# H60 DEPARTMENT APPLIED ARTIFICAL INTELLIGENCE/INTELLIGENCE AUTOMATION SUPPORT SERVICES

## STATEMENT OF WORK

## SECTION C – DESCRIPTION/SPECIFICATION/WORK STATEMENT

### C.1 BACKGROUND

The increasing complexity of the modern battlespace and the proliferation of advanced threats necessitate the development of autonomous capabilities to enhance mission effectiveness, increase operational tempo, and reduce risk to human operators. The Intelligent Automation Division (H60), Weapons Control and Integration Department (H), Naval Surface Warfare Center Dahlgren Division (NSWCDD) executes a critical mission to research, develop, test, integrate, and sustain Artificial Intelligence (AI) and Machine Learning (ML) solutions for weapon systems and autonomous platforms across the Department of War (DOW). H60 is responsible for pioneering capabilities that provide a decisive advantage to the warfighter by the integration of autonomy, artificial intelligence (AI), machine learning (ML), robotics, and unmanned systems. These technologies are empowered by the application of intelligent automation to defeat current and future enemy threats and technologies. This contributes to the defense of the nation and protection of the warfighter through continued advancement and integration of AI/ML technical solutions onto weapon systems. This technical focus area continuously requires innovative, focused, and expeditious responses to conquer threats that pose challenges to US forces and lead to the expansion of coalition warfighting capabilities.

To deliver these complex systems, H60 requires contractor support in implementing a modern Machine Learning Operations (MLOps) framework and conducting rigorous Assured AI (AAI) Test and Evaluation (T&E), along with other Engineer support activities. This SOW outlines the comprehensive technical and engineering services required for the contractor to successfully support H60 in fulfilling these vital national security objectives.

### C.2 SCOPE

The complexities and importance of H60's responsibilities necessitate deep expertise in several cutting-edge fields. This SOW defines the tasks the contractor shall perform to augment H60's capabilities and execute its mission objectives. Contractor performance shall directly contribute to automating and weaponizing weapon systems and the maturation of the autonomous kill chain. This includes engineering for perception autonomy, algorithmic development for weapon autonomy, and systems integration for full killchain autonomy.

The scope of this effort encompasses the entire lifecycle of AI/ML-based autonomous systems, from concept design through fielding and sustainment. The Contractor shall provide a comprehensive suite of services to support the Intelligent Automation Division's (H60) diverse portfolio. The contractor shall be proficient in and provide support across the following disciplines:

- Acquisition, Program, and Project Management
- Systems Engineering and Systems Integration

**H60 DEPARTMENT APPLIED ARTIFICAL INTELLIGENCE/INTELLIGENCE AUTOMATION SUPPORT SERVICES**

**STATEMENT OF WORK**

- Data and Configuration Management
- Computing Hardware Engineering
- Prototyping and Model Making
- Software Engineering
- AI/ML Algorithm Development
- Analyses, Assessments, Test and Evaluation
- Cybersecurity and Systems/Network Support
- Safety and Ethical Assurance
- DevSecOps, ML Ops, and IT Infrastructure Engineering
- Integrated Logistics Support
- Training and Instruction
- Technical and In-Service Engineering Support
- Facilities, Fabrication, and Low-Rate Production

The Contractor shall provide the necessary personnel, resources, and management to perform all tasks outlined in this SOW, working in close collaboration with Government personnel and other stakeholders to ensure alignment with Department of the Navy (DoN) operational requirements.

Given that programs and projects in the H60 Division's portfolio are at various phases of the acquisition framework—from science and technology to life cycle sustainment—the Contractor shall provide flexible and scalable support to all current and new projects as they mature through the acquisition, technology, and logistics framework.

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 War 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.

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

| **Number** | **Document Name** |
|---|---|
| DOD 8570.01-M | Information Assurance Workforce Improvement Program |
| SAE AS5553 | SAE Aerospace Standard 5553 |
| NISPOM – 32 Code of Federal Regulation Part 117 | National Industrial Security Program Operating Manual (NISPOM) |
| NSWCDDINST 5510.4B | NSWCDD Command Security Manual |

| Number | Document Name |
|---|---|
| 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 |
| DODI 5200.48 | Controlled Unclassified Information |
| SECNAVINST 5210.8F | Department of Navy Records Management Program |
| NSWCDDINST 5100.1F | Occupational Safety and Health Program |
| NAVADMIN 216/15 | Cyber Hygiene Authorization to use Personal Wearable Fitness Devices |
| NAVSEA S0420-AA-RAD-010 – REV 2A | Radiological Affairs Support Program (RASP) Manual |
| DODI 8510.01 | Risk Management Framework for DoD Systems |
| CJCSI 6211.02D | Defense Information Systems Network (DISN) Responsibilities |
| DODM 1000.13 | Department of War Identification (ID) Cards |
| NAVSEAINST 4200.19 (series) | Planning, Use and Control of Services Contracting |
| COMUSFLTFORCOM/ COMPACFLT 6320.3B | Medical Screening for U.S. Government Civilian Employees, Contractor Employees, Guests and Visitors Prior to Embarking Fleet Units |

## C.3 REQUIREMENTS

### C.3.1 Program/Project Management, Acquisition and Governance for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.1.1 The Contractor shall provide all necessary programmatic support to the Government Program Manager (PM) for the successful execution of the programs/projects in the H60 portfolio. This support shall include

a) Drafting and maintaining management plans and strategies for Government review and approval. (CDRL A001)

b) Executing project leadership operations as directed by the Government, including Milestone tracking, progress monitoring, and managing project tasks.

c) Proposing and drafting new or enhanced business processes and performance metrics for Government consideration and approval.

d) Organizing, attending, and documenting all program and project meetings, including generating attendee lists, drafting meeting minutes, and tracking action items for Government awareness. (CDRL A002)

e) Supporting project leadership operations to include preparing briefs, tasking, progress monitoring, programmatic reviews, acquisition documentation, risk management, budget development, requirements analysis, design reviews, production planning, material fielding planning, systems sustainment management, operator and maintenance training, logistics planning and management, and other project management tasking.

DRAFT

C.3.1.2 The Contractor shall implement and manage a quality assurance and process improvement framework to support Government oversight. The Contractor shall:

a) Conduct evaluations of products and processes and provide the results and recommendations to the Government.

b) Collect, analyze, and deliver production and performance metrics. The Contractor shall conduct trend analysis, impact analysis, and causal analysis, and provide the results to the Government to support its decision-making process. (CDRL A003)

c) Conduct peer reviews, code reviews, and audits, and report all findings to the Government. The Contractor shall collect and analyze lessons learned and recommend process improvements for Government approval.

C.3.1.3 The Contractor shall provide subject matter expertise and analysis to support the Government's strategic planning for Asure AI (AAI) systems. The Contractor shall:

a) Draft and maintain, for Government approval, an AI Development and Management Plan (ADMP) that defines the governance for AI models, datasets, and the Machine Learning Operations (MLOps) pipeline. (CDRL A004)

b) Analyze and prepare reports on how near and long-term modernization plans, doctrine, and policy could impact the H60 portfolio. (CDRL A005)

c) Provide research, analysis, and recommendations on emerging lifecycle standards and industry best practices for AAI systems.

C.3.1.4 The Contractor shall provide financial and cost analysis support for the H60 portfolio. The Contractor shall:

a) Generate, maintain, update, programs/projects budget estimates for Government review.

b) Utilize Government financial systems to track budget execution and provide regular status reports to the Government.

c) Perform cost excursions and provide the resulting data to support what-if analysis.

d) Use financial systems to create and track requisitions and procurement requests.

C.3.1.5 The Contractor shall provide acquisition and procurement support by preparing all necessary documentation for Government approval and execution. The Contractor shall:

a) Conduct market intelligence and cost evaluations and prepare complete Simplified Acquisition Threshold (SAT) and MILSTRIP procurement packages for submission to the acquisition team.

b) Draft all required acquisition documentation, including Justification and Approval (J&A) letters, for Government review and signature.

c) Prepare and route all required approval documentation (e.g., safety, ITPR, DADMS, etc.) and track them to completion, reporting status to the Government.

C.3.1.6 The Contractor shall perform the role of Lead Systems Integrator (LSI) for designated H60 programs, responsible for orchestrating the integration of complex systems and bringing

DRAFT

together diverse components to create a cohesive and functional whole. The Contractor shall perform the following LSI functions:

a) Provide the technical management for the entire project lifecycle. This shall include drafting, for Government review and approval, the project scope, objectives, technical requirements, Integrated Master Schedule (IMS), and budget estimates. (CDRL A006)

b) Develop and maintain a comprehensive System Integration Plan. This plan shall detail how different subsystems, including third-party vendor hardware, COTS software, and other Government-furnished components, will be combined, tested, and validated to create the final system, ensuring full compatibility and interoperability. (CDRL A007)

c) Serve as the primary technical liaison between all project stakeholders, including component vendors, other contractors, and Government labs. The Contractor shall facilitate technical communication and collaboration to ensure all parties are aligned with the Government's approved project goals.

d) Identify, analyze, and track all technical risks associated with system integration. The Contractor shall develop and propose risk mitigation strategies and contingency plans for Government approval and shall monitor project progress to address identified technical issues.

e) Execute the quality assurance plan for the fully integrated system. This includes conducting system-level tests and inspections and applying quality control measures to ensure that end-to-end system meet all technical performance specifications and Government requirements.

f) Provide and manage a team of technical experts with the specialized knowledge required for the project, including in the areas of systems engineering, software development, cybersecurity, and platform-specific integration.

g) Maintain detailed documentation of the entire integration process. This includes maintaining technical specifications, project plans, and providing regular progress reports to the Government on project status, technical challenges, and any deviations from approved plan.

h) Provide ongoing engineering support to ensure the continued functionality and performance of the integrated system. This includes troubleshooting fleet-identified issues, developing and integrating system upgrades, and providing technical support to end-users.

i) Conduct client satisfaction and other surveys.

C.3.1.7 The Contractor shall collect lessons learned to assist future projects.

C.3.1.8 The Contractor shall provide a status of funds for all the projects after each funding modification is awarded. The status of funds, at a minimum, shall include an estimate to completion for each project, estimated weekly/monthly burned rate, obligated amount, remaining balance, 75% complete date, and 100% complete date. (CDRL A008)

C.3.1.9 The Contractor shall provide subject matter expertise to support the Government's governance of the AI/ML lifecycle. The Contractor shall:

a) Draft and maintain an AI/ML Maturation Process. This plan shall define the processes for model traceability, criteria for model promotion through development and testing environments, and procedures for model retraining and retirement. (CDRL A009)

b) Provide analysis and recommendations on the data governance strategy, including data acquisition, labeling standards, quality assessment, and security, ensuring a reliable source for all AI model development.

c) Establish and report on key performance indicators (KPIs) related to the health and maturity of the AI development process, such as data quality scores, model training efficiency, and time-to-deployment.

