the Government during the performance of this Task Order shall become the property of the Federal Government. The Contractor shall transfer all materials, not depleted or previously delivered to the Government, to the COR by way of an electronic DD Form 250 in WAWF in accordance with Class Deviation 2026-O0046 DFARS PGI 245.402-71.

C.6.3 Counterfeit Parts and Materiel

DRAFT

(a) The following minimum processes shall be implemented and flowed down by the Contractor to all Sub-contractors in order to minimize the risk of use of counterfeit parts.

(b) The Contractor shall establish processes to minimize the risk of procuring and using counterfeit parts and materiel. The Contractor shall document these processes and provide those documented processes to Government representatives upon request. The Contractor shall ensure that all requirements are flowed down to Sub-contractors and suppliers at all tiers.

(c) At a minimum, these processes shall ensure that:

- Materiel that is either in production or currently available shall be purchased from an original manufacturer, aftermarket manufacturer, or other authorized supplier.
- Materiel that is neither in production nor currently available may be purchased from suppliers, including unauthorized suppliers, that meet appropriate counterfeit avoidance criteria documented in industry anti-counterfeit standards. The Contractor shall notify the KO and COR when critical or high-risk materiel is procured from an unauthorized source. The Contractor shall provide this notification before materiel is installed so mitigation actions can be taken.
- The Contractor shall maximize the use of authentic, originally designed and/or qualified parts.
- The Contractor shall assess potential suppliers to minimize the risk of receiving counterfeit parts or materiel.
- The Contractor shall have purchasing procedures which confirm whether a selected supplier is authorized (as defined in SAE AS5553) for each purchase.
- The Contractor shall define minimum inspection and test requirements for parts being procured and shall ensure that in-house, third-party, and/or supplier inspection and test procedures and facilities comply with the requirements of this section. These minimum inspection and test requirements shall specify appropriate test methods to detect potential counterfeit parts and materiel.
- The Contractor shall require a certificate of conformance (as defined in SAE AS5553) and supply chain traceability for all electronic part purchases.
- The Contractor shall use government or industry services such as Government-Industry Data Exchange Program (GIDEP) and other commercially available services to identify part or supplier quality or authenticity problems.
- The Contractor shall maintain critical or high-risk materiel traceability that enables tracking through the supply chain to the original manufacturer if purchased from an authorized source or to the unauthorized source at a minimum if purchased from an unauthorized source.

(d) The Contractor shall immediately notify the COR of the occurrence of a suspect or confirmed counterfeit part or materiel. Contractor shall notify the COR of all actions taken to identify, contain, and impound all product from the lot, within 7 working days of confirmation of the counterfeit status. The Contractor shall initiate and submit an ALERT to GIDEP within 60 days of knowledge of the counterfeit part or materiel.

(e) Suspect counterfeit parts and materiel shall be impounded with all other items from the same lot. The Contractor shall identify and locate all potential users or hardware items with the

suspect part or materiel and contain the product which has this suspect part or materiel, pending confirmation of the part or materiel's authenticity. The Original Equipment Manufacturer (OEM) may be involved at this point to verify authenticity. Confirmed counterfeit materiel shall be contained and provided to investigative agencies for ongoing investigation or prosecution. The counterfeit product shall not be scrapped or otherwise disposed of without approval from investigative authorities or the Contracting Officer. Confirmed counterfeit product shall be disposed of in a way which would not allow its resale or reuse.

(f) Counterfeit parts are defined in SAE AS5553. Counterfeit parts may be electronic or mechanical in nature. Counterfeit electronic parts may typically be used parts which have been refurbished and represented as new. Commonly counterfeited electronic parts include parts such as microcontrollers or specially screened devices, or common parts, which have several pin-compatible versions from multiple manufacturers, such as memory devices and operational amplifiers. Counterfeit mechanical parts are typically improperly made, marked, or treated products. Examples are improper anodization or heat treatments (or falsified data), mismarked parts sold as higher grade steel, or used/fake parts such as valves or circuit breakers.

C.7 GOVERNMENT FURNISHED SPACE/GOVERNMENT FURNISHED PROPERTY/GOVERNMENT FURNISHED INFORMATION

C.7.1 Government Furnished Space

(a) Government Furnished Office Space, will be provided for the following labor categories and number of personnel. This office space will be the primary work location for these positions.

Labor Category	Base Year	Option 1	Option 2	Option 3	Option 4
Senior Systems Engineer	1	1	1	1	1
Senior Weapons Systems Engineer	1	1	1	1	1
Senior System Tester	1	1	1	1	2
Software Engineer	4	5	5	5	5
System Engineer	7	7	8	8	8

(b) Access to Government Lab Space will be provided. Lab space does not constitute office space. Government Furnished Lab Space will be provided for the following labor categories and number of personnel. No separate office space will be provided.

Labor Category	Base Year	Option 1	Option 2	Option 3	Option 4
Junior Engineer	**6**	**6**	**6**	**6**	**6**
Configuration Management Analyst	3	3	3	3	3

DRAFT

System Tester	10	10	10	10	10

(c) Access to Government rental space will be provided for the following labor categories and number of personnel. This office space will be the primary work location for these positions.

Labor Category	Base Year	Option 1	Option 2	Option 3	Option 4
AR/VR Software Engineer	20	22	24	25	26
Jr. AR/VR Engineer	2	2	2	3	4
Computer Simulation Developer	10	11	11	12	12
Software Engineer	18	18	19	20	21
Software Tools Developer	5	5	5	5	5
Information Assurance (IA) Specialist	1	1	1	1	1
System Tester	5	6	6	6	6

(d) Government Furnished Property (GFP) (hardware, software, firmware) will be provided to support access to NMCI/Nautilus or other Government computer resources as required during performance of this Task Order.

C.7.2 Government Furnished Property (GFP)

(a) GFP may be issued under this Task Order. The Government will make available the Government Property identified in the attachment J.X, Government Furnished Property on a rent-free basis in performance of the Task Order. The Contractor is responsible for all costs related to making the property available for use, such as payment of all transportation, installation, or rehabilitation costs.

(b) The Contractor shall maintain and report the inventory of GFP (**CDRL A002X, A004x, A008x**) issued under this Task Order. This requirement is in addition to anything required by regulation, statute, or the assigned Government Property Administrator.

Commented [KU2]: A GFP CDRL is required in contracts with GFP. The DID to be used depends upon the type of contract:
a)For non-sustainment contracts, the DID is Government Property Inventory Report, DI-MGMT-80441D.
b)For sustainment contracts, the DID is Government Furnished Material (GFM) by national Stock Number (NSN), DI-PSSS-80727A. A sustainment contract is a contract that supports the maintenance and management of a product or service over its life cycle.
Code 107 mailbox should be included on the distribution for this CDRL.

C.7.3 Government Furnished Information (GFI)

(a) The Government will provide access to information and documentation required for Task Order performance (Attachment J.X, Government Furnished Information).

(b) All information and documentation shall be retained at the Government work site.

DRAFT

(c) Upon completion of any task, the Contractor shall return all GFI associated with the task and return the hard copy files and electronic copies of all documents produced under this Task Order.

C.8 SECURITY

C.8.1 Personnel and Facility Clearance Requirements

(a) Facility Clearance Level (FCL) Requirement: The Prime Contractor supporting this Task Order is required to have an FCL of TOP SECRET and safeguarding clearance level of SECRET at the primary facility supporting this Task Order.

(b) Personnel Clearance Level (PCL) Requirement: All personnel directly supporting this Task Order, except Management and Support personnel, are required to have, as a minimum, a current SECRET security clearance in the Defense Industrial Security System (DISS). Interim clearances are acceptable. Personnel performing in the following labor categories shall have a final TOP SECRET security clearance with Sensitive Compartmented Information (SCI) eligibility in DISS: Senior Software Engineer (1 FTE); Senior Systems Engineer (1 FTE); and Systems Engineer (1 FTE).

C.8.2 The Contractor will have access to information and compartments with a SECRET /TOP SECRET / SCI classification. All deliverables associated with this Task Order are unclassified unless otherwise specified. Access to classified spaces and material and generation of classified material shall be in accordance with the attached DD Form 254 (Attachment J.X).

C.8.3 The Department of Defense Contract Security Classification Specification (DD Form 254) provides the security classification requirements for this effort. The Contractor shall obtain facility and personnel security clearances as required by the National Industrial Security Program prior to starting to work on tasks requiring clearances. Access to classified spaces and material and generation of classified material shall be in accordance with the National Industrial Security Program Operating Manual (NISPOM) 32 Code of Federal Regulation (CFR) Part 117 and the NSWCDD Command Security Manual.

C.8.4 Some work accomplished under this Task Order will be classified up to the level of TOP SECRET. The Contractor shall maintain the capability to store information up to and including SECRET. All data generated under this Task Order shall be classified in accordance with the guidance in the NISPOM 32 CFR Part 117 and the NSWCDD Command Security Manual.

C.8.5 The Contractor must comply with guidelines specified on the DD Form 254. Contractors SCI indoctrinated in support of this Task Order shall comply with the reporting requirements as outlined in DOD policies Security Executive Agent Directive (SEAD)-3 dtd 12 June 2017 Implementation memo dtd 02 Nov 2020 and SEAD-4 Implementation memo dtd 12 Jan 2018.

