STATEMENT OF WORK (SOW) TITLE: *Command & Control Experimentation (C2X) and Modernization Software Engineering Services for Future Naval Operations*

1.0 BACKGROUND

PMW 150 (The Command and Control Program Office) and the Naval Information Warfare Center Pacific (NIWC PAC) provides operational and tactical command and control capabilities by integrating real-time and near real-time representations of tactical situations while including Operational Picture, targeting support, chemical-biological warnings and tactical data link support for the Navy, Marine Corps, joint and coalition warfighters. This includes programs such as Global Command and Control System – Maritime (GCCS-M), Maritime Tactical Command and Control (MTC2), Nites Next, Command and Control Processor (C2P), Link 16 Network, Link Monitoring and Management Tool (LMMT), and a variety of other systems and sub-projects.

The work proposed under this project builds upon Basic and Applied Research performed by the contractor and funded through a variety of sponsors including but not limited to Office of the Secretary of War (OSW), NAVWAR, PEO C4I, Office of Naval Research (ONR) and NIPO in cooperation with the NIWC PAC. The intent of this proposed effort will be to further mature the technologies developed under these previous research programs, increase their Technology Readiness Level (TRL) and prepare them for transition to a number of possible Programs of Record.

This is a severable effort.

1.1 SCOPE

The main objective of this effort is to modernize and align Naval Command and Control for Integrated Joint/Coalition Fires and make it deployable to afloat and ashore sites such as the Carrier Strike Groups (CSG) to include CRUDES/DDGs and Carrier Airwing assets, Expeditionary Strike Group (ESG), Marine Corps NMESIS, Army HIMARS, Airforce assets, Coalition Forces, Tactical Fleet Command Centers (TFCC), Operational Command Post (OCP) and the Maritime Operations Centers (MOC). This effort will enhance the warfighters' decision-making and information gathering effectiveness by integrating and taking advantage of Machine Learning/Artificial Intelligence (ML/AI) approaches. The intent is to mature / modernize the technologies, increase their Technology Readiness Level (TRL) and prepare them for transition to a number of possible Programs of Record (PoR). This effort will include providing prototype validation, research and development, software development, implementation, test and verification for advanced C2 technologies. Specifically, this effort will provide development of software products utilizing microservices, containers, service mesh, and Kubernetes previously explored under the C2X project for use in command and control environment. The development work will include the design and implementation of container-based software, research and performance characterization of C2 application functionality, Artificial Intelligence, Machine Learning, Operations Research (AI/ML/OR), capturing and validating user stories, workflows, applying cybersecurity best practices, utilizing a DEVSECOPS pipeline, and related Navy Mission Essential Tasks, and development of associated technical documentation.

Development work will include but is not limited to:

a. Development, implementation, and testing of software code for the Rapid Asset Pairing Tool (RAPT),
b. Development, implementation and testing of software code for the Warfighting Capability Tool (WarCaT).
c. Development, implementation and testing of software code for the True Numbers (TN) data environment and evolving data analytics.
d. Developing, implementation and testing of software code for the Battlespace Integrated Graphics Styler (BIGS).
e. Development, implementation and testing of software code for the Natural-language Ontologies for battlespace Visualizations and Analytics (NOVA).
f. Developing, implementation and testing software code for the Altering Current-state to an Effective Desired-state (ACED).
g. Development, implementation and testing of software code for the Advanced Correlator- Navy (ACOR-N).
h. Development, implementation and testing of Large Language Models (LLM) to support operational requirements for planning and execution.

i. Development, implementation, and testing of AEGIS Combat System such REAPER and the Command, Control Combat System Interface (C3SI).
j. Development, implementation, and testing of the Naval Aviation Readiness Dashboard (NARD)
k. Integration of Generative AI (GENAI)
l. Implementation, and testing into the Command and Control Experimentation (C2X) Service Mesh Architecture for all applications.
m. Implementation, and testing into the Maritime Tactical Command and Control (MTC2) application for alignment with the PoR.
n. Implementation, and testing of applications to support Coalition Partners pursuant to Foreign Disclosure Office (FDO) guidance.
o. Delivering software builds, testing, and cyber scans in the C2X DEVSECOPS environment and the Overmatch Software Armory (OSA) and posting containers in the OSA Software Artifactory.
p. Development of software for processing by information systems of human originated inputs and queries providing automated machine to machine data source ingest.
q. Development of Dynamic and/or probabilistic mission execution enablers of modern tools that would decrease the time of decision making by increasing situational awareness and understanding during operations
r. Development of Human-information system interaction capabilities in distributed computing environments, including command system applications by introducing ML/AI/OR methods to interpret displays/information in the Common Operating Picture (COP) and providing 'ALERTS' for recommended Pre Planned Responses (PPRs) based on the Commander's Critical Information Requirements (CCIRs), and predictive enemy courses of action (ECOAs).
s. Development of Domain dependent and independent information detection, extraction, and retrieval using Natural language Processing (NLP) methods to ingest and interpret Navy-wide and CSG messages including OPTASKS/PPRs. Application of automation to aggregate historical information into a repository for design exploration and future application. Implementation of 'real time' application of AI tools for Current Operations enhancing awareness and applying prototype validation to current and future operations.
t. Development of new concepts in perception and visualization for display of current and future scenarios generated in real time where Warfare Commanders (WC) have assets with weapons 'covering' enemy platforms.
u. Utilization of C2X DEVSECOPS environment and OSA for implementation builds, code scanning, packaging into containers and testing deployments.
v. Provide support for operational deployment of C2X, exercises and experimentation.
w. Ensuring that software developed under this effort is running correctly within the CANES representative test environments in OSA, CSE, OPE, afloat, and/or the CTB hardware in the loop lab.