C.3.1.10 The Contractor shall provide programmatic support for the oversight of the MLOps infrastructure. The Contractor shall:

a) Provide support for the creation of a governance plan for the MLOps pipeline. This includes defining the automated processes for continuous integration, continuous testing (CT), continuous training, and continuous delivery (CI/CD) of AI models.

b) Monitor and report on the health, security, and efficiency of the MLOps pipeline. This includes tracking metrics on automated test pass/fail rates, model build times, and deployment frequencies.

c) Provide analysis on the resources consumed by the MLOps pipeline, including cloud compute costs and data storage, to support Government financial planning.

C.3.1.11 The Contractor shall provide analysis and tracking for risks unique to AAI systems to support the Government's overall risk management program. The Contractor shall:

a) Identify, analyze, and document potential AAI-specific risks, including but not limited to algorithmic bias, data poisoning, model evasion, catastrophic forgetting, and unintended model behaviors.

b) Develop and propose mitigation strategies for identified AAI risks for Government review and approval.

c) Maintain a dedicated section within the program risk register to track the status of all AAI-specific risks and their associated mitigation plans.

<u>C.3.2 Systems Engineering and Systems Integration Support for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems</u>

C.3.2.1 The Contractor shall provide systems engineering to support the integration of AI/ML technologies into current and new projects in the H60 portfolio.

C.3.2.2 The Contractor shall provide engineering support during the development of systems and implement best rigorous engineering approaches and processes throughout the acquisition process, from requirements generation through disposal (cradle to grave) to ensure all threshold and objective requirements are achieved.

C.3.2.3 The Contractor shall draft a Systems Engineering Management Plan (SEMP), and Project's Systems Engineering Plans (SEPs) when applicable. (CDRL A00A)

DRAFT

C.3.2.4 The Contractor shall develop and maintain Integrated Master Plans and Schedules (IMP/IMS) for projects. (CDRL A006)

C.3.2.5 The Contractor shall apply model-based systems engineering (MBSE) when conducting engineering analysis and review and evaluation of data from different reliable sources to develop DoW architecture framework products to effectively develop systems and transition them to the field and/or programs of record.

C.3.2.6 The Contractor shall provide engineering support to conduct technology readiness assessments of projects in support of Milestones events.

C.3.2.7 The Contractor shall maintain requirements traceability matrix (RTM) to document, track, and manage program requirements, and test results using Government designated tool (s). (CDRL A00B)

C.3.2.8 The Contractor shall assist with the verification and validation of new and existing autonomous systems and technologies. This verification shall include evaluation of technical baselines documentation such as equipment design, operation and maintenance, requirements, architectures, interface control, etc.

C.3.2.9 The Contractor shall assist with validating tasks, such as technical performance, safety features, and reliability/maintainability thresholds/objectives.

C.3.2.10 The Contractor shall conduct systems integration to permit developmental testing, analytical testing, and data analysis of selected technologies, prototyped capabilities, and related systems.

C.3.2.11 The Contractor shall integrate subassembly hardware, develop system and component test plans, develop test data collection and analysis plans, conduct testing, and document test results.

C.3.2.12 The Contractor shall analyze new AI/ML technologies for integration into systems. The Contractor's analysis shall identify opportunities for improvement in performance, sustainability, reliability, and maintainability while considering cost impacts.

C.3.2.13 The Contractor shall integrate new technologies into existing systems, upon approval by the Government, ensuring that established system requirements continue to be met.

C.3.2.14 The Contractor shall conduct studies, analyses, and assessments through technology reviews, systems engineering decomposition, experimentation and testing, and any other means of collecting information to identify potential artificial intelligence solutions and to assess operational, logistical, and supportability requirements and risks of those solutions. (CDRL A00C)

DRAFT

C.3.2.15 The Contractor shall apply engineering, scientific analytical disciplines to identify, refine and document operational and functional requirements.

C.3.2.16 The Contractor shall translate systems autonomy operational and functional requirements from requirements documents such as Concepts of Operations (CONOPS), Capability Development Document (CDD), Capability Production Document (CPD), etc., and create Performance Specifications (PSpecs). (CDRL A00D)

C.3.2.17 The Contractor shall develop system, subsystem and component level requirements and design software/hardware specifications documents. (CDRL A00D)

C.3.2.18 The Contractor shall develop system PSpecs that shall include software and hardware interface requirements and description. (CDRL A00D)

C.3.2.19 The Contractor shall provide comprehensive systems engineering support to the Government across the entire program lifecycle. This support shall be governed by a Systems Engineering Management Plan (SEMP), which the contractor shall draft and maintain for Government review and approval.

C.3.2.20 The Contractor shall develop and maintain Integrated Master Plans and Schedules (IMP/IMS) to track engineering activities (CDRL A006). The Contractor shall perform all work shall using rigorous and documented engineering processes.

C.3.2.21 The Contractor shall support the Government in all formal technical reviews (e.g., SRR, PDR, CDR), providing the necessary engineering data and analysis.

C.3.2.22 The Contractor shall perform the necessary analysis and engineering to support the Government's definition of the technical baseline. The Contractor shall:

a) Conduct studies, analyses, and assessments of technologies and engineering approaches, and provide the results to the Government to identify potential AAI solutions and assess requirements, risks, and supportability. (CDRL A00E)

b) Draft and propose all levels of requirements (operational, functional, system, subsystem, performance) and interface specifications for Government review and approval. This includes translating operational needs into formal documentation (e.g., CONOPS, CDD, CPD). (CDRL A00D)

c) Develop and maintain the system architecture using a Model-Based Systems Engineering (MBSE) approach, creating the necessary DoW Architecture Framework products for Government approval.

d) Develop and maintain a Requirements Traceability Matrix (RTM) to ensure every requirement is allocated and tracked through verification. (CDRL A00B)

C.3.2.23 The Contractor shall provide technical support for the integration and verification of systems and subsystems. The Contractor shall:

a) Conduct systems integration of hardware, software, and prototype capabilities to support all forms of testing.

b) Draft, for Government approval, and execute system and component test plans. (CDRL A00F)

c) Provide all necessary data and analysis to assist the Government with formal verification and validation activities. This includes supporting the evaluation of technical baselines, technical performance, safety, and reliability characteristics against the approved requirements.

d) Document and deliver all test results and analysis to the Government. (CDRL A00G)

C.3.2.24 The Contractor shall provide subject matter expertise to support the Government in identifying and maturing new technologies. The Contractor shall:

a) Analyze new AI/ML technologies for potential integration and provide the Government with formal analysis reports identifying opportunities for improvement in performance, sustainability, and reliability, including cost-impact analysis. (CDRL A00H)

b) Integrate approved new technologies into existing systems, ensuring that the established system requirements baseline continues to be met.

C.3.2.25 The Contractor shall develop and propose for Government approval a methodology for defining, documenting, and managing requirements for non-deterministic and autonomous behaviors. This methodology must address how to specify performance for AI/ML components in terms of probabilities, confidence levels, and operational envelopes (e.g., 'The classification algorithm shall achieve 98% accuracy on the validation dataset').

C.3.2.26 The Contractor shall provide Human Systems Integration and Human Factors Engineering support throughout the design and development lifecycle. The Contractor shall analyze operator tasks, design user interfaces, and conduct usability testing to ensure the system is effective, intuitive, and reduces operator workload. The HSI analysis shall focus on how operators receive, understand, and act upon information provided by AI/ML components, especially in high-stress, time-critical situations.

C.3.2.27 The Contractor shall conduct a continuous System Safety program in accordance with MIL-STD-882. The Contractor shall perform and deliver a System Safety Hazard Analysis (SSHA) that identifies and assesses risks posed by system hardware, software, and autonomous functions. The analysis must include hazards associated with unexpected AI/ML model behavior and propose mitigations for Government review and approval.

C.3.2.28 The Contractor shall develop, maintain, and deliver a Government-owned Digital Engineering Environment (DEE) for the H60 portfolio. This environment shall integrate the MBSE architecture models with high-fidelity simulation tools and analysis software. As part of the DEE, the Contractor shall develop and maintain 'Digital Twins' of key systems (e.g., the USV), which shall be used to conduct virtual integration, performance analysis, and simulated Test & Evaluation.

DRAFT

C.3.2.29 The Contractor shall conduct engineering and other technical reviews.

C.3.3 Data and Configuration Management of Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.3.1 The Contractor shall provide configuration management (CM) and quality assurance to support Intelligent Automation programs and projects.

C.3.3.2 The Contractor shall develop CM plans for projects/programs. (CDRL A00I).

C.3.3.3 The Contractor shall provide configuration management of products throughout their Life Cycle for the following document types: requirements documents; design documents; and production procedures for delivery to sponsors or other external organizations.

C.3.3.4 The Contractor shall organize program and project level documentation into repositories, including web-based repositories, and maintain the repository to facilitate documentation storage and retrieval.

C.3.3.5 The Contractor shall support the Government CM process by maintaining controlled and versioned documentation in accordance with the program or project CM plan.

C.3.3.6 The Contractor shall attend and provide technical subject matter expertise during Configuration Control Boards (CCBs).

C.3.3.7 The Contractor shall evaluate proposed changes to systems, subsystems, or components for impact or other associated system applicability.

C.3.3.8 The Contractor shall establish program or project-level software CM data repositories tracking Software Trouble Reports (STRs), STR analysis, inactive configurations, and other configuration item data.

C.3.3.9 The Contractor shall maintain and operate web-based CM server repositories, including project databases.

C.3.3.10 The Contractor shall develop and maintain Change Notices (SCNs). [CDRL A00J]

C.3.3.11 The Contractor shall prepare Software Version Descriptions (SVDs). (CDRL A00K).

C.3.3.12 The Contractor shall provide process improvement suggestions towards the program or project CM plan and assist other personnel with CM processes.

DRAFT

C.3.3.13 The Contractor shall maintain internal documents placed under CM control for version control, change control, or archiving purposes. This shall include the maintenance of an electronic master filing and documentation management system.

C.3.3.14 The Contractor shall perform document scanning, storage, version control, routing, and review; transfer Microsoft Word files to PDF; apply optical recognition capabilities to allow search ability; and post documents to designated shared spaces.

C.3.3.15 The Contractor shall develop, maintain, test, and install databases and database interfaces at sponsor sites.

C3.3.16 The Contractor shall perform database upgrade and patching.

C.3.3.17 The Contractor shall provide support for database interfaces to third party systems for data exchange.

C.3.3.18 The Contractor shall maintain data repositories (both hard and soft copy) on both hardware and software for projects/programs.

C.3.3.19 The Contractor shall update the data repository as changes occur to the hardware and software and perform regular audits of repository data against the current systems configuration as well as against third party data, updating the data as necessary.

C.3.3.20 The Contractor shall extend the CM process to explicitly manage AI/ML datasets and trained models as distinct Configuration Items (CIs). The Contractor shall:

a) Assign unique identifiers and version controls to all datasets, including raw, processed, training, validation, and testing sets. The CM system must be able to retrieve any specific version of a dataset.

b) Assign unique identifiers and version controls to all trained AI models and their corresponding model weights. The model's status (e.g., experimental, candidate, production) shall be managed within the CM system.

c) Incorporate dataset and model management into the CM Plan. The plan shall describe the process for baselining, checking in/out, and archiving datasets and models.