C.8.6 The Contractor shall require access to Communications Security (COMSEC) information and materials. A COMSEC account is also required in order to maintain and use COMSEC material, which includes accountable/non-accountable COMSEC Material and Controlled Cryptographic Items (CCI). The Contractor shall utilize CRYPTO and have access to Secure

Terminal Equipment (STE) and associated encryption device(s) at the Contractor site(s). SCI requirements are hereby authorized. Questions regarding Block 10e (1) and requests for retention or release of intelligence shall be through the NSWCDD SSO, (540) 284-0419. All SCI work on this contract will be performed at cleared government/contractor installations listed in block 8a. (Cleared Contractor facilities require current Physical and TEMPEST Accreditations along with copies of FFC and TEMPEST Addendum.) The Contractor requires access to Non-SCI intelligence is needed in order to utilize intelligence documents related to foreign government weapons systems. The Contractor will be required to take NATO training to obtain a SIPRnet (or cRDTE) account/s and to utilize the DTIC system to obtain documents on intelligence. Access to classified NATO information is also required by the Contractor. All personnel who have access to classified NATO information will be a U.S. citizen, have a need-to -know and a final government security clearance. Access to Foreign Government Information is required to obtain United Kingdom documents on specific weapon systems. In performing under this Task Order, the Contractor shall have access to U.S. classified information outside the U.S., Puerto Rico, U.S. Possessions, and Trust Territories: Bahrain, Japan, Israel, Korea, Guam, Italy, United Kingdom, Spain, Turkey, and the Netherlands. Controlled Unclassified Information (CUI), formerly For Official Use Only (FOUO) and Personally Identifiable Information (PII), generated and/or provided under this Task Order shall be safeguarded and marked as specified in DoDI 5200.48, Controlled Unclassified Information (CUI) and DoDM 5400.07. All above accesses are needed to support and provide the system engineering, software development, tactical initiatives and baseline developments to support NSWCDD.

C.8.7 Facility Clearance: The Contractor shall possess and maintain a TOP SECRET facility clearance as verified within the National Industrial Security System (NISS).

C.8.8 Physical Security: The Contractor shall be responsible for safeguarding all Government information or property provided for Contractor use. At the end of each work period, Government information, facilities, equipment and materials shall be secured as specified by the 32 CFR Part 117 and the NSWCDD Command Security Manual. Secret storage is required at the Contractor's facility in order to meet requirements of receiving and generating classified material in accordance with this Task Order.

C.8.9 Contractors working in Open Storage Secret (OSS) spaces with Open/Close privileges shall be aware of their responsibility and be trained in procedures for end-of-day security checks to include closing OSS spaces.

C.8.10 Electronic Spillage

C.8.10.1 Electronic Spillages (ES) are unacceptable and pose a risk to national security. An electronic spillage is defined as classified data placed on an information system (IS), media or hardcopy document possessing insufficient security controls to protect the data at the required classification level, thus posing a risk to national security (e.g., sensitive compartmented information (SCI) onto collateral, Secret onto Unclassified, etc.). The Contractor's performance as it relates to ES will be evaluated by the Government. ES reflects on the overall security posture of NSWCDD and a lack of attention to detail with regard to the handling of classified information of IS security discipline and will be reflected in the Contractor's performance rating.

If a Contractor is determined to be responsible for an ES, all direct and indirect costs incurred by the Government for ES remediation could be charged to the Contractor.

C.8.10.2 NSWCDD Security will continue to be responsible for the corrective action plan in accordance with the security guidance reflected on the DOD Contract Security Classification Specification – DD Form 254. NSWCDD Security will identify the Contractor facility and contract number associated with all electronic spillages that involve the Contractor. NSWCDD Security will notify the Contracts Division with the Contractor facility name and contract number, incident specifics and associated costs for clean-up. The Contracting Officer will be responsible to work with the Contractor Facility to capture the costs incurred during the spillage clean up. The Contractor is also responsible for taking Information Security Awareness training annually, via their Facility Security Officer (FSO), as part of the mandatory training requirements. If a spillage occurs additional training will be required to prevent recurrence.

C.8.11 Portable Electronic Devices (PEDs)

C.8.11.1 Non-Government and/or personally owned portable electronic devices (PEDs) are prohibited in all NSWCDD buildings with the exception of personally owned cell phones which are authorized for use in General Office Spaces (GOS). All personnel need to be aware of the PEDs policy and what is permitted in a building by asking authorized personnel or reviewing the entrance area signs and instructions. The Contractor/personnel visiting shall ensure the onsite personnel remain compliant with this PED policy. NSWCDD instruction defines PEDs as the following: any electronic device designed to be easily transported, with the capability to store, record, receive or transmit text, images, video, or audio data in any format via any transmission medium. PED's include, but are not limited to, pagers, laptops, radios, compact discs and cassette players/recorders. In addition, this includes removable storage media such as flash memory, memory sticks, multimedia cards and secure digital cards, micro-drive modules, ZIP drives, ZIP disks, CD-RWs, DVD-RWs, MP3 players, iPADs, digital picture frames, electronic book readers, kindle, nook, cameras, external hard dish drives, and floppy diskettes.

C.8.11.2 Personal Wearable Fitness Devices (PWFDs) marketed primarily as fitness or sleep devices are allowed in all Navy spaces, if they are compliant with NAVADIN 216/15, where collateral non-Sensitive Compartmented Information (SCI), classified information is processed, stored, or discussed up to and including SECRET. The user must ensure the PWFD is compliant with all requirements in NAVADMIN 216/15, Cyber Hygiene Authorization to use Personal Wearable Fitness Devices (e.g., FitBit, Jawbone UP, etc.) in Navy Spaces, dated 14 September 2015 and register PWFD in the NSWCDD Fitness Device Tracker.

C.8.11.3 Personnel requiring the use of Medical Portable Electronic Devices (MPEDS) must submit Form NSWCDD 5239/4 for SCIF authorization to the SCIF authorizations to the Special Security Officer (SSO). For Special Access Program Facility (SAPF) authorizations, follow the guidance provided by the Government Special Access Program Security Officer (GSSO). Authorizations for use in SAPFs that are co-utilized within NSWCDD SCIFS require coordination between both the GSSO and SSO. For authorizations to use MPED in Collateral Classified spaces, submit form to the Special Programs Branch, Code 1053.

C.8.11.4 PED's belonging to an external organization shall not be connected to NSWCDD networks or infrastructure without prior approval from the NSWCDD Information Assurance and Compliance Branch. This approval will be granted using the Temporary Approval Request for Information System (TARIS) form and action tracker process.

C.8.11.5 Personally owned hardware or software shall not be connected or introduced to any NSWCDD hardware, network or information system infrastructure.

C.8.11.6 Navy-issued peripheral:

C.8.11.6.1 Government procured headsets with or without microphones must be wired, use either a 3.5 millimeter (mm) audio jack or universal serial bus (USB) port, cannot contain active-noise cancelling functionality and may be used on systems of classification up to and including collateral Top Secret. The headsets are considered unclassified when unplugged, and must be unplugged when not in use within classified spaces.

C.8.11.6.2 Government procured Bluetooth earbuds and headsets that do not require a USB dongle or any other physical connection to enable wireless connectivity are allowed for use on Government issued tablets, phones, and personal devices in telework environments or unclassified general office space where no classified discussion are occurring.

C.8.11.6.3 Web cameras may only be used on systems at the classification level of the space. For example, in a collateral SECRET open storage area an external web camera may be connected to the SECRET workstation only. No camera pass is required for these devices.

C.8.11.6.4 Government provided printers and/or scanners are authorized in a telework environment. Users must ensure that any paper or media containing CUI or unclassified information not authorized for public release is safeguarded by locking in a drawer, cabinet or room. CUI and unclassified information not approved for public release must be returned to the worksite for destruction.

C.8.11.6.5 Government issued peripherals may be used on personal devices.

C.8.11.6.6 While connected to any Navy network, whether on site or while in a telework environment, the use of headsets with microphones and web cameras are restricted to official Government duties.

C.8.12 Operations Security (OPSEC)

Contractor personnel shall follow OPSEC concepts and principles in the conduct of this requirement to protect critical information, personnel, facilities, equipment, and operations from compromise. All Contractors (including Sub-contractors) shall supplement their current security practices by requiring any personnel involved in executing this Task Order to complete Government-sponsored and administered Operations Security (OPSEC) training. In addition, all Contractors should be aware of the Critical Information and Indicators List (CIIL) for the organization they are supporting as well as the OPSEC Manual for NSWCDD. These OPSEC

DRAFT

requirements will be in effect throughout the life of the procurement from award through the conclusion of services at the end of the period of performance (PoP) or other procurement termination. The Contractor must immediately notify the Government upon the discovery of any nonconformance with the OPSEC Manual.

C.8.13 Privacy Program Training

Privacy training is mandatory for all NSWCDD personnel (military, civilian, and Contractor) and must be completed annually. Total Workforce Management Services (TWMS) is the official database for workforce training and is the tool for taking and recording Privacy Act training. The Contractor is responsible for ensuring individual annual privacy training requirements are met.

C.8.14 IT-1 Designation Requirements

C.8.14.1 In accordance with (IAW) DON Chief Information Officer (CIO), NSWC Headquarters, and NSWCDD 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 Government, and will be at the Government's 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.

C.8.14.2 Any Contractor employee, who has a final clearance and submitted T5/T5R that is accepted by Office of Personnel Management (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.

C.8.14.3 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, shall remain at IT level-II status and shall not be assigned to a contract position requiring IT Level-I designation.

C.9 ON-SITE ENVIRONMENTAL REQUIREMENTS

C.9.1 The Contractor shall strictly adhere to all Federal, State and local laws and regulations, Executive Orders, and Department of Defense and Navy policies.

C.9.2 The Contractor shall ensure that each Contractor employee who has been or will be issued a Common Access Card (CAC), performs work in direct support of NSWCDD programs under the NSWCDD Commanding Officer, and sits on-site at NSWCDD, completes the NAVSEA Environmental Awareness Training (TWMS-695388) within 30 days of commencing Task Order performance and at least every three (3) years thereafter or as directed by their NSWCDD training coordinator or their COR.

DRAFT

C.9.3 The Contractor shall ensure that each Contractor employee not required to complete the training described above (i.e., those who do not have and will not be issued a CAC, do not perform work in direct support of NSWCDD programs under the NSWCDD Commanding Officer, and do not sit on-site at NSWCDD) reads the NSWCDD Environmental Policy Statement within 30 days of commencing Task Order performance. This document will be available from the COR, however, the policy is also provided on the publicly-available NSWCDD website, https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Dahlgren/Resources/.

C.9.4 Within 30 days of commencing Task Order performance, the Contractor shall certify by email to their COR that the requirements captured above have been met. The email shall include each employee name and work site and shall indicate which requirement each employee has satisfied.