2.0 APPLICABLE DOCUMENTS

DODM 5200.01, Volume 1, DoD Information Security Program: Overview, Classification, And Declassification, dated February 24, 2012, Change 3 17 January 2025
DODM 5200.01, Volume 2, DoD Information Security Program: Marking Of Classified Information, dated February 24, 2012, Change 4 28 July 2020
DODM 5200.01, Volume 3, DoD Information Security Program: Protection Of Classified Information, dated February 24, 2012, Change 4 17January 2025
DODI 5200.48, Controlled Unclassified Information (CUI), dated 6 March 2020
DoDM 5200.02 - DoD Manual – Procedures for the DoD Personnel Security Program (PSP) dtd 3 Apr 17, Change 1 29 October 2020
DoDI 5200.02, DoD Personnel Security Program (PSP), 21 Mar 2014, Ch-3, 24 Sep 2020
DOD 5205.02-M, DOD Operations Security (OPSEC) Program, Ch-2 29 October 2020
DoDI 5220.31, National Industrial Security Program (NISP), 9 May 2023
DoDM 5220.32, Volume 1, National Industrial Security Program: Industrial Security Procedures for Government Activities, 1 August 2018, Ch-2 10 December 2021
DoDM 5220.32, Volume 2, National Industrial Security Program: Procedures For Government Activities Relating To Foreign Ownership, Control, Or Influence (FOCI), 17 April 2014, Ch-2 10 December 2021

Code of Federal Regulations, 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM), 24 Feb 2021
DoDI O-2000.16 Volume 1, DoD Antiterrorism Program Implementation: DoD Antiterrorism Standards,17 November 2016, Ch-3 7 May 2021
SECNAVINST 5510.30C, Department of Navy Personnel Security Program, 24 January 2020
SECNAVINST 5510.36B, DON Information Security Program, 12 July 2019
SPAWARINST 3432.1 (Series), Operations Security Policy, 2 February 2005
DoDD 5205.02E, DoD Operations Security (OPSEC) Program, 20 June 2012, Ch-2 20 August 2020
Navy Tactics, Techniques, and Procedures (NTTP) Operations Security (OPSEC) Manual: NTTP 3-13.3 dated 16 December 2022
NIWCPACINST 5500.1D, Command Security Manual, 15 August 2023
DoD 5015.21-M Volume I, Ch-2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security, 6 Oct 2020
DoD 5105.21-M Volume II, Ch-2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security, 2 Nov 2020
DoD 5105.21-M Volume III, Ch-2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security, 14 Sep 2020

3.0 PERFORMANCE REQUIREMENTS

3.1 Office of the Secretary of Defense (OSD)

As reflected under the scope above, the main technical objective of this program is to modernize the Navy's command and control capabilities to provide Joint/Coalition Integrated support for Fires. This effort will be accomplished by enhancing the warfighters' decision automation tools and information gathering effectiveness by integrating and taking advantage of ML/AI/OR approaches.

The contractor shall perform the tasks identified below to accomplish the above objectives of this effort.

A. Requirements

A.1. The contractor shall perform the following tasks.

A.1.1. The contractor shall gather and analyze system requirements for Processing by Information Systems of Human Originated Inputs and Queries and perform implementation tailoring for Fleet Naval Forces, Fires Coordination, Maritime Operations Center (MOC) and Coalition support. This will entail automation processes provided through software widgets/component development that enables 'real time' updates to status, including warfare conduct, state assessment of systems and munition by type and capability remaining, and prototype validation of which assets are suitable to conduct missions. Then composing most suitable assets, using the most appropriate capability, to perform the correct task, accomplishing the best result(s) achieving the required effect and on time is the ultimate goal.

A.1.2. The contractor shall gather and analyze system requirements for Dynamic and/or Probabilistic decision automation tools. The contractor shall develop decision aids tracking, evaluating and projecting key indicators, measures of performance and effectiveness to provide a comprehensive mission state and impact assessment. This will entail developing a suite of modern tools to decrease the time of decision making by increasing situational awareness and understanding during operations. The contractor shall develop automated, updated, comprehensive status boards, integrated with modern processing, prototype validation (Machine Learning {ML}/Artificial Intelligence {AI}) and Operations Research (OR), implementing GENAI and LLMs, coupled with data ingest methods from disparate data sources to feed the applications to build understanding of the Common Operational Picture (COP) Area of Responsibility (AoR).