C.3.3.21 The Contractor shall implement and maintain a system for ensuring end-to-end traceability and provenance for every trained AI model. For any given model version, the Contractor shall produce a definitive record that links it to:

a) The exact version(s) of the dataset(s) used for its training and validation.

b) The exact version of the source code (e.g., Git commit hash) of the training algorithm and data pipelines.

c) The complete set of hyperparameters and configuration files used during the training process.

d) The resulting training and performance metrics associated with that model.

C.3.3.22 The Contractor shall be responsible for the management and administration of the MLOps artifact repository (e.g., container registry, model registry). The Contractor shall:

a) Implement versioning and access control policies for the repository to ensure that only tested and approved AI model artifacts can be staged for deployment.

b) Conduct regular audits of the repository to ensure its content aligns with the baselines established in the CM system.

c) Manage the promotion of artifacts through the repository (e.g., from a 'development' registry to a 'production' registry) in accordance with the Government-approved CM plan.

C.3.4 Computer Hardware Engineering for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.4.1 The Contractor shall provide the expert-level computer hardware engineering capability to design, develop, integrate, and test the computational systems and electronic subsystems required to execute AAI workloads on tactical platforms.

C.3.4.2 The Contractor shall provide the expertise to architect the complete computational system. The Contractor shall:

a) Conduct trade studies and analysis to select the optimal combination of Central Processing Units (CPUs), Graphics Processing Units (GPUs), and other AI accelerators (e.g., TPUs, FPGAs) to meet the system's performance and Size, Weight, and Power (SWaP) requirements.

b) Design the high-speed data architecture between processors, memory, storage, and peripherals, ensuring sufficient bandwidth for real-time sensor data processing and AI inference.

c) Define the system's power architecture, including power distribution, regulation, and conditioning, to ensure reliable operation in harsh electrical environments.

C.3.4.3 The Contractor shall be responsible for the integration and optimization of all computer hardware components. The Contractor shall:

a) Integrate and test COTS and custom computing components, including single-board computers, embedded systems, and high-performance servers, into ruggedized enclosures.

b) Conduct hardware-level performance tuning, including optimizing BIOS/UEFI settings and peripheral configurations, to maximize computational throughput and minimize latency.

c) Develop and execute Hardware Qualification Tests (HQT) to validate that the integrated computer system is fully functional and meets all performance and environmental requirements.

C.3.4.4 The Contractor shall provide the capability to design and fabricate custom electronics when COTS solutions are not suitable. The Contractor shall:

a) Design and layout multi-layer, high-speed digital and analog Printed Circuit Boards (PCBs) for custom processing boards, sensor interfaces, and power distribution units.

DRAFT

b) Perform signal integrity and power integrity analysis on PCB designs to ensure reliable operation.

c) Manage the fabrication and assembly of prototype PCBs and conduct functional testing to verify their performance.

C.3.4.5 The Contractor shall develop the low-level software that directly interfaces with and controls the hardware. The Contractor shall:

a) Develop and maintain firmware and BIOS/UEFI for custom computer hardware.

b) Develop Board Support Packages (BSPs) and device drivers for various operating systems (e.g., Linux, RTOS) to enable communication with custom hardware and peripherals.

c) Program microcontrollers and FPGAs to perform dedicated, real-time tasks such as sensor signal pre-processing, motor control, or safety monitoring.

C.3.4.6 The Contractor shall provide the capability to evaluate and integrate emerging, post-GPU computing architectures. The Contractor shall:

a) Monitor the state-of-the-art in specialized AI hardware, including Neuromorphic Processing Units (NPUs) and other low-power, event-based processors.

b) Upon Government direction, acquire and evaluate prototype next-generation processors to assess their suitability for defense applications.

c) Develop the necessary software, firmware, and drivers to integrate these future hardware architectures into H60 systems.

d) Maintain and provide SMEs with deep technical knowledge of critical subsystems, including Remote Weapon Stations (RWS), specific camera and sensor payloads, and associated vendor software, to support all tiers of troubleshooting and integration.

C.3.5 Prototyping and Model-Making for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.5.1 The Contractor shall provide the subject matter expertise required to design, model, and fabricate mechanical and structural solutions. The Contractor shall:

a) Capture and document design requirements and develop 3-D models using Government-approved CAD software (e.g., SolidWorks, ProE).

b) Perform mechanical, thermal, and stress analysis using Finite Element Analysis (FEA) software to validate designs.

c) Generate and maintain all necessary machines and assembly drawings for fabrication and documentation. (CDRL A00L)

d) Operate fabrication equipment, including machining and welding, to produce components and assemble end-items.

e) Utilize Additive Manufacturing (e.g., 3D printing) with a variety of materials, including polymers and metals, to rapidly fabricate complex components, custom enclosures, and one-off prototype parts.

DRAFT

f) Ensure all physical prototypes and modifications are fully documented and reflected in the system's Digital Twin and associated MBSE models, maintaining consistency between the physical and digital representations of the system.

g) Fabricate components using advanced composite materials, including but not limited to carbon fiber and fiberglass, to meet specific weight, strength, and radio-frequency (RF) transparency requirements.

C.3.5.2 The Contractor shall provide the subject matter expertise required to design, fabricate, and assemble electrical and electronic solutions. The Contractor shall:

a) Draft requirement documentation for and design integrated circuits, Printed Circuit Boards (PCBs), and microcontroller-based systems.

b) Perform thermal and electro-magnetic interference (EMI) analysis on electronic designs.

c) Assemble and test prototype circuits, cable harnesses, and wire assemblies for design verification and system integration.

d) Provide Radio Frequency (RF) engineering support, including the design, fabrication, and integration of custom antennas and RF-shielded enclosures to ensure communications and sensor performance while minimizing electromagnetic interference.

C.3.5.3 The Contractor shall apply its fabrication capabilities to the specific needs of AAI-enabled platforms and systems. The Contractor shall:

a) Design and fabricate ruggedized, environmentally sealed enclosures for deploying high-performance computing hardware (e.g., GPUs, TPUs). Designs shall include specific solutions for advanced power distribution and thermal management (e.g., active cooling, heat dissipation) to ensure system reliability in constrained, power-limited environments like Unmanned Surface Vehicles (USVs).

b) Design and fabricate custom mounts, fixtures, and power/data distribution systems for integrating advanced sensors (e.g., EO/IR, LiDAR, radar) and weapon systems onto tactical vehicles, aircraft, and operational platforms.

c) Rapidly prototype and modify existing systems to support user evaluations, technology insertions, and the fielding of low-density, specialized capabilities to meet validated warfighter needs.

d) Design and construct Hardware-in-the-Loop (HWIL) testbeds and specialized test tools that enable the safe and effective evaluation of weapon autonomy functions in a lab environment.

e) Design and integrate advanced robotic and actuation systems, including servo-mechanisms, robotic manipulators, and automated payload handling systems, into prototype platforms.

C.3.5.4 The Contractor shall provide the necessary support to acquire components and install completed prototypes. The Contractor shall:

a) Conduct research and procurements of Commercial-Off-the-Shelf (COTS) and other components required for prototyping and fabrication.

DRAFT

b) Provide on-site installation support for prototyped equipment aboard tactical vehicles, aircraft, USVs, and other operational platforms.

c) Provide maintenance and repair support for both in-house and fielded prototype equipment.

C.3.6 Software Engineering Support for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.6.1 The Contractor shall provide the software engineering and programming support to implement automation and AI/ML software in systems, sub-systems, and components utilizing computers, electronics, and software.

C.3.6.2 The Contractor shall provide a comprehensive software engineering capability to design, develop, integrate, test, and sustain all non-AI software components required for AI/ML-enabled systems.

C.3.6.3 The Contractor shall follow a disciplined and documented software development process compliant with SEI CMM Level 3 (or equivalent) and employ agile methodologies where applicable.

C.3.6.4 The Contractor shall conduct software development consistent with industry best practices to ensure software quality assurance and shall provide software deliverables that follow Open Architecture (OA) procedures, standards, and guidelines.

C.3.6.5 The Contractor shall perform full-lifecycle software engineering in accordance with Government-approved requirements and design documents. The Contractor shall:

a) Plan, design, code, test, and integrate all software components.

b) Deliver complete software packages including all source code, build files, and executables for all deliverables. (CDRL A00M)

c) Provide software maintenance and sustainment support, including bug fixes, performance enhancements, and obsolescence management.

d) Develop and maintain all required software documentation, including but not limited to: Software Development Plans (SDP), Software Requirements Specifications (SRS), and software test plans. (CDRL A00N)

e) Provide all necessary technical documentation and subject matter expertise to support formal program reviews, including PDRs, CDRs, PRRs, and SVRs.

f) Provide technical analysis and recommendations for software modifications, upgrades, and technology refresh.

g) Draft and maintain software transition plans for Government review and approval. (CDRL A00O)

h) Draft and provide all necessary technical input for Software Engineering Change Proposals (ECPs) for Government review and approval.

DRAFT

C.3.6.6 The Contractor shall develop the software necessary to integrate AI components and to connect with digital engineering environments. The Contractor shall:

a) Design and develop Application Programming Interfaces (APIs) and data services that allow the core software system to dynamically load, configure, and receive outputs from containerized AI models delivered by the MLOps pipeline.

b) Develop software interfaces to connect with the Digital Twin and Hardware-in-the-Loop (HWIL) testbeds. This includes creating the necessary middleware to pass data between the operational software and the virtual simulation environment.

c) Develop software for data collection, logging, and visualization to support AAI Test & Evaluation, providing the tools needed to record and analyze system performance during test events.

C.3.6.7 The Contractor shall develop software adaptable to a hybrid computing environment. The Contractor shall:

a) Develop cloud-native software components and services intended for execution in Government-approved cloud environments (e.g., for large-scale data processing or simulation).

b) Develop and optimize software for deployment on Size, Weight, and Power (SWaP)-constrained edge computing devices, such as those found on USVs and other unmanned platforms. This includes customizing open-source Linux distributions and developing efficient, low-latency code.

C.3.6.8 The Contractor shall maintain proficiency in and utilize a modern, flexible technology stack as approved by the Government. The Contractor shall also provide support for other languages, databases, or tools not explicitly listed as directed by the Government to meet evolving project needs. The final stack will be determined on a per-project basis and documented in the Government-approved Software Development Plan.

C.3.6.9 The Contractor shall demonstrate the capability to provide experts proficient in the following representative technology categories:

a) Core Systems and Performance Languages: C/C++, Python, Java, C#. This includes modern systems languages designed for safety and concurrency, such as Rust or Go.

b) GPU and Parallel Computing Frameworks: NVIDIA CUDA, OpenCL, and equivalent frameworks for GPU/parallel processor development.

c) AI/ML Development Frameworks: Deep expertise in building software that integrates with models developed in common frameworks such as PyTorch and TensorFlow.

d) Robotics and Autonomy Frameworks: Robot Operating System (ROS/ROS 2), Joint Architecture for Unmanned Systems (JAUS), and associated simulation tools (e.g., Gazebo, AirSim).

e) Web/UI and Visualization Technologies: Modern web frameworks (e.g., React, Angular, Vue) built on JavaScript/TypeScript, HTML/CSS for the development of user interfaces and data visualization dashboards.

f) Database and Data Streaming Technologies: Relational (e.g., PostgreSQL), NoSQL (e.g., MongoDB), and high-throughput data streaming platforms (e.g., Apache Kafka, gRPC).

g) Infrastructure, Cloud, and MLOps Tools: Git, Docker, Kubernetes, and Infrastructure as Code (IaC) tools (e.g., Terraform, Ansible) for managing cloud and on-premises environments.

h) Operating Systems: Microsoft Windows and deep expertise in various UNIX/Linux distributions, including customization for real-time and embedded applications.