C.9.5 Contractor copies of the records generated by the actions described above will be maintained and disposed of by the Contractor in accordance with Secretary of Navy Instruction (SECNAVINST) 5210.8 (series) Department of the Navy Records Management Program.

C.9.6 The Contractor shall perform work under this Task Order consistent with the relevant policy and objectives identified in the NSWCDD environmental management system (EMS). The Contractor shall perform work in a manner that conforms to all appropriate EMS Plans of Actions and Milestones identified by the NSWCDD EMS Plan. In the event an environmental nonconformance or noncompliance associated with the contracted services is identified, the Contractor shall respond and take immediate corrective and/or preventative actions to ensure the actions do not continue. In addition, the Contractor shall ensure that their employees are aware of their roles and responsibilities identified by the NSWCDD EMS and how these requirements affect their work performed under this Task Order.

C.10 ON-SITE SAFETY REQUIREMENTS

C.10.1 The Contractor shall strictly adhere to Federal Occupational Safety and Health Agency (OSHA) Regulations, Environmental Protection Agency (EPA) Regulations, NSWCDDINST 5100.1 (series) Occupational Safety and Health Program (current revision), and all applicable state and local requirements.

C.10.2 The Contractor shall ensure that each Contractor employee reads the document entitled, "Occupational Safety and Health (OSH) Policy Statement" within 30 days of commencing performance at NSWCDD. This document is available at: https://flankspeed.sharepoint-mil.us/sites/NAVSEA_NSWCDD_SE/SitePages/OSH-Bulletin-Board.aspx.

C.10.3 The Contractor shall provide each Contractor employee with the training required to do his/her job safely and in compliance with applicable regulations. The Contractor shall document and provide, upon request, qualifications, certifications, and licenses as required. Contractors conducting lead or asbestos abatement activities shall also provide a written abatement plan to the Safety & Environmental Branches for review and approval.

DRAFT

C.10.4 The Contractor shall provide each Contractor employee with the personal protective equipment required to do their job safely and in compliance with all applicable regulations.

C.10.5 Contractors working with ionizing radiation (radioactive material or machine sources) must comply with the latest revision of NAVSEA S0420-AA-RAD-010 (provided upon request). Prior to bringing radioactive materials or machine sources on base, the Contractor must notify the Command Radiation Safety Officer in the Safety Branch.

C.10.6 Contractors shall not procure hazardous material (HAZMAT) on behalf of NSWCDD without following the approved HAZMAT procurement process and obtaining approval from the Safety & Environmental Branches. For emergency HAZMAT purchases only, the Contractor shall alert the Safety & Environmental Branches and request a waiver to procure outside the HAZMAT procurement process. For emergency purchases, the Contractor shall submit an Authorized Use List Addition form and the Safety Data Sheet to the Safety & Environmental Branches for approval. Once the HAZMAT arrives onsite, the Contractor shall alert the Environmental Branch so that it can be barcoded and added to the inventory.

C.10.7 HAZMAT owned by the Contractor and brought into NSWCDD work spaces for temporary use shall be reviewed and approved by the Safety & Environmental Branches prior to use. The Contractor shall submit the Safety Data Sheet that must be routed through the Government supervisor responsible for the specific work area. This HAZMAT must clearly be marked that it is Contractor owned and shall not be stored in NSWCDD spaces.

C.10.8 Contractors shall not procure lithium batteries on behalf of NSWCDD without first receiving an approved Initial Procurement Report or certification letter and obtaining approval from the Safety & Environmental Branches.

C.10.9 Applicable Contractors shall submit Total Case Incident Rate (TCIR) and Days Away, Restricted and Transfer (DART) rates for the past three (3) years upon request by the Safety Branch. A Contractor meets the definition of applicable if its employees worked 1,000 hours or more in any calendar quarter onsite and where oversight is not directly provided in day-to-day activities by the command.

C.10.10 The Contractor shall report all work-related injuries/illnesses that occurred while working at NSWCDD, or an off-site location (including shipboard), to the Safety Branch.

C.11 INFORMATION SYSTEMS (IS) AND COMPUTER USAGE

In accordance with U.S. Navy policy, any personnel, including the Contractor, who utilizes DOD owned systems, shall assume responsibility for adherence to restrictions regarding internet and email usage. Navy policy prohibits racist, sexist, threatening, pornographic, personal business, subversive or politically partisan communications. All personnel, including the Contractor, are accountable and must act accordingly. DOD computer systems are monitored to ensure that the use is authorized, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. During monitoring, information may be

DRAFT

examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over a DOD system may be monitored. Use of a DOD system constitutes consent to monitoring. Unauthorized use may result in criminal prosecution. Evidence of unauthorized use collected during monitoring may be used as a basis for recommended administrative, criminal or adverse action.

C.12 USE OF INFORMATION SYSTEM (IS) RESOURCES

Except in special circumstances explicitly detailed elsewhere in this document, the Contractor shall provide all IS resources needed in the performance of this Task Order. This includes, but is not limited to computers, software, networks, certificates, and network addresses.

C.12.1 CONTRACTOR USE OF NSWCDD IS RESOURCES

(a) In the event that the Contractor is required to have access to NSWCDD IS resources, the login name used for access shall conform to the NMCI/Nautilus login naming convention. If the Contractor requires access to applications/systems that utilize client certificates for authentication, the Contractor is responsible for obtaining requisite certificates from a DOD or External Certificate Authority

(b) If this Task Order requires that the Contractor be granted access and use of NSWCDD IS resources (at any site), the IS shall be accredited for Contractor use in accordance with procedures specified by the Information Assurance Office.

C.12.2 CONNECTIONS BETWEEN NSWCDD AND CONTRACTOR FACLITIES

If there is a requirement (specifically delineated elsewhere in this Task Order) for interconnection (e.g., link level or Virtual Private Network (VPN)) between any facilities and/or ISs owned or operated by the Contractor and ISs owned or operated by NSWCDD, such interconnection shall take place only after approval from the Information Assurance Office. All such connections as well as the ISs connected thereto will be accredited in accordance with DOD policy (DODI 8510.01 Risk Management Framework for DoD Systems) by the cognizant Designated Approving Authority (DAA) and comply with the requirements of Chairman Joint Chiefs of Staff Instruction (CJCSI) 6211.02 (series) Defense Information Systems Network (DISN) Responsibilities regarding Memorandums of Agreement. All such connections will be made outside the appropriate NSWCDD firewall.

C.13 PRIVACY INFORMATION

Work under this Task Order may require that personnel have access to Privacy Information. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code Section 552a, FAR 52.224-2 Privacy Act, and applicable agency rules and regulations.

C.14 NON-DISCLOSURE AGREEMENTS (NDAs)

DRAFT

(a) Access to and preparation of sensitive information subject to Privacy Act and Business Sensitive safeguarding and destruction may be required in the execution of tasking associated with this Task Order. NDAs may be utilized to allow for access to company sensitive/proprietary or Privacy Act data. For tasks requiring NDAs, the Contractor shall obtain appropriate agreements for all their employees that are associated with the task requiring such an agreement.

(b) Contractor personnel may be required, from time to time, to sign NDAs as applicable to specific SOW tasking. The COR will notify the Contractor of the number and type of personnel that will need to sign the NDAs. The signed NDAs shall be executed prior to accessing data or providing support for information that must be safeguarded. Copies of all executed NDAs shall be provided to the COR for endorsement and retention.

C.15 NON-PERSONAL SERVICES/INHERENTLY GOVERNMENT FUNCTIONS

(a) The Government will neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. The Government will not direct the hiring, dismissal or reassignment of Contractor personnel. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual Contractor employees. 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 that personal services are being provided. If the Contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's responsibility to notify the Contracting Officer immediately in accordance with FAR 52.243-7 Notification of Changes(DEVIATION 2026-O0034).

(b) Inherently-Governmental functions are not within the scope of this Task Order. Decisions relative to programs supported by the Contractor shall be the sole responsibility of the Government. The Contractor may be required to attend technical meetings for the Government; however, they are not, under any circumstances, authorized to represent the Government or give the appearance that they are doing so.

C.16 CONTROL AND ADMINISTRATION OF CONTRACTOR PERSONNEL

(a) The Contractor shall comply with the requirements of NAVSEA and NSWCDD instructions regarding performance in Government facilities. All Contractor personnel engaged in work while on Government property shall be subject to all applicable DOD and Navy Standards of Conduct.

(b) The Contractor shall be required to obtain identification badges from the Government for all Contractor personnel requiring regular access to Government property. When on-site in Government office spaces, laboratories, test facilities, or ship assets, Contractor employees shall be clearly identified as a Contractor (e.g., utilizing badge identifications and sign identifications in office spaces). The identification badge shall be visible at all times while employees are on Government property. The Contractor shall furnish all requested information required to facilitate issuance of identification badges and shall conform to applicable regulations in the

Department of Defense Manual (DODM) 1000.13 DoD Identification (ID) Cards ID Card Life-Cycle concerning the use and possession of the badges.

(c) The Contractor shall ensure that all identification badges issued to Contractor employees are returned to the appropriate Security Office within 48 hours following completion of the Task Order, relocation or termination of an employee, and upon request by the Contracting Officer.

(d) All Contractor personnel shall identify their company affiliation when answering or making telephone calls and sending email and when attending meetings where Government personnel or representatives from other Contractors are present. In addition, Contractor personnel cannot lead/manage/supervise Government personnel. Contractor program/project managers shall be clearly identified and known as such by Government employees.

(e) All persons engaged in work while on Government property shall be subject to search of their persons (no bodily search) and vehicles at any time by the Government and shall report any known or suspected security violations to the appropriate Security Department. Assignment, transfer, and reassignment of Contractor personnel shall be at the discretion of the Contractor. However, when the Government directs, the Contractor shall remove from Task Order performance any person who endangers life, property, or national security through improper conduct.

C.17 TERMINATION OF EMPLOYEES WITH U.S. GOVERNMENT BADGES

(a) The Contractor shall ensure that all employees who have a DOD Common Access Card (CAC), turn in the CAC immediately upon employee separation and/or termination of their employment under this Task Order. The above requirement shall be made a part of the standard employee facility clearance procedures for all separated personnel. The Contractor shall advise Command Physical Security of all changes in their personnel requiring DOD base access.

(b) For involuntarily separated personnel and those separated under adverse circumstances, the Contractor shall notify Command Physical Security in advance of the date, time, and location where the Command representative retrieve the DOD CAC prior to the employee departing the Contractor's facility. In the event the employee is separated in his or her absence, the Contractor shall immediately notify Command Physical Security of the separation and make arrangements between the former employee and Command Physical Security for the return of the CAC. If circumstances arise which necessitate urgent revocation of a CAC after normal business hours, the Mission Partner Identity, Credential and Access Management (MP ICAM) Mission Partner Affiliation Sponsor (MPAS) shall be immediately contacted. MPAS contact information will be provided by the COR after Task Order award.

C.18 LABOR CATEGORIES/QUALIFICATIONS

See Attachment J.X, Labor Category Qualifications.

C.19 POST AWARD CONTRACTOR PERSONNEL APPROVAL

(a) See NAVSEA C-237-H002 Substitution of Key Personnel, regarding substitution of key personnel. Requests for post award approval of additional and replacement key personnel shall be submitted via email. Email submissions shall be made simultaneously to the Contract Specialist, COR, and the Alternate COR. Electronic notification via email from the Contract Specialist will serve as written approval or disapproval on behalf of the Contracting Officer. This approval is required before an individual may begin charging to the Task Order.

(b) Resumes shall be submitted in the format required in C.20. However, minor deviations in formatting may be overlooked, providing sufficient information is submitted for an independent comparison of the individual's qualifications with Labor Category requirements.

C.20 POST AWARD RESUME FORMAT AND CONTENT REQUIREMENTS

In order to facilitate evaluation of resumes submitted in accordance with C.19 and C-237-H002 Substitution of Key Personnel, all résumés shall be provided in the following format and are not to exceed three (3) pages each. The page limit does not apply to the certification and signature.

(a) HEADER

- Complete Name
- Current Employer
- Task Order Labor Category
- Contractor Labor Category
- Percentage of time to be allocated to this effort upon award of this Task Order
- Current security clearance level per DISS (identify if interim or final)
- Current work location
- Planned work location upon award of this Task Order

Note if the individual is key on another contract with a Period of Performance that will overlap this requirement. Note plans to satisfy both contracts if the candidate is approved.

(b) EDUCATION/PROFESSIONAL DEVELOPMENT

Show any degrees, honors, publications, professional licenses, specialized certifications, and other evidence of professional accomplishments that are directly relevant and will impact the Offeror's qualifications to perform under the Task Order. For education and training, the following format is preferred:

- Academic: degree(s); date(s); institution; major/minor
- Academic: course title, date(s), approximate length (as cited in labor categories)
- Non-Academic: course title, date(s), approximate length
- Professional licenses and specialized certifications. (Note the date obtained for each, as well as the date when each license/certification requires renewal.)

(c) CHRONOLOGICAL WORK HISTORY/EXPERIENCE

DRAFT

(i) Employer: dates (month/year); title(s) held

(ii) Work experience shall be presented separately for each employer, clearly marked with proper category of experience (i.e., relevant experience; nonrelevant experience.). If relevant and nonrelevant experience were obtained while at the same employer, separate time periods shall be noted for each assignment. Responsibilities shall be discussed in sufficient detail for each assignment so as to permit comparison with experience levels in Attachment J.X, Labor Category Qualifications. Specific examples of work assignments, accomplishments, and products shall be provided.

(iii) Phrases such as "assisted with," "participated in," or "supported" are unacceptable except as introductory to a detailed description of the actual work performed. If no such description is provided, the sentence or bulleted information will not be considered in the résumé evaluation process.

(iv) Résumé information is encouraged to be presented in bullet format.

(v) Lack of specific definition in job responsibilities, services performed, or products produced may be viewed as a lack of understanding of the Labor Category requirements.

(vi) All relevant military experience claimed shall be described such that each relevant tour is treated as a separate employer. Time frames/titles /responsibilities shall be provided in accordance with the level of detail prescribed above. Military experience not documented in this manner will not be considered.

(vii) Gaps in experience shall be explained.

(viii) Certification of correctness of information signed and dated by both the person named and the Contractor. The employee certification shall include the following statement:

CERTIFICATION: "I certify that the experience and professional development described herein are complete and accurate in all respects. I consent to the disclosure of my résumé for NSWCDD Task Order TBD by [insert company name] and intend to make myself available to work under the Task Order."

_____ _____

Employee Signature and Date Contractor Signature and Date

(ix) Résumés without this certification, together with either a handwritten or digital signature, will be unacceptable and will not be considered.

(x) If the employee is not a current employee of the Contractor (or a Sub-contractor), a copy of the accepted offer letter shall be provided. The letter shall identify the projected start date.

DRAFT

C.21 LABOR TRIPWIRE JUSTIFICATIONS

The Contractor shall monitor monthly average actual spend rates compared to monthly average fully burdened proposed rates on a per CLIN basis. The Contractor shall advise the COR and the Contract Specialist, by email, of any variation of actual-to-proposed rate averages greater than 15 percent. The Contractor's notification shall include the following information:

(a) an actual vs. proposed average dollar per hour comparison;

(b) the percentage variation between the actual and proposed average;

(c) explanation of what is causing the variation;

(d) whether or not the Contractor expects this condition is temporary or permanent;

(e) the Contractor's plan for addressing and correcting the variation; and

(f) additional information as requested by the Government to assist in reporting per the NAVSEAINST 4200.19(series) Planning, Use, and Control of Services Contracting.

C.22 DATA RIGHTS

(a) This is a Task Order for the provision of services by the Contractor. In accordance with law and policy and with the provisions of this Task Order, Contractor personnel shall perform as required by this Task Order, and such work shall include working in cooperation and collaboration with Government Personnel.

(b) Performance of this Task Order work shall require, among other things, the Contractor to access and use Government-owned data such as software, documentation, technical data, process and report templates, and the like. Any and all software, documentation, technical data, and the like generated from such access and use shall also be and remain Government-owned data and shall be included in an appropriate technical report or other deliverable. The Contractor's use of and access to Government-owned data shall neither constitute nor create any Contractor rights in or license to such data; the only Contractor permissions to use and access the data shall be those necessarily required by the Contractor to perform the work herein.

(c) On occasion and incidental to the provision of support services by the Contractor, the Contractor may be tasked to independently create discrete new data products (e.g., technical analysis, drawings) that do not derive from existing data. Such products shall be specifically identified by the Government in writing and shall be delivered pursuant to the appropriate Contract Data Requirements List (CDRL) document. Rights in such products shall be governed by the appropriate Task Order clauses.

C.23 DIGITAL DELIVERY OF DATA

DRAFT

(a) Delivery by the Contractor to the Government of certain technical data and other information is now frequently required to be made in digital form rather than in hardcopy form. The method of delivery of such data and/or other information (i.e., in electronic, digital, paper hardcopy, or other form) shall not be deemed to affect in any way either the identity of the information (i.e., as "technical data" or "computer software") or the Government's and the Contractor's respective rights therein.

(b) Whenever technical data and/or computer software deliverables required by this contract are to be delivered in digital form, any authorized, required, or permitted markings relating to the Government's rights in and to such technical data and/or computer software must also be digitally included as part of the deliverable and on or in the same medium used to deliver the technical data and/or software. Such markings must be clearly associated with the corresponding technical data and/or computer software to which the markings relate and must be included in such a way that the marking(s) appear in human-readable form when the technical data and/or software is accessed and/or used. Such markings must also be applied in conspicuous human-readable form on a visible portion of any physical medium used to effect delivery of the technical data and/or computer software. Nothing in this paragraph shall replace or relieve the Contractor's obligations with respect to requirements for marking technical data and/or computer software that are imposed by other applicable clauses such as, where applicable and without limitation, DFARS 252.227-7989, Rights in Technical Data, Computer Software, and Computer Software Documentation—Other Than Commercial Products and Commercial Services (DEVIATION 2026-O0036).

(c) Digital delivery means (such as but not limited to Internet tools, websites, shared networks, and the like) sometimes require, as a condition for access to and/or use of the means, an agreement by a user to certain terms, agreements, or other restrictions such as but not limited to "Terms of Use," licenses, or other restrictions intended to be applicable to the information being delivered via the digital delivery means. The Contractor expressly acknowledges that, with respect to deliverables made according to this contract, no such terms, agreements, or other restrictions shall be applicable to or enforceable with respect to such deliverables unless such terms, agreements, or other restrictions expressly have been accepted in writing by the Contracting Officer; otherwise, the Government's rights in and to such deliverables shall be governed exclusively by the terms of this Task Order.

[This paragraph should be deleted if you do not require the Contractor to operate Government vehicles during your contracting efforts.]

C.24 OPERATION OF GOVERNMENT VEHICLES

(a) The Contractor shall be required to drive Government vehicles both onsite at NSWCDD and offsite in the performance of duties associated with the tasking of this Task Order. Government provided vehicles shall be used solely for the purposes as described in the SOW. All drivers must present proof of a valid state driver's license prior to operating a Government vehicle. A valid state driver's license shall be accepted as proper authority for operation of vehicles up to and including 10,000 pounds gross vehicle weight and carrying less than 15 passengers. For vehicles over 10,000 pounds and carrying more than 15 passengers a valid state driver's license

and proof of required Navy training for vehicle are required. The state driver's license must be valid for the class and weight of the vehicle which the Contractor will be operating.

(b) An authorized drivers list shall be added to the Monthly Status Report and maintained by the Contractor. The Contractor shall submit within the preceding 30 days a Department of Motor Vehicles (DMV) driving record to the COR for review and approval, prior to adding an individual to the Authorized Driver List. No Driving Under the Influence (DUI) or Driving While Intoxicated (DWI) convictions in the past 11 years will be considered.