C.3.6.10 The Contractor shall provide expertise in developing highly parallelized software for heterogeneous computing hardware. This shall include:

a) Developing and optimizing code using NVIDIA CUDA, OpenCL, or equivalent frameworks to maximize the performance of AI/ML algorithms on Graphics Processing Units (GPUs) and other parallel processors.

b) Profiling and debugging performance bottlenecks in GPU-accelerated code to ensure real-time processing capabilities for perception and weapon control systems.

c) Developing software that efficiently manages data transfer between CPUs and GPUs to minimize latency.

C.3.6.11 Real-Time and Embedded Systems Software: The Contractor shall provide expertise in developing software for real-time embedded systems. This shall include:

a) Developing software for Real-Time Operating Systems (RTOS), such as VxWorks or real-time variants of Linux, ensuring deterministic performance for critical tasks like sensor processing and actuator control.

b) Applying safety-critical software development standards, such as MISRA C/C++ or other relevant standards, for code that controls hardware or weapon functions.

c) Developing low-level software, including device drivers and firmware, to interface with custom hardware, sensors, and peripherals.

C.3.6.12 The Contractor shall be proficient in developing software that utilizes common frameworks for robotics and autonomy. This shall include:

a) Developing, testing, and deploying software nodes and packages using the Robot Operating System (ROS/ROS 2) and its ecosystem of tools (e.g., Gazebo for simulation, RViz for visualization).

b) Developing interfaces to and extending other relevant autonomy frameworks and data standards, such as the Joint Architecture for Unmanned Systems (JAUS) or platform-specific SDKs

C.3.6.13 The Contractor shall provide the capability to apply formal methods and advanced software verification techniques to critical software components. This support includes:

a) Utilizing static and dynamic analysis tools to detect code defects, security vulnerabilities, and violations of coding standards.

b) Developing formal models of software components and, where directed by the Government, applying model-checking or theorem-proving techniques to mathematically verify properties related to safety and security.

DRAFT

C.3.7 AI/ML Algorithm Development for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.7.1 The Contractor shall provide the subject matter expertise required to research, design, develop, and train machine learning models and algorithms to enable autonomous system behaviors. This includes the development of algorithms for perception, planning, decision-making, and action.

C.3.7.2 The Contractor shall develop and train machine learning models for advanced perception and comprehensive environmental understanding, creating a persistent world model for the autonomous system. The Contractor shall:

a) Develop deep learning models (e.g., CNNs, Transformers, Graph Neural Networks) for the detection, classification, identification, and tracking of targets using a wide range of sensor modalities, including: Electro-Optical/Infrared (EO/IR), RADAR (including Synthetic Aperture Radar - SAR), LiDAR, multi-spectral and hyperspectral imagery, acoustic/sonar data, Signals Intelligence (SIGINT), and Communications Intelligence (COMINT).

b) Develop robust algorithms for multi-sensor data fusion and object-level tracking (e.g., using Kalman filters, particle filters, or deep learning techniques) to create a single, unified, and persistent world model from disparate, asynchronous, and potentially conflicting sensor inputs.

c) Develop algorithms specifically designed for GPS-denied navigation and localization, including techniques such as Visual-Inertial Odometry (VIO), SLAM (Simultaneous Localization and Mapping), and terrain/celestial navigation.

d) Develop and train models that are robust to environmental clutter (e.g., high sea states, adverse weather), sensor degradation, and a wide range of adversarial deception techniques, including spoofing, camouflage, and the presentation of novel sensor data.

e) Develop and apply Generative AI techniques (e.g., GANs, Diffusion Models) for high-fidelity synthetic data generation to augment training datasets, especially for rare targets, denied-area operations, and edge-case scenarios.

h) Provide expertise in synthetic data generation techniques to augment real-world training datasets and cover edge cases.

C.3.7.3 The Contractor shall develop algorithms that enable autonomous platforms (e.g., USVs, UAVs) to navigate and maneuver intelligently, safely, and tactically in contested, dynamic environments. The Contractor shall:

a) Develop and implement algorithms for tactically-aware, multi-objective path planning, enabling platforms to dynamically re-route based on emerging threats, mission objectives, fuel constraints, and environmental factors, while adhering to required constraints (e.g., COLREGs for maritime platforms).

b) Develop and apply Deep Reinforcement Learning (RL) and Inverse RL techniques to train agents for complex, sequential decision-making tasks, such as breach-and-clear maneuvers, covert infiltration, or optimizing sensor placement for maximum coverage.

DRAFT

c) Develop algorithms for precise automated launch and recovery of subordinate assets (e.g., a UAV or UUV from a host USV) and for the dexterous control of on-board robotic manipulators and payload systems.

d) Develop algorithms that enable adaptive autonomous behaviors based on the system's understanding of the tactical situation, including transitioning between operational modes (e.g., from low-observable transit to high-speed engagement).

e) Develop algorithms for control of on-board manipulators and payloads.

C.3.7.4 The Contractor shall develop, mature, and integrate a suite of AI/ML algorithms designed to automate functions across the entire killchain (Find, Fix, Track, Target, Engage, Assess) and reduce operator workload. All algorithms shall be developed to integrate with the Government-Owned Weapon Autonomy Architecture.

C.3.7.5 The Contractor shall provide experts proficient in the following Find & Fix Algorithms:

1. Automatic Target Recognition (ATR): Develop and refine ATR algorithms for detecting, identifying, and classifying targets from various sensor feeds, including providing for the ability to switch between multiple ATR models optimized for different targets or conditions.
2. 3D Scene Reconstruction: Develop algorithms to create 3D models of the battlespace from sensor data to support targeting and visualization.
3. Change and Anomaly Detection: Develop algorithms for Coherent Change Detection (CCD) to automatically identify relevant changes in an area over time, and Anomaly Detectors to flag objects or activities that are out of context.

C.3.7.6 The Contractor shall provide experts proficient in the following Tracking Algorithms:

1. Target Tracking: Develop and improve algorithms that perform robust, frame-to-frame tracking of designated objects.
2. Pose and Speed Estimation: Develop algorithms that use computer vision techniques, including Keypoint Detection, to automatically estimate a target's orientation (pose), heading, and speed for input into weaponeering solutions.

C.3.7.7 The Contractor shall provide experts proficient in the following Targeting and Weaponeering Decision Aids:

1. Weapon-Target Pairing Recommenders: Develop algorithms that provide optimized weapon-to-target pairing recommendations, including Multi-Platform scenarios involving heterogeneous assets (e.g., AC-130J, USVs, UAVs).
2. Optimized Weapon Settings: Develop algorithms that recommend the optimal weapon settings (e.g., fuse, delay, impact angle/aspect) to achieve a desired Probability of Kill (Pk) based on the target type and kill level.
3. Lethality and Collateral Damage Estimation: Develop algorithms that provide real-time, on-platform ("at the edge") lethality estimates using Government-approved models (e.g., AJEM) and provide 2D/3D visualizations of estimated collateral damage.

DRAFT

C.3.7.8 The Contractor shall provide experts proficient in the following Engagement and Assessment Algorithms:

1. Engagement Sequence Optimization: Develop algorithms that recommend the optimal order in which to engage a group of targets to maximize efficiency and effectiveness.
2. Gun Systems Automation: Develop algorithms to support gun-based engagements, including "Auto-Leading" for moving targets and optimized gun firing patterns for area targets.
3. Battle Damage Assessment (BDA): Develop algorithms that analyze post-engagement sensor data to provide an automated assessment of battle damage.

C.3.7.9 The Contractor shall provide experts proficient in newer technology & concepts that support the overall killchain and future killchain components. The Contractor shall support AI-based decision aids that can reason under uncertainty, evaluate courses of action (COAs), and provide recommendations to a human operator in accordance with the system's rules of engagement.

C.3.7.10 The Contractor shall develop algorithms to enable teams of autonomous platforms (USVs, UAVs) to work together to accomplish complex missions. The Contractor shall:

a) Develop and implement decentralized control algorithms for swarm and collaborative behaviors, including formation flying/sailing, coordinated search patterns, and distributed sensing.

b) Develop algorithms for dynamic task allocation and resource management within a swarm, allowing the collective to adapt to changing mission needs or the loss of individual agents.

c) Research and develop negotiation and consensus protocols for multi-agent systems, enabling them to collaborate in a communication-constrained or contested environment.

d) Develop algorithms that enable heterogeneous teaming, where different types of platforms (e.g., USVs and UAVs) collaborate, each performing tasks best suited to their capabilities.

C.3.7.11 The Contractor shall provide the expertise to research and develop next-generation autonomous capabilities. The Contractor shall:

a) Research, Develop and implement algorithms based on state-of-the-art technologies and implementation techniques.

b) Investigate and apply emerging AI techniques, such as Generative AI, Large Language Models (LLMs), and neuro-symbolic AI, to solve complex defense and intelligence problems.

C.3.7.12 The Contractor shall provide the expertise to research and develop AI/ML architectures capable of safe, bounded learning and adaptation after deployment. This shall include:

a) Researching and developing 'Online Learning' and 'Continual Learning' algorithms that can update and improve AI models based on new data observed during a mission, without catastrophically forgetting previous knowledge.

b) Developing the safety and validation architecture required to bound in-field learning, ensuring that any adaptations do not violate pre-defined safety constraints or the system's Rules of Engagement (ROE).

DRAFT

c) Developing techniques for "one-shot" or "few-shot" learning, enabling systems to learn to recognize new threats or objects from a very small number of examples provided by an operator in the field."

C.3.8 Analysis, Assessments, and Test & Evaluation (T&E) of Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.8.1 The Contractor shall provide a comprehensive T&E capability to ensure that AAI-enabled systems are effective, suitable, secure, and ready for deployment. This includes planning, executing, and reporting on all T&E activities, as well as developing the environment and tools required to conduct rigorous testing.

C.3.8.2 The Contractor shall develop and maintain the comprehensive planning documents required for the T&E program. The Contractor shall:

a) Draft and maintain the Test and Evaluation Master Plan (TEMP) for Government approval. This TEMP shall include a dedicated AI Test & Evaluation Annex that defines the strategy for testing and validating AI/ML components. (CDRL A00P)

b) Develop detailed Test and Evaluation Plans (TEPs) and Test Procedures for each test event, including specific test cases, data collection plans, and pass/fail criteria. (CDRL A00Q)

c) Document the results of all laboratories, developmental, operational, and field testing in formal Test Reports for delivery to the Government. (CDRL A00G)

C.3.8.3 The Contractor shall provide the engineering expertise to develop and sustain the environments and tools required to conduct AAI T&E. The Contractor shall:

a) Develop and maintain a high-fidelity Modeling and Simulation (M&S) environment that serves as the core of the system's Digital Twin. This includes developing realistic sensor models, environment models (weather, sea states), and physics-based entity models.

b) Develop the software and hardware interfaces required to connect the M&S environment to the Hardware-in-the-Loop (HWIL) and Software-in-the-Loop (SITL) testbeds, enabling large-scale, automated testing.

c) Develop custom data analysis, logging, and visualization tools to process the large volumes of data generated during T&E events, enabling the rapid evaluation of system performance and AI model behavior.