(c) The Contractor may be required to operate specialized Government vehicles such as tanks, Mine Resistant Ambush Protected (MRAP) Vehicle, Amphibious Assault Vehicle (AAV), High Mobility Multipurpose Wheeled Vehicle (HMMWV) etc. Government provided vehicles will be used solely for the purposes as described in the Statement of Work and, if applicable, Technical Instructions or work areas of this contract. All operators must have completed the appropriate NSWCDD-determined training syllabus.

(d) The Contractor may be required to operate Government-owned waterborne vessels both on-site at NSWC Dahlgren and off-site at various test range locations in the performance of duties associated with the tasking of this Task Order. Government provided vessels will be used solely for the purposes as described in the SOW. All operators must have completed the appropriate NSWCDD training syllabus and/or have a U.S. Coast Guard license.

C.25 SHIPBOARD PROTOCOL

(a) This tasking may involve platform engineering and fleet support onboard ship. As such, the Contractor is reminded of its responsibility to assure that shipboard protocol is stringently followed. Specifically, visit clearances must be arranged through the Government sponsor and must be forwarded to the individual command being visited as well as to all supporting commands, such as the base, squadron, tender, etc. that the visitor must pass through to get to the ship; the Contractor is responsible for obtaining and maintaining specialized training (i.e. nuclear awareness, safety, quality control, etc.) and certification (i.e. Submarine Safety Program (SUBSAFE) certificates etc.); personnel performing on board US Navy Ships must have at a minimum, a current SECRET Security Clearance; if not led by a Government representative the Contractor is responsible for briefing the ship/command upon arrival; and the Contractor is responsible for debriefing the ship/command upon departure to include operational status of the equipment.

(b) The Contractor shall ensure its personnel adhere to these requirements when performing shipboard tasking. Compliance shall be reported in the trip report (CDRL A00X).

(c) All assigned personnel must possess, at a minimum, a current SECRET Security Clearance.

(d) All personnel, while shipboard, shall conform to the rules and regulations of the ship. It is the responsibility of the Contractor to determine the proper rules, regulations, actions, policy and procedures.

(e) Alarms - actual or drill - shall be reported and procedures appropriately adhered.

(f) Safety - hardhats, tag-outs, safety shoes, goggles, safety harnesses, etc., as appropriate - shall be utilized.

(g) Some shipboard tasking may require ascending and descending vertical ladders to and from the highest points of the ship both pier side and underway.

(h) Each Contractor employee must be able stand; walk; climb stairs; balance; stoop; kneel; crouch or crawl around and lift a maximum of 50 lbs. (single person) in the test environment.

(i) HAZMAT must be used safely according to local Standard Operating Procedures (SOPs).

(j) The designated team lead shall, upon arrival, brief the Commanding Officer or his/her designated representative as to the purpose of the visit and expected duration.

(k) The designated team lead shall, upon final departure, debrief the Commanding Officer or his/her designated representative as to the success of the tasking and the operational condition of affected equipment.

(l) The Contractor shall comply with the Commander, U.S Fleet Forces Command (COMUSFLTFORCOM)/Commander, U.S. Pacific Fleet (COMPACFLT) INSTRUCTION 6320.3B regarding the medical and dental screening of all personnel that may embark aboard any U.S. Navy vessel.

(m) The Contractor shall ensure that repair and maintenance employees working aboard vessels, dry docks and piers shall have a valid 10 hour OSHA Maritime Shipyard Employment Course #7615 completion card within 60 days of employment.

C.26 GOVERNMENT FLIGHT REPRESENTATIVE

The contractor is required to provide personnel capable of conducting ground and flight test operations. These individuals shall have the ability to meet requirements necessary to obtain an operations support physical or obtain a FAA Flying Class III medical certificate or better. In addition to these clearances, flight test personnel shall obtain physiological training to support unpressurized operations on military or non-standard aviation (NSAV) aircraft, as required, operating below 25,000 feet. Flight tests will occur at Eglin AFB, FL, Dahlgren, VA, Waco, TX, NSWC China Lake, CA, White Sands Missile Range, NM, Pacific Missile Range Facility, HI, and Cannon AFB, NM; and other locations as required. In some instances OCONUS flight support may be necessary. Dismounted testing personnel will be required to achieve and maintain needed qualifications to perform Joint Terminal Attack Controller Evaluator Qualifications and shall obtain physiological training to support unpressurized operations on military or non-standard aviation (NSAV) aircraft, as required, operating below 25,000 feet. Dismounted Ground Test/Flight tests will occur at Hurlburt Field, FL, Eglin AFB, FL, and other locations as required. In some instances OCONUS testing support may be necessary.

C.27 SECTION C CLAUSES INCORPORATED BY FULL TEXT

C-202-H001 ADDITIONAL DEFINITIONS—BASIC (NAVSEA) (OCT 2018)

(a) Department - means the Department of the Navy.

(b) Commander, Naval Sea Systems Command - means the Commander of the Naval Sea Systems Command of the Department of the Navy or his duly appointed successor.

(c) References to The Federal Acquisition Regulation (FAR) - All references to the FAR in this contract shall be deemed to also reference the appropriate sections of the Defense FAR Supplement (DFARS), unless clearly indicated otherwise.

(d) National Stock Numbers - Whenever the term Federal Item Identification Number and its acronym FIIN or the term Federal Stock Number and its acronym FSN appear in the contract, order or their cited specifications and standards, the terms and acronyms shall be interpreted as National Item Identification Number (NIIN) and National Stock Number (NSN) respectively which shall be defined as follows:

(1) National Item Identification Number (NIIN). The number assigned to each approved Item Identification under the Federal Cataloging Program. It consists of nine numeric characters, the first two of which are the National Codification Bureau (NCB) Code. The remaining positions consist of a seven digit non-significant number.

(2) National Stock Number (NSN). The National Stock Number (NSN) for an item of supply consists of the applicable four-position Federal Supply Class (FSC) plus the applicable nine-position NIIN assigned to the item of supply.

C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)

(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained. These official files may contain information that is considered a trade secret, proprietary, business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as “protected information”. File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein.

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that:

(1) The support contractor not disclose any information;

(2) Individual employees are to be instructed by the support contractor regarding the sensitivity of the official contract files;

(3) The support contractor performing these services be barred from providing any other supplies and/or services, or competing to do so, to NAVSEA for the period of performance of its contract and for an additional three years thereafter unless otherwise provided by law or regulation; and,

(1) In addition to any other rights the contractor may have, it is a third party beneficiary who has the right of direct action against the support contractor, or any person to whom the support contractor has released or disclosed protected information, for the unauthorized duplication, release, or disclosure of such protected information.

(c) Execution of this contract by the contractor is considered consent to NAVSEA's permitting access to any information, irrespective of restrictive markings or the nature of the information submitted, by its file room management support contractor for the limited purpose of executing its file room support contract responsibilities.

(d) NAVSEA may, without further notice, enter into contracts with other contractors for these services. Contractors should enter into separate non-disclosure agreements with the file room contractor. Contact the Procuring Contracting Officer for contractor specifics. However, any such agreement will not be considered a prerequisite before information submitted is stored in the file room or otherwise encumber the government.

C-204-H002 IMPLEMENTATION OF ENHANCED SECURITY CONTROLS ON SELECT DEFENSE INDUSTRIAL BASE PARTNER NETWORKS (NAVSEA) (SEP 2024)

1. System Security Plan and Plans of Action and Milestones (SSP/POAM) Reviews

a) Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which is included in this contract. The Contractor shall fully cooperate in the Government's review of the SSPs at the Contractor's facility.

b) If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The contracting officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a plan of action and milestones (POAM) for the correction of the identified deficiencies. The Contractor shall immediately notify the

contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.

c) Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the Contractor's facilities. The Government may continue to conduct follow-on reviews until the Government determines that the Contractor has corrected all identified deficiencies in the SSP(s).

d) The Government may, in its sole discretion, conduct subsequent reviews at the Contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of contract award) and may conduct such reviews at any time upon thirty (30) days' notice to the Contractor.

2. Compliance to NIST 800-171

a) The Contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 2) (NIST SP 800-171), or establish a SSP(s) and POA&Ms that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered contractor information systems affecting this contract.

b) Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

(1) Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

(2) Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

(3) Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods.

(4) Audit user privileges on at least an annual basis;

(5) Implement:

DRAFT

i. Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POAM); and,

ii. NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program);

(6) Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.

(7) Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

3. Cyber Incident Response

a) The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

b) Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx. In delivery of the incident data, the Contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.
F
c) If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

4. Naval Criminal Investigative Service (NCIS) Outreach

The Contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

5. NCIS/Industry Monitoring

a) In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the Naval Criminal Investigative Service (NCIS), which may include cooperation related to: threat

indicators; pre-determined incident information derived from the Contractor's infrastructure systems; and the continuous provision of all Contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

b) If the Government determines that the collection of all logs does not adequately protect its interests, the Contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the Contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the Contractor. In the alternative, the Contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the Contractor.

c) In all cases, the collection or provision of data and any activities associated with this statement of work shall be in accordance with federal, state, and non-US law

C-211-H016 SPECIFICATIONS AND STANDARDS (NAVSEA) (OCT 2018)

(a) Definitions.

(i)A "zero-tier reference" is a specification, standard, or drawing that is cited in the contract (including its attachments).

(ii)A "first-tier reference" is either: (1) a specification, standard, or drawing cited in a zero-tier reference, or (2) a specification cited in a first-tier drawing.

(b) Requirements. All zero-tier and first-tier references, as defined above, are mandatory for use. All lower tier references shall be used for guidance only unless specifically identified below.

C-211-H017 UPDATING SPECIFICATIONS AND STANDARDS (NAVSEA) (DEC 2018)

The contractor may request that this contract be updated to include the current version of the applicable specification or standard if the update does not affect the form, fit or function of any deliverable item or increase the cost/price of the item to the Government. The contractor should submit update requests to the Procuring Contracting Officer with copies to the Administrative Contracting Officer and cognizant program office representative for approval. The contractor shall perform the contract in accordance with the existing specifications and standards until notified of approval/disapproval of its request to update by the Procuring Contracting Officer. Any approved alternate specifications or standards will be incorporated into the contract.

DRAFT

C-211-H018 APPROVAL BY THE GOVERNMENT (NAVSEA) (JAN 2019)

Approval by the Government as required under this contract and applicable specifications shall not relieve the Contractor of its obligation to comply with the specifications and with all other requirements of the contract, nor shall it impose upon the Government any liability it would not have had in the absence of such approval.

C-212-W002 COMMERCIAL SUPPLIER AGREEMENTS (NAVSEA) (MAR 2019)

(a) Commercial Supplier Agreement means End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement.

(b) Any Commercial Supplier Agreement must be provided in full text as part of a quote or offer without hyperlinks.

(c) The contract/order Schedule and Federal Acquisition Regulation (FAR) 52.212-4, Contract Terms and Conditions—Commercial Items, shall take precedence over any conflicting provisions in a Commercial Supplier Agreement.

(d) If any requirement in the Commercial Supplier Agreement conflicts with Federal law or regulations (see FAR 12.212(a)), the following shall apply:

(i) Any such requirement is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such requirement by virtue of it appearing in the Commercial Supplier Agreement. If the Commercial Supplier Agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such requirement.

(iii) Any such requirement is deemed to be stricken from the Commercial Supplier Agreement.

(e) Automatic renewals. License Agreements will expire at end of the term identified in the Purchase Order/Contract. Automatic renewals are not permitted and any such provision is void.

(f) Changes to the Commercial Supplier Agreement. Unilateral changes of the Commercial Supplier Agreement are impermissible and any requirement authorizing such changes is unenforceable. Changes must be in writing and executed by both parties to be effective.

(g) Third Part License (Embedded Software).

DRAFT

(i) The Contractor agrees that it has obtained all necessary licenses for the Government for any third party materials (including without limitation all Open Source licenses) provided within the product.

(ii) Contractor agrees that it complies with and shall continue to comply with all of its obligations under Third Party Licenses (including without limitation all Open Source licenses) associated with any third party materials provided within each product.

(iii) To the extent that the Government's use of the software products licensed herein is in compliance with the Contractor's Commercial Supplier Agreement, the Government's use will also be in compliance with any Third Party Licenses.

(h) Audits. In lieu of any audit provisions in the Commercial Supplier Agreement, the Government agrees that, no more than once every twelve (12) months or within a reasonable time after a transfer, the Contractor shall, upon reasonable notice, have the right to require that the Government conduct an internal audit to ascertain and verify the number of licenses in use and to verify that the Government's use of the product is in conformity with this Agreement. The Government is not required to use any tools provided by the Contractor to conduct the audit and shall not be required to pay for any tools provided by the Contractor to conduct the audit. The results of any such audit shall be kept confidential.

If verification discloses that the Government's use is not in conformity with this Agreement, the Government agrees to resolve any noncompliance by either removing or correcting the unlicensed installation and use of the software identified by the audit as not in conformity with this Agreement.

(i) Confidentiality. Commercial Supplier Agreements' terms and the final contract pricing may not be deemed confidential. Other marked confidential information will be appropriately guarded.

(j) Assignment. The Government shall have the right, without the prior written consent of the Contractor or its authorized resellers, to assign, reassign, or transfer software licenses among Government employees or the Government's rights in the Contractor's product to any governmental organization that is managed, operated, or controlled by the Government.

Such authorization includes sublicensing, and assignment or transfer among or between authorized users. In the event authorized users are reorganized or restructured such that their responsibilities and operations are transferred to another government agency, the agency shall have the right to assign the affected program licenses to a successor agency. The licensed agency and the successor agency agree to be bound to the Commercial Supplier Agreement as modified. The transferee shall be bound by the license metrics and limitations in this license. Government shall complete any documentation required by the Contractor to facilitate the transfer of this license, and continuation of support shall be the responsibility of the transferee.

DRAFT

For the avoidance of doubt, any assignment or transfer of licenses of the Contractor's products is also subject to all other terms of the Commercial Supplier Agreement, as well as the Contractor's policies governing product dependencies and version compatibility. Reassignment does not require that the license be under maintenance or support in order to execute a transfer.

(k) Litigation. Any requirement insisting that the commercial supplier or licensor control any litigation arising from the government's use of the contractor's supplies or services is deleted and unenforceable.

(l) Equitable Remedies. Equitable remedies, injunctive relief, and binding arbitration requirements shall not be enforced unless explicitly authorized by agency guidance or statute.

(m) Venue. Any claim or dispute shall be resolved under the Contract Disputes Act and FAR 52.233-1. The forum for resolution of disputes and applicable statutes of limitation shall be governed by federal law.

(n) Applicable law. In accordance with FAR 52.233-4, United States law shall apply to resolve any claim of breach of this contract and such actions shall be handled in the applicable Federal court of jurisdiction.

C-215-H002 CONTRACTOR PROPOSAL (NAVSEA) (OCT 2018)

(a) Performance of this contract by the Contractor shall be conducted and performed in accordance with detailed obligations to which the Contractor committed itself in Proposal dated in response to NAVSEA Solicitation No. .

(b) The technical volume(s) of the Contractor's proposal is(are) hereby incorporated by reference and made subject to the "Order of Precedence" (FAR 52.215-8) clause of this contract. Under the "Order of Precedence" clause, the technical volume(s) of the Contractor's proposal referenced herein is (are) hereby designated as item (f) of the clause, following "the specifications" in the order of precedence.

C-223-W001 ACCIDENT REPORTING (NAVSEA) (OCT 2018)

(a) In accordance with DFARS 252.223-7002 (d), the Contractor shall immediately notify the Administrative Contracting Officer (ACO) and Procuring Contracting Officer (PCO) following an accident or incident. Also, the Contractor shall provide a written report within (insert number of days) days of the accident or incident containing, at a minimum, the following:

(1) Location, date and local time of the occurrence;

(2) Category of accident (fire, explosion, natural disaster, etc.);

(3) Identification of equipment, material and type of activity involved;

(4) Contract number;

(5) Procuring activity (name of PCO and ACO);

(6) Narrative of occurrence, including cause(s), if known;

(7) Personnel involved and degree of injury, if any. Specify whether Contractor and/or Government personnel;

(8) Assessment of damage. Estimate in dollars for contractor and/or government owned material, property, equipment;

(9) Was a news release made? If so, by whom? If not, will a news release be made?

(10) Was a request made for any assistance?

(11) Will there be any effect on production? If so, explain in detail.

(12) Corrective action taken, if any.

(13) Name and title of person submitting this report.

(b) The Contractor shall forward weekly written reports to the ACO and PCO until the accident or incident no longer affects production or when contract deliveries are on schedule.

C-223-W002 ON-SITE SAFETY REQUIREMENTS (NAVSEA) (OCT 2018)

(a) The contractor shall ensure that each contractor employee reads any necessary safety documents within 30 days of commencing performance at any Government facility. Required safety documents can be obtained from the respective safety office. Contractors shall notify the Safety office points of contact below to report completion of the required training via email. The email shall include the contractor employee's name, work site, and contract number.

(b) It is expected that contractor employees will have received training from their employer on hazards associated with the areas in which they will be working and know what to do in order to protect themselves. Contractors are required to adhere to the requirements of 29 CFR 1910, 29 CFR 1926 and applicable state and local requirements while in Government spaces. The contractor shall ensure that all on-site contractor work at the Government facility is in accordance with any local safety instructions as provided via the COR. The contractor shall report all work-related injuries/illnesses that occurred while working at the Government site to the COR.

(c) Contractors whose employees perform work within Government spaces in excess of 1000 hours per calendar quarter during a calendar year shall submit the data elements on OSHA Form 300A, Summary of Work Related Injuries and Illnesses, for those employees to the safety office , via the COR by 15 January for the previous calendar year, even if no work related injuries or illnesses occurred. If a contractor's injury/illness rates are above the Bureau of Labor Statistics

industry standards, a safety assessment may be performed by the Safety Office to determine if any administrative or engineering controls can be utilized to prevent further injuries/illnesses, or if any additional Personal Protective Equipment or training will be required.

(d) Any contractor employee exhibiting unsafe behavior may be removed from the Government site. Such removal shall not relieve the contractor from meeting its contractual obligations and shall not be considered an excusable delay as defined in FAR 52.249-14.

(e) The Safety Office points of contacts are as follows:

_____ [insert name and code]

C-227-H006 DATA REQUIREMENTS (NAVSEA) (OCT 2018)
The data to be furnished hereunder shall be prepared in accordance with the Contract Data Requirements List, DD Form 1423, Exhibit(s) , attached hereto.

C-227-H007 SOFTWARE DEVELOPMENT REQUIREMENTS (NAVSEA) (OCT 2018)

(a) The contractor shall define a general Software Development Plan (SDP) appropriate for the computer software effort to be performed under this contract. The SDP shall be delivered to the Government for concurrence under CDRL and shall not vary significantly from that proposed to the Government for evaluation for award. The contractor shall follow the Government concurred with SDP for all computer software to be developed or maintained under this effort. Any changes, modifications, additions or substitutions to the SDP also require prior Government concurrence.

(b) The SDP shall, at a minimum:

(1) Define the contractor's proposed life cycle model and the processes used as a part of that model. In this context, the term "life cycle model" is as defined in IEEE Std. 12207:2017;

(2) Contain the information defined by ISO/IEC/IEEE 15289:2017, section 7.3 “Plan - generic content” and Table 2 “Mapping of ISO/IEC 12207:2008 (IEEE Std. 12207:2008) Clauses to Information Items for Each Software Life Cycle Process.” In all cases, the level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted for this contract;

(3) Identify the specific standards, methods, tools, actions, strategies, and responsibilities associated with development and qualification;

(4) Document all processes applicable to the system to be acquired, including the Primary, Supporting, and Organizational life cycle processes as defined by IEEE Std. 12207:2017 as appropriate. Such processes shall be equivalent to those articulated by CMMI®;

(5) Adhere to the characteristics defined in ISO/IEC/IEEE 15289:2017 section 6.1 "Life-cycle data characteristics," as appropriate;

(6) Be in accordance with the framework defined in IEEE Std. 12207:2017, including, but not limited to, defining the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks;

(7) Contain a level of information sufficient to allow the use of the SDP as the full guidance for the developers. In accordance with ISO/IEC/IEEE 15289:2017 Section 7.3, such information shall at a minimum contain, specific standards, methods, tools, actions, reuse strategy, and responsibility associated with the development and qualification of all requirements, including safety and security.