C.3.8.4 The Contractor shall conduct and/or support all phases of system testing. The Contractor shall:

a) Execute Developmental Testing (DT) to assess technical performance and progress against design requirements.

b) Support Government-led Operational Testing (OT) and live-force experimental exercises to measure mission effectiveness.

c) Conduct formal System Operational and Verification Tests (SOVT) prior to system delivery to verify that the system meets all specified functional and performance requirements in an operationally representative environment.

DRAFT

d) Conduct T&E activities in austere terrain and maritime environments (e.g., military ranges, field conditions, shipboard), including working non-standard hours to support test events.

C.3.8.5 The Contractor shall conduct T&E specifically focused on the performance and robustness of the AI/ML models. The Contractor shall:

a) Perform AI model performance evaluation against curated validation and testing datasets, measuring and reporting on key metrics such as precision, recall, F1-score, and confusion matrices.

b) Conduct Data-Centric Testing to evaluate model performance and degradation under a wide range of conditions, including low-quality or corrupted sensor data, varied environmental conditions, and out-of-distribution inputs.

c) Conduct Adversarial T&E by actively attempting to deceive, evade, or poison the AI models to identify vulnerabilities and test defensive measures.

d) Test and verify the performance of the entire MLOps pipeline, including automated data validation, model training, and deployment workflows, to ensure the integrity of the end-to-end process.

e) Develop and execute T&E methodologies for adaptive and learning systems. This includes testing the stability and safety of online learning algorithms and designing test scenarios to specifically induce and evaluate the emergent behaviors that may arise from multi-agent collaboration or in-field model updates.

C.3.9 Cybersecurity for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.9.1 The Contractor shall provide a comprehensive cybersecurity capability to ensure AAI-enabled systems are developed, deployed, and sustained in a secure manner. The Contractor shall be responsible for implementing security throughout the system lifecycle, protecting against both traditional and AI-specific threats. All activities shall be documented in a Cybersecurity Strategy, which the Contractor shall draft and maintain for Government approval. (CDRL A00R)

C.3.9.2 The Contractor shall perform the security engineering required to achieve and maintain system accreditation. The Contractor shall:

a) Provide all necessary engineering, documentation, and testing support for the Risk Management Framework (RMF) or other Assessment and Authorization (A&A) processes (e.g., Platform IT - PIT), with the goal of achieving and maintaining an Authority to Operate (ATO).

b) Implement and validate all applicable Security Technical Implementation Guidelines (STIGs), security controls, and installation checklists for operating systems, software, and network components.

c) Develop and implement Information Assurance (IA) methods for protecting data-at-rest and data-in-transit, including all tactical data links and interfaces with external systems.

C.3.9.3 The Contractor shall integrate security into the entire software development lifecycle. The Contractor shall:

a) Design, implement, and operate a DevSecOps pipeline that automates security testing and analysis.

b) Integrate Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools into the CI/CD pipeline to automatically scan for code vulnerabilities.

c) Perform Software Composition Analysis (SCA) to identify and manage vulnerabilities in third-party and open-source libraries.

C.3.9.4 The Contractor shall provide the expertise to secure the end-to-end AI/ML development pipeline from compromise. The Contractor shall:

a) Implement processes to ensure the integrity and security of all training data. This includes scanning datasets for malicious payloads and implementing techniques to detect and mitigate data poisoning attacks.

b) Implement procedures for vetting and scanning third-party or pre-trained AI models and open-source libraries before they are integrated into the system.

c) Secure the MLOps pipeline infrastructure itself, including the source code repositories, dataset storage, training servers, and artifact repositories, against unauthorized access or modification.

C.3.9.5 The Contractor shall design and implement defenses against attacks that specifically target AI models. The Contractor shall:

a) Develop and implement technical measures to detect and defend against adversarial machine learning attacks, including evasion, model inversion, and membership inference attacks.

b) Implement robust input validation and sanitization for all data being fed to AI models to prevent injection and manipulation attacks.

c) Design the system architecture to minimize the attack surface of the AI models and to contain the impact of a potential model compromise.

C.3.9.6 The Contractor shall provide continuous monitoring and respond to security threats. The Contractor shall:

a) Implement a Continuous Monitoring (ConMon) strategy to detect security anomalies in both the IT infrastructure and the behavior of the AI models.

b) Draft and maintain, for Government approval, an Incident Response (IR) plan that includes specific procedures for responding to a suspected compromise of an AI component. The IR plan shall be part of the Cybersecurity Strategy. (CDRL A00R)

C.3.10 Safety and Ethical Assurance for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.10.1 The Contractor shall provide the engineering and analysis expertise to ensure that all AAI-enabled systems are designed, developed, and tested to be safe, reliable, and trustworthy for operational use. All work in this section shall be documented in a comprehensive AI Safety Case

Report, which shall be delivered for Government review and approval prior to operational testing. (CDRL A00S)

C.3.10.2 The Contractor shall ensure that the system's design, development, and operational concepts are aligned with the Department of Defense Ethical Principles for AI (Responsible, Equitable, Traceable, Reliable, and Governable). The Contractor shall:

a) Provide analysis and technical data to support the Government's legal and ethical reviews of the system's capabilities.

C.3.10.3 The Contractor shall design and implement robust human-machine interfaces and control mechanisms to ensure appropriate human judgment and oversight. The Contractor shall:

a) Design, implement, and test the Human-in-the-Loop (HITL) and/or Human-on-the-Loop (HOTL) controls for all safety-critical and lethal functions.

b) Develop and test "fail-safe" mechanisms that allow a human operator to immediately halt, override, or disarm the autonomous system.

c) Conduct Human Factors Engineering and operator-in-the-loop testing to measure and verify that operators can effectively oversee and control the system, especially under high-stress conditions.

C.3.10.4 The Contractor shall implement a formal process to detect and mitigate unintended bias in AI models. The Contractor shall:

a) Analyze all training datasets for statistical bias related to demographic, environmental, or other factors that could lead to inequitable or poor performance against certain groups or conditions.

b) Conduct specific tests on trained models to evaluate their performance across different subgroups and identify any performance disparities.

c) Document all findings of bias and propose and implement mitigation strategies (e.g., data augmentation, algorithmic modifications) for Government approval.

C.3.10.5 The Contractor shall develop and implement techniques to improve the transparency and trustworthiness of the AI models. The Contractor shall:

a) Implement AI Explainability (XAI) methods (e.g., saliency maps, feature attribution) that provide human operators with insights into why an AI model made a specific recommendation or classification.

b) Develop and display model confidence scores to the user, providing a clear indication of the AI's certainty in its outputs.

c) Conduct analysis to define and characterize the "operational envelope" of each AI model, identifying the conditions under which the model is known to be reliable and providing warnings to the operator when the system is operating outside of those conditions.

DRAFT

C.3.10.6 The Contractor shall conduct formal Validation and Verification (V&V) on the behavior of the integrated autonomous system. The Contractor shall:

a) Develop formal verification test cases to prove that the system's autonomous logic correctly adheres to pre-defined constraints and Rules of Engagement (ROE).

b) Where applicable, utilize formal methods to mathematically verify the properties of safety-critical software and AI components.

c) Provide a final V&V report summarizing the evidence that the autonomous system behaves as specified and is ready for operational assessment. (CDRL A00T)

C3.11 DevSecOps, MLOps, and IT Infrastructure Engineering for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.11.1 The Contractor shall provide expert-level systems engineering and administration to architect, build, automate, secure, and sustain the entire digital ecosystem required for modern AAI development. The Contractor shall be capable of performing these functions by either modifying and extending Government-provided infrastructure and pipelines or by engineering, delivering, and sustaining a complete, equivalent contractor-provided ecosystem, as directed by the Government. All infrastructure, pipelines, and processes shall be documented as-built and maintained under configuration management.

C.3.11.2 The Contractor shall perform expert-level System Administration (SA) to ensure the stability, availability, and security of all supporting IT infrastructure. The Contractor shall:

a) Architect, deploy, and administer physical and virtual servers (Linux and Windows), storage solutions (e.g., NAS, SAN, object storage), and network infrastructure (switches, routers, firewalls).

b) Implement and operate a robust data backup, restore, and disaster recovery solution for all critical systems and data repositories.

c) Perform continuous system monitoring, performance tuning, and OS/software patching in accordance with cybersecurity directives.

d) Manage the full lifecycle of user accounts, groups, and permissions using directory services.

C.3.11.3 The Contractor shall engineer, operate, and continuously improve a fully automated DevSecOps pipeline for all non-AI software. The Contractor shall:

a) Design and build the CI/CD pipeline using tools such as GitLab CI or Jenkins to automate the build, integration, and testing of source code.

b) Integrate automated security scanning directly into the pipeline, including Static/Dynamic Application Security Testing (SAST/DAST) and Software Composition Analysis (SCA) to identify vulnerabilities in code and third-party dependencies.

DRAFT

c) Manage the full lifecycle of software artifacts, including versioning and storing compiled binaries in an artifact repository (e.g., Nexus, Artifactory).

C.3.11.4 The Contractor shall engineer, operate, and continuously improve a specialized MLOps pipeline to manage the end-to-end lifecycle of AI models. The Contractor shall:

a) Design and build automated data pipelines for data ingestion, validation, cleaning, transformation, and versioning.

b) Engineer and automate the Continuous Training (CT) process to orchestrate complex training jobs, log all experiment parameters and metrics, and version control the resulting trained models.

c) Develop and automate a model validation and testing pipeline that evaluates trained models against curated test datasets and checks for desired performance characteristics (e.g., bias, robustness).

d) Engineer the Continuous Delivery for Machine Learning process, automating the packaging of validated models into secure, versioned artifacts and deploying them to a model registry.

C.3.11.5 The Contractor shall provide expert-level support for containerization technologies as the foundation for modern application deployment. The Contractor shall:

a) Develop and maintain hardened, STIG-compliant base container images (using Docker or equivalent) for all applications and services.

b) Manage the container image lifecycle, including automated vulnerability scanning and storage in a secure container registry.

c) Architect and administer a container orchestration platform (e.g., Kubernetes), including managing cluster resources, networking, storage, security policies, and service meshes.

d) Develop and maintain Kubernetes operators and Helm charts to automate the deployment and management of complex applications.

C.3.11.6 The Contractor shall use modern Infrastructure as Code (IaC) practices to manage all computing environments. The Contractor shall:

a) Use IaC tools (e.g., Terraform, Ansible) to define, deploy, and manage all infrastructure, including virtual machines, networks, Kubernetes clusters, and cloud resources, ensuring all environments are reproducible and version-controlled.

b) Administer and optimize on-premises High-Performance Computing (HPC) clusters and Government-approved cloud environments, managing GPU allocation, job scheduling, and cloud cost monitoring.

c) Develop and maintain a library of reusable IaC modules to enable the rapid and consistent deployment of new development, testing, and production-like environments.