C-227-H009 ACCESS TO DATA OR COMPUTER SOFTWARE WITH RESTRICTIVE MARKINGS (NAVSEA) (JAN 2019)

(a) Performance under this contract may require that the Contractor have access to technical data, computer software, or other sensitive data of another party that contains restrictive markings. If access to such data or software is required or to be provided, the Contractor shall enter into a written agreement with such party prior to gaining access to such data or software. The agreement shall address, at a minimum, (1) access to, and use of, the restrictively marked data or software exclusively for the purposes of performance of the work required by this contract, and (2) safeguards to protect such data or software from unauthorized use or disclosure for so long as the data or software remains properly restrictively marked. In addition, the agreement shall not impose any limitation upon the Government or its employees with respect to such data or software. A copy of the executed agreement shall be provided to the Contracting Officer. The Government may unilaterally modify the contract to list those third parties with which the Contractor has agreement(s).

(b) The Contractor agrees to: (1) indoctrinate its personnel who will have access to the data or software as to the restrictions under which access is granted; (2) not disclose the data or software to another party or other Contractor personnel except as authorized by the Contracting Officer; (3) not engage in any other action, venture, or employment wherein this information will be used, other than under this contract, in any manner inconsistent with this requirement; (4) not disclose the data or software to any other party, including, but not limited to, joint venturer, affiliate, successor, or assign of the Contractor; and (5) reproduce the restrictive stamp, marking, or legend on each use of the data or software whether in whole or in part.

(c) These restrictions on use and disclosure of the data and software also apply to information received from the Government through any means to which the Contractor has access in the performance of this contract that contains restrictive markings.

(d) The Contractor agrees that it will promptly notify the Contracting Officer of any attempt to gain access to any information with restrictive markings. Such notification shall include the

name and organization of the individual, company, or Government representative seeking access to such information.

(e) The Contractor shall include this requirement in subcontracts of any tier which involve access to information covered by paragraph (a), substituting "subcontractor" for "Contractor" where appropriate.

(f) Compliance with this requirement is a material requirement of this contract.

C-227-H010 COMPUTER SOFTWARE AND COMPUTER DATA BASES DELIVERED TO OR RECEIVED FROM THE GOVERNMENT (NAVSEA) (JAN 2019)

(a) The Contractor agrees to test for viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4, in all computer software and computer data bases (as defined in the clause entitled “Rights In Noncommercial Computer Software and Noncommercial Computer Software Documentation” (DFARS 252.227-7014)), before delivery of that computer software or computer data base in whatever media and on whatever system the computer software or data base is delivered whether delivered separately or imbedded within delivered equipment. The Contractor warrants that when delivered any such computer software and computer data base shall be free of viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1.

(b) The Contractor agrees that prior to use under this contract, it shall test any computer software and computer data base received from the Government for viruses, malware, Trojan Horses, and other security threats listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4.

(c) Any license agreement governing the use of any computer software or computer software documentation delivered to the Government as a result of this contract must be paid-up, irrevocable, world-wide, royalty-free, perpetual and flexible (user licenses transferable among Government employees and personnel under Government contract).

(d) The Contractor shall not include or permit to be included any routine to enable the contractor or its subcontractor(s) or vendor(s) to disable the computer software or computer data base after delivery to the Government.

(e) No copy protection devices or systems shall be used in any computer software or computer data base delivered under this contract with unlimited or Government purpose rights (as defined in DFARS 252.227-7013 and 252.227-7014) to restrict or limit the Government from making copies.

(f) It is agreed that, to the extent that any technical or other data is computer software by virtue of its delivery in digital form, the Government shall be licensed to use that digital-form data with exactly the same rights and limitations as if the data had been delivered as hard copy.

DRAFT

(g) Any limited rights legends or other allowed legends placed by a Contractor on technical data or other data delivered in digital form shall be digitally included on the same media as the digital-form data and must be associated with the corresponding digital-form technical data to which the legend(s) apply to the extent possible. Such legends shall also be placed in human-readable form on a visible surface of the media carrying the digital-form data as delivered, to the extent possible.

C-228-H002 MINIMUM INSURANCE REQUIREMENTS (NAVSEA) (JAN 2019)

(a) In accordance with the clause(s) of this contract entitled "Insurance--Work On a Government Installation" (FAR 52.228-5) and "Liability and Insurance" (DFARS 252.217-7012), as applicable, the Contractor shall procure and maintain insurance, of at least the kinds and minimum amounts set forth below:

(i) Workers' compensation and employer's liability coverage shall be at least $100,000, except as provided in FAR 28.307-2(a), if applicable

(ii) Bodily injury liability insurance coverage shall be written on the comprehensive form of policy of at least $500,000 per occurrence.

(iii) Automobile liability policies covering automobiles operated in the United States shall provide coverage of at least $200,000 per person and $500,000 per occurrence for bodily injury and $20,000 per occurrence for property damage. The amount of liability coverage on other policies shall be commensurate with any legal requirements of the locality and sufficient to meet normal and customary claims.

(b) To be approved by the Contracting Officer, insurance certificates must include the following cancellation policy statement: Prior to cancellation or material change in coverage, the contractor shall give 30 days written notice to the Contracting Officer.

(c) Physical work cannot begin until the insurance certificate has been approved by the Contracting Officer. Failure to provide an acceptable insurance certificate will not remove the contractor's responsibility to meet the delivery requirements outlined in Section F and FAR 52.211-11, Liquidated Damages – Supplies, Services, or Research and Development, if applicable.

C-237-H002 SUBSTITUTION OF KEY PERSONNEL (NAVSEA) (OCT 2018)

(a) The Contractor agrees that a partial basis for award of this contract is the list of key personnel proposed. Accordingly, the Contractor agrees to assign to this contract those key persons whose resumes were submitted with the proposal necessary to fulfill the requirements of the contract. No substitution shall be made without prior notification to and concurrence of the Contracting Officer in accordance with this requirement. Substitution shall include, but not be limited to, subdividing hours of any key personnel and assigning or allocating those hours to another individual not approved as key personnel.

DRAFT

(b) All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The Contracting Officer shall be notified in writing of any proposed substitution at least forty-five (45) days, or ninety (90) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include: (1) an explanation of the circumstances necessitating the substitution; (2) a complete resume of the proposed substitute; (3) an explanation as to why the proposed substitute is considered to have equal or better qualifications than the person being replaced; (4) payroll record of the proposed replacement; and (5) any other information requested by the Contracting Officer to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

(c) Key personnel are identified in an attachment in Section J.

C-237-W001 ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (eCRAFT) SYSTEM REPORTING (NAVSEA) (FEB 2026)

(a) The Contractor agrees to upload the Contractor's Funds and Man-hour Expenditure Reports in the Electronic Cost Reporting and Financial Tracking (eCRAFT) System and submit the Contract Status Report on the day and for the same timeframe the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination.

(b) The Contract Status Report indicates the progress of work and the status of the program and of all assigned tasks. It informs the Government of existing or potential problem areas.

(c) The Contractor's Fund and Man-hour Expenditure Report reports contractor expenditures for labor, materials, travel, subcontractor usage, and other contract charges.

(1) Access: eCRAFT: Reports are uploaded through the eCRAFT System Periodic Report Utility (EPRU). The EPRU spreadsheet and user manual can be obtained at: https://www.navsea.navy.mil/Home/Warfare-Centers/NUWC-Newport/Partnerships/Commercial-Contracts/Information-eCraft-/ under eCRAFT information. The link for eCRAFT report submission is: https://www.pdrep.csd.disa.mil/pdrepweb/ecraft. If you have problems uploading reports, please see the Frequently Asked Questions at the site address above.

(2) Submission and Acceptance/Rejection: The contractor shall submit their reports on the same day and for the same timeframe the contractor submits an invoice in WAWF. The amounts shall be the same. eCRAFT acceptance/rejection will be indicated by e-mail notification from eCRAFT.

C-239-W001 ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) ACCESSIBILITY STANDARDS/SECTION 508 COMPLIANCE (NAVSEA) (OCT 2018)

DRAFT

(a) Requirements for accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) are determined to be relevant for product(s)/service(s) procured under this solicitation.

(b) Each Electronic and Information Technology (EIT) item or service provided under this contract shall comply with the EIT Accessibility Standards listed below:

_____ 36 C.F.R. § 1194.21 - Software applications and operating systems

_____ 36 C.F.R. § 1194.22 - Web-based and internet information and applications

_____ 36 C.F.R. § 1194.23 - Telecommunications products

_____ 36 C.F.R. § 1194.24 - Video and multimedia products

_____ 36 C.F.R. § 1194.25 - Self-contained, closed products

_____ 36 C.F.R. § 1194.26 - Desktop and portable computers

_____ 36 C.F.R. § 1194.31 - Functional Performance Criteria

_____ 36 C.F.R. § 1194.41 - Information, Documentation, and Support

(c) For more information on Voluntary Product Accessibility Template (VPAT) and Government Product/Service Accessibility Template (GPAT) please refer to: http://www.buyaccessible.gov/ or http://www.section508.gov/content/sell/vpat.

(d) The Contractor shall comply with the VPAT or GPAT document submitted. If the Contracting Officer determines that any item or service delivered under this contract does not comply with the EIT Accessibility Standards, the Contracting Officer will notify the Contractor in writing accordingly. If the Contractor fails to promptly correct or replace the nonconforming products or services with conforming products or services within the delivery schedule contained in the contract, the Government will have the rights and remedies contained in the basic contract.

C-242-H001 EXPEDITING CONTRACT CLOSEOUT (NAVSEA) (OCT 2018)

(a) As part of the negotiated fixed price or total estimated amount of this contract, both the Government and the Contractor have agreed to waive any entitlement that otherwise might accrue to either party in any residual dollar amount of $1,000 or less at the time of final contract closeout. The term "residual dollar amount" shall include all money that would otherwise be owed to either party at the end of the contract, except that, amounts connected in any way with taxation, allegations of fraud and/or antitrust violations shall be excluded. For purposes of determining residual dollar amounts, offsets of money owed by one party against money that would otherwise be paid by that party may be considered to the extent permitted by law.

DRAFT

(b) This agreement to waive entitlement to residual dollar amounts has been considered by both parties. It is agreed that the administrative costs for either party associated with collecting such small dollar amounts could exceed the amount to be recovered.

C-242-H002 POST AWARD MEETING (NAVSEA) (OCT 2018)

(a) A post-award meeting with the successful offeror will be conducted within [*] days after award of the [contract / task order]. The meeting will be held at the address below:

Location/Address: [*]

(b) The contractor will be given [*] working days notice prior to the date of the meeting by the Contracting Officer.

(c) The requirement for a post-award meeting shall in no event constitute grounds for excusable delay by the contractor in performance of any provisions in the [contract / task order].

(d) The post-award meeting will include, but is not limited to, the establishment of work level points of contact, determining the administration strategy, roles and responsibilities, and ensure prompt payment and close out. Specific topics shall be mutually agreed to prior to the meeting.

[*] To be specified at [contract / task order] award

C-242-H003 TECHNICAL INSTRUCTIONS (NAVSEA) (OCT 2018)

(a) Performance of the work hereunder may be subject to written technical instructions signed by the Contracting Officer and the Contracting Officer's Representative specified in Section G of this contract. As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of drawings, specifications or technical portions of work description.

(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "CHANGES" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.

(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such

DRAFT

instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.

(d) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

C-243-H003 CONFIGURATION MANAGEMENT (NAVSEA) (APR 2024)

(a) Baseline Definition - All contractual documentation in effect at the time of contract award shall constitute the Contract Baseline, which shall be considered incorporated in the baseline documentation.

(b) General Requirement –

(1) The Contractor shall maintain a Configuration Control Program to assure that all detail level work being performed under this contract is in compliance with appropriate baseline documentation. The Contractor shall prepare a Configuration Management Plan in accordance with the requirements of the contract. If required, the Contractor's Configuration Management Plan shall be submitted through the appropriate Contract Data Requirements List (CDRL) for approval by the Government.

(2) Whenever a situation arises wherein the Contractor cannot comply with a baseline document, or whenever intent of such documentation is significantly changed by detail level documentation, the Contractor shall submit change documents to modify the baseline to resolve the conflict or to allow non-compliance. Whenever the cost of implementing a proposed change is less than the threshold requiring certified cost or pricing data, the Contractor shall provide such detail of related costs as to allow the Government to determine an equitable adjustment for the change document submission. Whenever the contract cost changes by an amount greater than the threshold requiring certified cost or pricing data, the Contractor shall complete such cost and pricing data as the Contracting Officer shall require detailing all related costs, and attach it to the change document. Requirements for cost and pricing data shall be determined by the gross amount of the change unless otherwise directed by the Contracting Officer. Change documentation shall be submitted to the Contracting Officer in accordance with the appropriate CDRL, and as described in paragraphs (c) through (f) below.

(c) Engineering Change Proposals (ECPs) - ECPs shall be prepared in accordance with the approved configuration management plan and the requirements of the contract. DI-SESS-80639E approved 11 February 2020, EIA-649-1A dated 10 August 2020, and MIL-HDBK-61B dated 7 April 2020 apply. An ECP shall be submitted whenever the detail level physical configuration, material quality, operational or functional performance of equipment or installed systems will not be in compliance with baseline design-related documents (Specifications, Contract Drawings, etc.), and a change to the baseline document is considered an appropriate means of resolving a design-related issue. The contractor shall develop documentation in

DRAFT

sufficient detail to enable Government review and evaluation of the merits of the proposed change, including cost and scheduling impact, ship class impact if applicable, and consequences if disapproved. List all existing drawings and technical manuals impacted by the change, including a brief narrative explanation of needed changes to incorporate the ECP if approved. Provide weight and moment data incidental to the change, if applicable. The Contractor shall also prepare applicable baseline document insert sheets, with specific word changes or proposed rewrite, to facilitate baseline documentation changes.

(d) Non-Engineering Change Proposals (NECPs) – An NECP shall be submitted whenever necessary to document administrative, procedural, scheduling, or documentation changes that do not directly impact the physical configuration of the equipment. The NECP shall explain the nature of the problem, identify the applicable baseline document (i.e., Contract Data Requirement List (CDRL), Contract Clause, etc.) and provide a detailed explanation justifying the proposed course of action desired to resolve the problem. Insert sheets for applicable documents shall also be attached to facilitate change action in the event the NECP is approved.

(e) Deviations/Waivers - In the event that a baseline design-related document requirement cannot be met, and a change to the baseline document is considered inappropriate, the Contractor shall submit a Request for Variance. The explanation of "Need for Deviation/Waiver" in the DD1694 shall provide detailed justification and consequences of approval, to include technical details explaining the degree of noncompliance and the effect on ship equipment or system operation.

(f) Equitable Adjustments for Change Documentation Preparations - For its effort expended in preparing ECPs, NECPs, and Deviations/Waivers, the Contractor shall receive equitable adjustment under the following circumstances:

(1) In the event the Contractor, on its own initiative, and without written request from the Contracting Officer, develops a change document that is later disapproved by the Government, the Contractor shall bear the cost of this effort.

(2) To avoid such loss, and at its option, the Contractor may submit a "preliminary" document that outlines intent, but without detailed supporting documentation and request the Contracting Officer's approval for expenditure of effort to complete the detailed supporting documentation. In the event the Contracting Officer denies this request, the Contractor will bear the cost of development of the "preliminary" document, and shall make no further effort to complete detailed supporting documentation.

(3) In the event the Contracting Officer approves the Contractor's request to develop supporting documentation, the Contractor shall be equitably compensated for its effort for both the "preliminary" and "final" documentation, regardless of whether or not the change document is later approved.

(4) In the event the Contracting Officer requests in writing that the Contractor develop change documentation, the effort expended by the Contractor in developing such

DRAFT

documentation shall be subject to equitable adjustment, regardless of whether or not the change document is later approved.

(5) In the event the Contractor, on its own initiative, and without written request from the Government, develops a change document that is later approved by the Contracting Officer, the cost of developing such documentation shall be subject to equitable adjustment.

(6) Failure to agree to such equitable adjustment in contract price shall constitute a dispute, and shall be adjudicated in accordance with the requirements of the clause entitled "Disputes" (FAR 52.233-1).

(g) Any cost reduction proposal submitted pursuant to the clause entitled "Value Engineering" (FAR 52.248-1) shall be submitted as a Value Engineering Change Proposal (VECP). The Contractor shall follow the VECP preparation requirements of FAR 52.248-1(c) and any additional guidance provided by the Contracting Officer.

C-244-H002 SUBCONTRACTORS/CONSULTANTS (NAVSEA) (FEB 2023)

In addition to the information required by FAR 52.244-2(e) of the contract, when consent to subcontract is required per FAR 52.244-2, the contractor shall also include the following information in requests to add subcontractors or consultants during performance:

(1) Impact on subcontracting goals,

(2) Impact on providing support at the contracted value,

(3) IF SEAPORT TASK ORDER - The results of negotiations to incorporate fee rate caps no higher than the lower of (i) SeaPort NXG fee rate caps for the prime contractor, or in the case where the proposed subcontractor is also a SeaPort NXG prime, (ii) fee rate caps that are no higher than the subcontractor's prime SeaPort NXG contract.

C-245-H005 INFORMATION AND DATA FURNISHED BY THE GOVERNMENT--ALTERNATE I (NAVSEA) (MAY 2019)

(a) Contract Specifications, Drawings and Data. The Government will furnish, if not included as an attachment to the contract, any unique contract specifications or other design or alteration data cited or referenced in Section C.

(b) Government Furnished Information (GFI). GFI is defined as that information essential for the installation, test, operation, and interface support of all Government Furnished Material identified in an attachment in Section J. The Government shall furnish only the GFI identified in an attachment in Section J. The GFI furnished to the contractor need not be in any particular format. Further, the Government reserves the right to revise the listing of GFI as follows:

(1) The Contracting Officer may at any time by written order:

(i) delete, supersede, or revise, in whole or in part, data identified in an attachment in Section J; or

(ii) add items of data or information to the attachment identified in Section J; or

(iii) establish or revise due dates for items of data or information in the attachment identified in Section J.

(2) If any action taken by the Contracting Officer pursuant to subparagraph (1) immediately above causes an increase or decrease in the costs of, or the time required for, performance of any part of the work under this contract, the contractor may be entitled to an equitable adjustment in the contract amount and delivery schedule in accordance with the procedures provided for in the "CHANGES" clause of this contract.

(c) Except for the Government information and data specified by paragraphs (a) and (b) above, the Government will not be obligated to furnish the Contractor any specification, standard, drawing, technical documentation, or other publication, notwithstanding anything to the contrary in the contract specifications, the GFI identified in an attachment in Section J, the clause of this contract entitled "Government Property" (FAR 52.245-1) or "Government Property Installation Operation Services" (FAR 52.245-2), as applicable, or any other term or condition of this contract. Such referenced documentation may be obtained:

(1) From the ASSIST database via the internet at https://assist.dla.mil/online/start/; or

(2) By submitting a request to the

Department of Defense Single Stock Point (DoDSSP)
Building 4, Section D
700 Robbins Avenue
Philadelphia, Pennsylvania 19111-5094
Telephone (215) 697-6396
Facsimile (215) 697-9398

Commercial specifications and standards, which may be referenced in the contract specification or any sub-tier specification or standard, are not available from Government sources and should be obtained from the publishers.

DRAFT