DRAFT

C.3.12 Integrated Logistics Support (ILS) for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.12.1 The Contractor shall provide a comprehensive ILS capability to ensure that AAI-enabled systems are supportable, sustainable, and ready for the warfighter throughout their entire lifecycle. The Contractor shall develop and maintain a Life Cycle Sustainment Plan (LCSP) for Government approval, which addresses both the physical and digital logistics required for autonomous systems. (CDRL A00U)

C.3.12.2 The Contractor shall perform the detailed engineering and analysis required to develop a complete supportability strategy. The Contractor shall:

a) Conduct a Logistics Support Analysis (LSA) to identify all requirements for spares, support equipment, and personnel.

b) Develop and document the Maintenance Concept for the system, defining the tiered maintenance strategy (O, I, and D-level) for both hardware and software, with specific considerations for AI/ML component failures.

c) Support the deployment and fielding of systems to ensure all necessary support elements are successfully delivered and transitioned to operational units.

d) Develop and maintain the Packaging, Handling, Storage, and Transportation (PHS&T) plan for all system components. (CDRL A00V)

e) Conduct Failure Modes, Effects, and Criticality Analysis (FMECA) to identify potential system failure points and inform sparing plans and maintenance procedures.

f) Perform Level of Repair Analysis (LORA) to determine the most cost-effective location and resource level for performing maintenance and repairs.

g) Develop and maintain a Reliability, Availability, and Maintainability (RAM) model for the system to predict and track field performance.

C.3.12.3 The Contractor shall develop a logistics strategy specifically for the digital components of the AAI system. The Contractor shall:

a) Develop and document the Digital Logistics Strategy, defining the process and infrastructure required to securely deliver, update, and manage AI models, software, and critical datasets to deployed and disconnected units.

b) Analyze the bandwidth and connectivity requirements needed to sustain the digital supply chain, including the transfer of large AI models and the collection of operational data from the field.

c) Define the process for operators to report, collect, and exfiltrate problematic operational data (e.g., false positives, missed detections) from the field back to the MLOps pipeline to support model retraining and improvement.

DRAFT

d) Develop and prototype a "Digital Logistics Locker" capability for deployed units, enabling them to securely store multiple versions of AI models and mission data, and to load them onto edge devices without needing a persistent network connection.

e) Define and document the data schema and format required for operational data logging, ensuring that data collected in the field is in a usable format for rapid ingestion into the MLOps pipeline.

f) Analyze and propose strategies for "Over-the-Air" (OTA) updating of AI models and software on deployed platforms, including methods for ensuring update integrity and performing rollbacks.

C.3.12.4 The Contractor shall develop and deliver the full suite of technical documentation required to operate, maintain, and provision the system. The Contractor shall:

a) Develop and deliver comprehensive Interactive Electronic Technical Manuals (IETMs) for operators and maintainers.

b) Develop manuals that include clear descriptions of the AI's intended function, known limitations, and operational envelopes.

c). Develop manuals that include specific troubleshooting procedures for AI-related failures, such as differentiating between a hardware fault, a software bug, and an AI model performance issue.

d) Provide all necessary technical data to support the establishment of National Stock Numbers (NSNs) and other supply system identifiers for all line-replaceable units (LRUs) and spares.

e) Develop documentation and provisioning data compatible with Government systems such as the Navy's Configuration Data Managers Database-open architecture (CDMD-OA).

C.3.12.5 Supply Support and Property Management: The Contractor shall provide the support necessary for managing the physical assets of the program. The Contractor shall:

a) Identify and provision for all General Purpose and Special Purpose Test Equipment.

b) Manage the inventory of all program property, including Government Furnished Property (GFP).

c) Execute the physical logistics of tracking, packaging, and shipping items to and from test sites and operational units.

d) Support the formal disposal of items in accordance with Government processes.

e) Develop and implement a specific maintenance and sparing plan for high-cost, specialized AAI hardware, such as GPU-based computers and advanced sensor suites, including procedures for diagnostics, repair, and technology refresh.

DRAFT

C.3.13 Training and Instruction Support for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems

C.3.13.1 The Contractor shall provide a comprehensive training and instruction capability to ensure that all personnel can employ, maintain, and trust the AAI-enabled weapon system safely, effectively, and in accordance with established doctrine. The Contractor shall develop and maintain a role-based Training and Certification Plan for Government approval, outlining the full training strategy and defining proficiency standards. (CDRL A00W)

C.3.13.2 The Contractor shall develop and deliver a curriculum focused on the ethical and procedural employment of the autonomous weapon system. The Contractor shall:

a) Conduct a Training Needs Analysis to define specific learning objectives for operators, maintainers, intelligence analysts, and commanders.

b) Develop a dedicated training module on the system's embedded Rules of Engagement (ROE) and firing doctrines. This shall include scenario-based testing to verify the operator's understanding of when the system is, and is not, authorized to be employed.

c) Create instructional content that explicitly links the system's functions to the DoD Ethical Principles for AI, ensuring operators understand the ethical framework governing the system's use.

d) Develop and deliver comprehensive Interactive Electronic Technical Manuals (IETMs) and tactical aides (TACAIDs) that are clear, concise, and accessible under operational stress. (CDRL A00X)

C.3.13.3 The Contractor shall develop a training program focused on building lethal and effective human-machine combat teams. The Contractor shall:

a) Design and deliver training scenarios focused on building calibrated trust, teaching operators to understand the system's strengths and, critically, its operational envelopes and known failure modes.

b) Develop curriculum that trains operators on the cognitive skills required to manage cognitive load, effectively supervise multiple autonomous systems, and interpret AI-generated recommendations and warnings.

c) Train operators on how to use the system's AI Explainability (XAI) features to rapidly assess the "why" behind an AI recommendation before making a final engagement decision.

d) Conduct training on procedures for graceful degradation of autonomy, ensuring operators can effectively transition from fully autonomous to semi-autonomous or manual control in response to system casualties or a changing tactical environment.

DRAFT

C.3.13.4 The Contractor shall leverage the Digital Engineering Environment to provide immersive and realistic combat training. The Contractor shall:

a) Develop a comprehensive Simulation-Based Training (SBT) program that utilizes the system's Digital Twin and HWIL testbeds to create a high-fidelity "virtual range."

b) Create a library of challenging training scenarios that allow operators to train against a full range of peer and near-peer adversary tactics, electronic warfare (EW) effects, and denied/degraded environments.

c) Develop a system for After-Action Review (AAR), using simulation data to provide operators with detailed feedback on their tactical decisions and their interaction with the autonomous system.

d) Develop scenarios that allow commanders and teams to rehearse complex, multi-platform, collaborative engagements involving multiple autonomous and manned systems.

C.3.13.5 The Contractor shall provide qualified personnel and logistical support to deliver standardized training and certification to the fleet. The Contractor shall:

a) Provide certified instructors, with experience in tactical operations, to conduct all training.

b) Form and deploy Mobile Training Teams (MTTs) to provide initial and sustainment training at fleet locations.

c) Develop and implement a formal Operator Certification Program, including practical evaluations, to ensure all personnel demonstrate proficiency before being authorized to operate the system.

d) Develop and implement a "train-the-trainer" program and provide the necessary materials to enable Government personnel to conduct organic unit-level training and certification.

C.3.13.6 The Contractor shall develop a dedicated training pathway for personnel responsible for the technical support and maintenance of the AAI system. The Contractor shall:

a) Develop course materials focused on advanced diagnostics and troubleshooting of the integrated weapon system, including procedures for isolating faults between hardware, software, networking, and AI model performance.

b) Provide training on the use of the "Digital Logistics Locker," teaching maintainers how to securely load, verify, and manage AI models, mission data packages, and cryptographic keys on deployed systems.

c) Develop training for maintainers on how to collect and exfiltrate high-quality data from the field (e.g., sensor logs, system performance data) to support remote diagnostics and future MLOps retraining cycles.

<u>C.3.14 Technical and In-Service Engineering Support for Autonomous Artificial Intelligence (AAI) & Machine Learning (AI/ML) Enabled Systems</u>

DRAFT

## H60 DEPARTMENT APPLIED ARTIFICAL INTELLIGENCE/INTELLIGENCE AUTOMATION SUPPORT SERVICES

## STATEMENT OF WORK

C.3.14.1 The Contractor shall provide a comprehensive in-service engineering capability to support the full operational lifecycle of fielded AAI-enabled systems. The Contractor shall serve as the primary technical resource for resolving fleet-identified issues, managing system upgrades, and ensuring sustained system performance.

C.3.14.2 The Contractor shall establish and operate a tiered technical support structure to provide timely and effective assistance to the fleet. The Contractor shall:

a) Provide Tier 1 (Help Desk) support to answer operator questions and resolve basic issues.

b) Provide Tier 2 (Field Support) support through deployed Field Service Representatives (FSRs) who can provide on-site troubleshooting, maintenance assistance, and over-the-shoulder training.

c) Provide Tier 3 (Deep-Level Engineering) support by making subject matter experts available to perform in-depth analysis and develop solutions for complex or systemic problems that cannot be resolved in the field.

C.3.14.3 The Contractor shall provide the engineering expertise to analyze and resolve technical issues identified by the fleet. The Contractor shall:

a) Log, track, and manage all fleet-reported issues, including Software Trouble Reports (STRs).

b) Perform deep-dive Root Cause Analysis (RCA) for complex system failures, with a specific capability to diagnose issues at the intersection of hardware, software, networking, and AI model performance.

c) Develop, test, and deploy corrective actions, including software patches and hardware modifications, in response to identified problems.

d) Provide engineering analysis and recommendations to the Government for all submitted Requests for Deviation, Requests for Waivers, and Engineering Change Proposals (ECPs).

C.3.14.4 The Contractor shall continuously monitor the performance of fielded AI models to ensure they remain effective over time. The Contractor shall:

a) Analyze operational data and performance metrics collected from deployed systems to detect and report on any AI model performance degradation (e.g., "model drift").

b) Investigate and determine the root cause of model degradation, which may include changes in the operational environment, new adversary tactics, or emergent data quality issues.

c) Provide technical recommendations to the Government on the need for AI model retraining, updates, or the development of new models to counter performance degradation.

DRAFT

C.3.14.5 The Contractor shall provide the engineering support required to manage and execute system upgrades. The Contractor shall:

a) Conduct feasibility analyses and provide technical and cost assessments for proposed system upgrades and technology insertions.

b) Perform the necessary engineering to integrate new hardware, software, and AI capabilities into the existing system baseline.

c) Support the production and procurement of system upgrades, including conducting make-or-buy analyses and evaluating data packages for new production techniques or materials.

C.3.14.6 The Contractor shall maintain a capability to provide an agile and rapid response to urgent fleet needs. The Contractor shall:

a) Support the Government in analyzing and validating Urgent Operational Needs (UONs) reported from the field.

b) Upon Government direction, execute a rapid development, test, and deployment cycle to deliver solutions to meet validated UONs. This includes the ability to rapidly update software or retrain and deploy targeted AI models.

C.3.15 Facilities, Fabrication, and Low-Rate Production (LRP)

C.3.15.1 The Contractor shall provide, manage, and maintain all facilities necessary to perform the full scope of work described in this SOW. These facilities shall be sufficient in size, security, and capability to support the entire lifecycle of AAI-enabled systems, from initial fabrication to full system integration and storage.

C.3.15.2 Contractor shall provide a primary engineering and software development facility within a 20-mile radius of NSWCDD, Dahlgren, VA. This facility shall, at a minimum, provide:

a) A controlled-access, climate-controlled lab and integration space of no less than 320 square feet (16'x20').

b) Conference and collaboration space, including tables and chairs, to seat no fewer than 20 Government and contractor personnel.

c) All necessary IT infrastructure, including high-speed internet (WiFi), telephones, and virtual collaboration tools (e.g., Webex).

C.3.15.3 The Contractor shall provide and maintain a dedicated fabrication facility with the space and equipment required for large-scale prototyping and assembly. This facility shall provide:

a) Sufficient fabrication floor space to allow for the assembly, integration, and maintenance of large-scale prototypes, including multiple Unmanned Surface Vehicles (USVs) and tactical vehicle mock-ups simultaneously.

b) All necessary fabrication equipment, including but not limited to CNC machines, welders, composite material layup tools, and 3D printers for both polymers and metals.

c) An electronics fabrication lab with the necessary tools for PCB assembly, soldering, and cable harness construction.

C.3.15.4 The Contractor shall provide and maintain secure facilities for the storage and operation of developmental and test assets. The Contractor must provide evidence of access to or ownership of:

a) Secure, covered, or dry-dock storage space suitable for multiple USVs, protecting them from the elements during maintenance, integration, and storage periods.

b) Secure, environmentally controlled storage areas for sensitive equipment, including Remote Weapon Stations (RWS), sensor suites, and high-performance computing hardware.

c) A dedicated, caged, or otherwise approved flight area for conducting developmental testing and operator training for small Unmanned Aerial Vehicles (UAVs).

d) Access to a private or Government-approved firing range suitable for the live-fire testing, calibration, and verification of RWS and other weapon systems.

e) Access to a private or Government-approved marina, pier, or boat ramp suitable for the routine launch, recovery, and pier-side testing of USVs.

C.3.15.5 The Contractor shall maintain the capability to transition successful prototypes into limited production. This includes:

a) Developing and documenting the formal production processes, quality control checkpoints, and acceptance test procedures required for a low-rate production line.

b) Establishing and managing the supply chain needed to source materials for LRP.

c) Executing LRP runs as directed by the Government to produce small quantities of systems for specialized fielding, operational assessments, or to fill urgent needs.

## 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).

DRAFT

C.4.1 Progress Report

The Contractor shall submit a Contracting Officer's Management Report. (CDRL A00Y) 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. The Contractor shall provide evidence invoices have been reviewed to ensure that all costs represent services that have been performed and are deliverable items. In accordance with G-232-H005 and FAR 52.216-7, 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 IPRs of work being performed. IPRs shall be conducted at the overall Task Order level. Reviews will be scheduled by the Contractor. An initial formal IPR shall be planned and conducted within 90 days of the Task Order award date and will follow the agenda agreed to by the Contracting Officer Representative (COR). Subsequent formal IPRs shall be held approximately every six months thereafter unless waived by the Government. IPRs shall be conducted at a location mutually agreed upon by the Contractor and the Government. The Contractor shall provide the IPR slides documentation IOW the instructions provided in the DD Form 1423 (CDRL A00Z). The Contractor shall document meeting minutes. (CDRL A002)

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 A002)

C.4.4 Telework

Teleworking at an alternative worksite is permitted in accordance with H-216-H002 Level of Effort-Alternate I (NAVSEA) (OCT 2018). For contractor personnel seated onsite at NSWC Dahlgren, telework permitted with prior approval by the Government SME and COR. Telework is also dependent upon the type of work being performed. In the event of telework, the Contractor shall track all Government Furnished Property. The Contractor shall document and track all Government equipment in their possession for teleworking by asset tag numbers and serial numbers (NMCI/RDT&E computers, monitors, etc.). 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

## H60 DEPARTMENT APPLIED ARTIFICAL INTELLIGENCE/INTELLIGENCE AUTOMATION SUPPORT SERVICES

## STATEMENT OF WORK

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 DoW 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 B001. The CWF report shall address required CWF training including annual continuous learning

training requirements. The Contractor shall also submit Mandatory Training Completion Log (CDRL B002). The Mandatory Training Completion Log shall address all mandatory training completed as directed by the COR.

## 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 number of personnel traveling shall be limited to the minimum required to accomplish work requirements and shall be requested and authorized in advance by the COR via email. As defined in the Federal Travel Regulation, Contractors are only authorized to use the most economical travel method unless previously approved by the Approving Official. All requests shall show the appropriate order number, the number of people traveling, the number of days for the trip, the reason for travel, an estimated cost (with General and Administrative [G&A] separate) and any high cost or unusual costs expected. In addition, all travel requests shall include supporting documentation to assist the Contracting Officer Representative (COR) determine allowability; that is, copies/screen shots of estimated cost of lodging, car rental, air fare, parking, etc. The COR will make the final determination of what support documentation is required before approving any travel request. 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 FAR 31.205-46 Travel Costs.
Representative travel locations may include the ones listed on the table below. The average length of each trip is estimated to last four days.

| Location | Base Year | | OY-1 | | OY-2 | | OY3 | | OY-4 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | # of Trips | # of Travelers | # of Trips | # of Travelers | # of Trips | # of Travelers | # of Trips | # of Travelers | # of Trips | # of Travelers |
| 29 Palms, CA | 2 | 10 | 2 | 10 | 2 | 10 | 2 | 10 | 2 | 10 |
| Yuma PG, CA | 2 | 10 | 2 | 10 | 2 | 10 | 2 | 10 | 2 | 10 |
| Camp Lejeune, NC | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 |
| Camp Pendleton, NC | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 |
| Quantico, VA | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 |
| VA Beach, VA | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 |
| Washington. DC | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 |
| Panama City, FL | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Colorado Springs, CO | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 |
| Annapolis, MD | 3 | 1 | 3 | 1 | 3 | 1 | 3 | 1 | 3 | 1 |
| Crane, IN | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 |
| Pensacola, FL | 3 | 1 | 3 | 1 | 3 | 1 | 3 | 1 | 3 | 1 |
| Fort Belvoir, VA | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Denver, CO | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 |
| Tampa, FL | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Fort Picket, VA | 3 | 4 | 3 | 4 | 3 | 4 | 3 | 4 | 3 | 4 |
| Fort Campbel, KY | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 |

The Contractor shall submit trip reports following any travel under this effort. (CDRL B002)

### C.6.2 Direct Charge of Materials

(a) It may be necessary for the Contractor to procure materials to respond to the mission requirements listed in the SOW during the performance of this Task Order. 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 FAR 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. All individual ODC purchases up to $10,000 in value shall be reviewed and approved by the COR; individual item purchases over $10,000 in value shall not be executed until the COR reviews the request and obtain approval 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 resources shall not be purchased unless DoW 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.
(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:

| Item |
|---|
| Test consumables (e.g., Dummy parts for destructive testing, batteries, cell phones, SIM cards, machined items and prototypes, circuit boards, control boards, electronic devices, shipping materials, paint, wood, epoxy, metal, plastic, tools, test enclosures). |
| Hardware (e.g., connectors, batteries, switches, UPS, backup batteries, cables, adapters, dongles, power supplies, fiber optic materials, amplifiers, wire assemblies, racks, transformers, circuit breakers, ropes) |
| Technical manuals |
| Lab tools |
| Test and developmental computers, Servers, and peripherals |
| Software and software licenses |
| Radios and other communication equipment |

| |
|---|
| VOIP and gateway hardware and software |
| Telephones, cell phones, and peripherals and associated airtime costs |
| PCBs, board accessories/assemblies |
| Antennas |
| Analysis and test equipment and tools |
| Incidental material and logistics costs (shipping/packaging) |
| Prototype drones and other autonomous systems and associated equipment |
| Weapon's Automation Packages |
| Shipping of materials to test and evaluation events and limited fielding |

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 by e-mail. The COR shall review the request, if it is in accordance with paragraph (b) above and requires Contracting Officer approval, the COR shall 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. Upon completion of the Task Order Period of Performance, all material associated with this Task Order that was 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

DRAFT

Contractor shall transfer all materials not depleted or previously delivered to the Government to the COR using the Material Inspection and Receiving Report (DD Form 250) and in accordance with DFARS PGI 245.402-71.

C.6.3 Counterfeit Parts and Materiel

(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 Contracting Officer 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 generate a Counterfeit Prevention Plan in accordance with DI-MISC-81832 Counterfeit Prevention Plan, and the requirements of this Data Item Description (DID) and SAE Aerospace Standard 5553 (SAE AS5553) Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition. (CDRL A00X).
- 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 material.
- 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.

DRAFT

- 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 products 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 material 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 products shall be disposed of in a way which would not allow their 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 Office 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 | OY1 | OY2 | OY3 | OY4 |
|---|---|---|---|---|---|
| Procurement Analyst | 1 | 1 | 1 | 1 | 1 |
| Network Engineer | 1 | 1 | 1 | 1 | 1 |
| Principle Software Engineers | 4 | 4 | 4 | 4 | 4 |
| Software Engineers | 1 | 2 | 2 | 2 | 1 |

| Labor Category | Base Year | OY1 | OY2 | OY3 | OY4 |
|---|---|---|---|---|---|
| Senior Software Engineers | 3 | 3 | 3 | 3 | 3 |
| Program Management Analyst | 1 | 1 | 1 | 1 | 1 |
| Systems Engineers | 2 | 2 | 2 | 2 | 2 |
| Test Engineers | 4 | 4 | 4 | 4 | 4 |
| Cybersecurity Specialists | 3 | 3 | 3 | 3 | 3 |

(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 | OY1 | OY2 | OY3 | OY4 |
|---|---|---|---|---|
| Network Engineer | 1 | 2 | 2 | 1 |
| Principle Software Engineers | 1 | 1 | 1 | 1 |
| Software Engineer | 2 | 3 | 3 | 2 |

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

(d) In support of individual projects, the Contractor should be prepared to work non-standard workdays with regards to length as well as start and end times, on various occasions in support of preparation and execution of test events, exercises, and rapid response requirements. The Contractor should also be prepared to work in austere terrain/environments (i.e. Military ranges, field conditions) to include sleeping in the field with the Marines/soldiers during exercises (on rare occasions) or in shipboard environments.

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 B004) issued under this Task Order. This requirement is in addition to anything required by regulation, statute, or the assigned Government Property Administrator.

C.7.3 Government Furnished Information

DRAFT

**H60 DEPARTMENT APPLIED ARTIFICAL INTELLIGENCE/INTELLIGENCE AUTOMATION SUPPORT SERVICES**

**STATEMENT OF WORK**

(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.

C.8 SECURITY

C.8.1 Personnel Clearance Requirements

(a) Facility Clearance Level (FCL) Requirement: The Prime Contractor supporting this Task Order is required to have a FCL of 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 support personnel, are required to have, as a minimum, a current SECRET security clearance in the Defense Industrial Security System (DISS).

The labor categories listed in the table directly following this paragraph shall have a TOP SECRET security clearance with Sensitive Compartmented Information (SCI) eligibility in DISS; interim clearances are acceptable. In addition, personnel performing in the labor categories identified by an asterisk (*) shall be required to meet all the qualifications to be designated as IT-Level 2 Cyberspace Workforce.

| Labor Category | Quantity |
|---|---|
| Senior Software Engineer* | 2 |
| Principle Software Engineer* | 1 |
| Cybersecurity Specialist* | 1 |
| Senior Systems Engineer | 2 |

Personnel performing in the labor categories listed in the table directly following this paragraph shall have a TOP SECRET security clearance in DISS. Interim clearances are acceptable. In addition, personnel performing the labor categories identified by an asterisk (*) shall be required to meet all the qualifications to be designated IT-Level 2 Cyberspace Workforce.

| Labor Category | Quantity |
|---|---|
| Sr. Program Manager | 1 |
| Senior Systems Engineer | 1 |
| Principle Software Engineer* | 3 |
| Network Engineer* | 1 |
| Systems Engineer | 3 |
| Test Engineer* | 1 |

Personnel performing in the labor categories listed in the table directly following this paragraph shall have a final SECRET security clearance in DISS. In addition, personnel performing the

labor categories identified by an asterisk (*) shall be required to meet all the qualifications to be designated IT-Level 2 Cyberspace Workforce.

| Labor Category | Quantity |
|---|---|
| Senior Software Engineer* | 3 |
| Principle Software Engineer* | 5 |
| Systems Engineer | 5 |
| Network Engineer | 1 |
| Cybersecurity Specialist* | 2 |
| Systems Administrators* | 2 |
| Finance Analysts | 1 |
| Procurement Analyst | 1 |
| Logistician | 1 |
| Program Management Analyst | 2 |
| Configuration Management Analyst* | 2 |
| Software Engineer | 3 |
| Technical Specialists | 2 |
| Electrical Engineer | 1 |
| Mechanical Engineer | 1 |
| Test Engineer* | 5 |

(c) 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).

(d) The Department of Defense (DoD) 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.

(e) 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.

(f) The Contractor must comply with guidelines specified on the DD Form 254. Contractors SCI indoctrinated in support of this contract shall comply with the reporting requirements as outlined in DOW policies Security Executive Agent Directive (SEAD)-3 dtd 12 June 2017 and SEAD-4 Implementation memo dtd 02 Nov 2020. All deliverables associated with this Task Order will be non-SCI.

DRAFT

(g) 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).
The Contractor requires access to SCI Intelligence in order to perform analysis of weapons systems. 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. The Contractor shall identify covered defense information and mark information in accordance with the DoD procedures for identification and protection of controlled unclassified information (CUI) found in DoDI 5200.48, Controlled Unclassified Information, Controlled Unclassified Information (CUI). All above accesses are needed to support and provide the system engineering, software development, and maintenance of Navy tactical initiatives and spiral and baseline developments to support NSWCDD.

C.8.2 Facility Clearance

The Contractor shall possess and maintain a SECRET facility clearance as verified within the National Industrial Security System (NISS)

(a) 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.

(b) 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.8.3 Electronic Spillage

(a) 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. In the event that 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.

(b) NSWCDD Security will continue to be responsible for the corrective action plan in accordance with the security guidance reflected on the DoW 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 for working 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.8.4 Portable Electronic Devices (PEDs)

(a) 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 being 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.

(b) 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) 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.

(d) 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.

(e) Personally owned hardware or software shall not be connected or introduced to any NSWCDD hardware, network or information system infrastructure.

C.8.5 Navy Issued Peripherals

(a) 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.

(b) 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 is occurring.

(c) 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.

(d) 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.

(e) Government issued peripherals may be used on personal devices.

(f) 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.8.6 Operations Security (OPSEC)

DRAFT

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 shall 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 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.8.7 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.8.8 IT-1 Designation Requirements

(a) 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.

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

C.8.9 Visits by Foreign Nationals and Foreign Representatives

**H60 DEPARTMENT APPLIED ARTIFICAL INTELLIGENCE/INTELLIGENCE AUTOMATION SUPPORT SERVICES**

**STATEMENT OF WORK**

(a) Task Order performance may require that the Contractor host, at an off-base location, foreign nationals and/or foreign representatives. A foreign national is a person who is a citizen of a foreign nation, and who is not a citizen of the United States. A foreign representative is a person who represents a foreign interest in dealings with the U.S. Government, either directly or through dealings with a U.S. Government Contractor. A foreign representative may be a United States citizen.

(b) A Contractor-hosted visit of a foreign national or foreign representative may be either an "official" visit or an "unofficial" visit. An official visit is a visit where the foreign national or foreign representative represents a foreign government in an official capacity. An unofficial visit is a visit where the foreign national or foreign representative is not representing a foreign government.

(c) A visit by a foreign national or a foreign representative may be either "DoW Sponsored" or "Non-DoW Sponsored". A DoW Sponsored visit is a visit that is coordinated by a DoW entity. A Non-DoW Sponsored visit is a visit that does not involve DoW coordination (A visit by either a foreign national or a foreign representative pursuant to performance by the Contractor under this Task Order is not considered to be, by itself, a sponsored visit).

(d) The Contractor hosting a visit by either a foreign national or a foreign representative is responsible for adherence to Department of War and Department of the Navy directives, instructions, regulations, and manuals that govern foreign disclosure. "Foreign Disclosure" is defined as the disclosure of Classified Military Information (CMI) and Controlled Unclassified Information (CUI) to foreign nationals and/or foreign representatives. Disclosure of such information may be accomplished orally, visually, in writing, or by any other medium.

(e) Classified Military Information (CMI). This is information that is originated by or for the Department of War, or a Military Department, or an entity under its jurisdiction and control, and which requires protection in the interest of national security. Such information is designated as TOP SECRET, SECRET, or CONFIDENTIAL.

(f) Controlled Unclassified Information (CUI). This is information that although unclassified is subject to access or distribution limitations in accordance with statute or regulation. Included is information exempt from mandatory release to the public under the Freedom of Information Act, or information that is subject to export control.

(g) NSWCDD Foreign National Visitor and Foreign Disclosure Application process. The NSWCDD has established a foreign national visitor approval and foreign disclosure process. Whenever, pursuant to the terms of this Task Order, a visit to a Contractor facility or Contractor workspace by a foreign national or foreign representative is anticipated, and one or more NSWCDD employees will be in attendance at this visit/meeting for the purpose of potential discussions, above the public release level, resulting in disclosure of either CMI or CUI, a completed "NSWCDD Foreign National Visitor and Foreign Disclosure Application" e-form must

be supplied to the Contractor's Facility Security Officer (FSO). The accountable NSWCDD personnel attending the meeting must ensure that the NSWCDD disclosure process has been complied with and an approved copy of the "NSWCDD Foreign National Visitor and Foreign Disclosure Application" generated e-form has been provided to the COR and the Contractor's FSO. The Contractor's FSO should ensure that approved copies of the e-form are maintained at their facility as a record of compliance with requirements set forth in 32 CFR Part 117 as well as the requirements set forth above.

C.8.10 Secure Link

(a) The Contractor shall provide their own secure facility at the SECRET level. The Contractor is advised that in order to perform in accordance with the SOW requirements, the Contractor must be able to participate in a classified network connection to the computing environment.

(b) In order to participate in the network, the Contractor shall have a secure line or secure data connection from their facility (the primary facility/facilities proposed to support this Task Order) to NSWCDD. The following paragraphs delineate the basic requirements that must be met before network access is permitted.

(1) The Contractor shall have or be willing to provide no later than 180 days after Task Order award:

(i) A data transmission line connecting the Contractor's classified IT environment to NSWCDD's computing environment via Type 1 approved encryption device. The data transmission line shall be capable of carrying data at a rate commensurate in efficiently transferring large data files. The following options are acceptable for providing the required connectivity:

(a) Connection to the fiber distribution system that directly connects from the IWSL to select office buildings.

(b) An existing Secret Internet Protocol Router (SIPR) Point of Presence (PoP) (if a SIPR PoP is not already in place, the time required to put a SIPR PoP in place would fail to meet the schedule requirements).

(c) Utilize any current technology or most efficient connectivity available (I.E. Encrypted over Internet Service Provider (ISP) connection).

The Government will cover the non-recurring costs necessary to establish the secure data transmission link up to the established Not-to-Exceed (NTE) ODC amount. The Contractor shall be responsible for all recurring costs relating to the operation or maintenance of the secure data transmission link.

(ii) Access to an approved fiber connection providing connectivity to NSWCDD:

(a) The fiber connection must be encrypted utilizing National Security Agency (NSA) Type 1 encryption and must be approved at the Secret (or higher) level. The encryption device must be stored in a secure area that meets the construction requirements of the CFR Part 117, Section 117.15 and be accredited by the Defense Counterintelligence and Security Agency (DCSA) (IS Specialist, Capital Area phone 1-888-282-7682).

(b) Stand-alone PCs or Local Area Networks (LANs) used in the secure area must meet the minimum security requirements of CFR Part 117, Section 117.15 and be accredited by DCSA. System configuration must be approved by NSWCDD.

(c) A COMSEC account is required for the receipt of the hardware and keying material necessary to support the encrypted connectivity. The Contractor shall have a Defense Courier Service (DCS) account to support the receipt and shipment of the operational key.

(d) As part of the NSWCDD Security Office's Memorandum of Agreement (MOA) with DCSA, the Contractor shall complete a Network Participants' Data Sheet (NPDS) and submit it to the NSWCDD Network Security Representative for approval.

(e) The Contractor shall attend or have attended Tactical Local Area Network Encryptor (TACLANE) encryptor training at the Contractor's expense within 90 days of Task Order award.

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.

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/.

DRAFT

C.9.4 Within 30 days of the Task Order performance commencing, the Contractor shall certify by email to their COR that the requirements captured above have been met. The email shall include the name of each employee 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) 5210.8F 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 5100.01 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.

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).

DRAFT

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 workspaces 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 DoN 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. DoN 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 examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over a DoN system may be monitored. Use of a DoN 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 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 Facilities

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) 6211.02D 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.

(b) Inherently-Governmental functions are not within the scope of this Task Order. Decisions relating 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 DoW 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 personnel engaged in work while on Government property shall be subject to the 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 AWAWRD 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 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

(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, provide 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.)

DRAFT

(c) Chronological Work History/Experience

(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 bullet 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.

DRAFT

(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.

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 to be 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

(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.

(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.

C.24 OPERATION OF GOVERNMENT VEHICLES

(a) The Contractor shall be required to drive Government vehicles both onsite at NSWCDD and offsite when requested by the Government. 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 vehicles are

DRAFT

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 when applicable. 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 shall 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) 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 work onboard US Navy Ships must have a current SECRET Security Clearance, at a minimum. The Contractor is responsible for briefing the ship/command upon arrival if not led by a Government representative. The Contractor is responsible for debriefing the ship/command upon departure, if not led by a Government representative, 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 B002).

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

(d) All personnel shall conform to the rules and regulations of the ship while shipboard. 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 to.

(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 brief the Commanding Officer or his/her designated representative as to the purpose of the visit and expected duration upon arrival.

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

(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.

DRAFT