A.1.3. The contractor shall gather and analyze system requirements for Human/IS Interaction in Distributed Computing Environments, including C2 system applications. The contractor shall develop ML/AI/OR methods to interpret displays/information in the COP and provide 'ALERTS' for recommended Pre Planned Responses (PPRs) based on the Commander's Critical Information

Requirements (CCIRs), and predictive enemy courses of action (ECOAs). The contractor shall provide methods to label data on ingest and continue to train ML/AI technologies using new automated methods.

A.1.4. The contractor shall gather and analyze system requirements for Domain Dependent and Independent Information Detection Extraction and Retrieval. The contractor shall introduce the use of Natural language Processing (NLP) methods to ingest and interpret Navy-wide and CSG OPTASKS/PPRs, automation to aggregate historical information into a repository for prototype validation and future application, and 'real time' application of tools for Current Operations to enhance awareness and incorporate prototype validation to current and future operations data sets to support prediction with greater accuracy.

A.1.5. The contractor shall gather and analyze system requirements for new concepts in Perception and Visualization. The contractor shall create automated widgets that track maintenance, casualties, munitions, sensors, platforms, and communication status with detailed prototype validation of risk providing a marked increase in Situational Awareness for watch standers to support decreasing time of response thereby providing greater decision advantage to warfighters.

A.1.6 The contractor shall perform Software Engineering efforts that align to existing Development-Security-Operations (DEVSECOPS) platforms and policies. The contractor shall deliver software builds, test, and cyber scans in the C2X GITLAB environment and the Overmatch Software Armory (OSA) and post containers in the OSA Software Artifactory.

A.1.7 Support will be required from the unclassified to the TS/SCI level as directed by relevant SCGs and Original Classification Authorities. Designated TS/SCI support will be required to obtain and maintain SCI clearances and Joint Worldwide Intelligence Communication System (JWICS) accounts to support meetings, reviews, communications, actions, and datacalls at the SCI level.

A.2 Software Engineering Approach

The contractor shall define a software development approach appropriate for the computer software effort to be performed. This approach shall be documented in a Software Development Plan (SDP)(CDRL A005). The contractor shall follow this SDP for all computer software to be developed or maintained under this effort.

The SDP shall define the contractor's proposed life cycle model and the processes used as a part of that model. In this context, the term "life cycle model" is defined in IEEE/EIA Std. 12207.0. The SDP shall describe the overall life cycle and shall include primary, supporting, and organizational processes based on the work content of the solicitation. In accordance with the framework defined in IEEE/EIA Std. 12207.0, the SDP shall define the processes, the activities to be performed as a part of the processes which support the activities, and the techniques and tools to be used to perform the tasks. Because IEE/EIA Std. 12207 does not prescribe how to accomplish the task, the contractor must provide this detailed information so the Government can assess whether the contractor's approach is viable.

The SDP shall contain the information defined by IEEE/EIA Std 12207.1, section 5.2.1 (generic content) and the Plans or Procedures in Table 1 of the IEEE/EIA Std. 12207.1. In all cases, the level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted. Information provided must include, as a minimum, specific standard, methods, tools, actions, strategies, and responsibilities associated with development and qualifications.

Support for software engineering and capabilities will be required from the unclassified to the TS/SCI level as directed by relevant SCGs and Original Classification Authorities.

3.2 NAVWAR (PMW 150)

B. Requirements:

B.1. NAVWAR PMW 150 is another sponsor that intends to contribute funds toward the effort and ultimate goals identified under paragraph 3.1 above for all periods of performance.

3.3 Navy International Program Office (NIPO)

NIPO is another sponsor that intends to contribute funds toward specific portions of the contractor effort and ultimate goals identified under paragraph 3.1 above for all periods. The specific portions that NIPO intends to contribute funds toward are identified below.

C. Requirements

C.1. Tasking / goals identified under A.1.1.

C.2. Abbreviated tasking/goals identified under A.1.3 as follows: The contractor shall gather and analyze system requirements for Human/IS Interaction in Distributed Computing Environments, including Coalition for C2 system applications.

C.3 Similar to A.1.5 as follows: The contractor shall gather and analyze system requirements for new concepts in Perception and Visualization based on Coalition data sets. The contractor shall create automated widgets that track maintenance, casualties, munitions, sensors, platforms, and communication status with detailed prototype validation of risk providing a marked increase in Situational Awareness for watch standers to support decreasing time of response thereby providing greater decision advantage to warfighters.

C.4 Tasking / goals identified under A.1.6.

3.4 NAVWAR (Overmatch)

D. Requirements:

D.1. NAVWAR is another sponsor that intends to contribute funds toward the effort and ultimate goals identified under paragraph 3.1 above for all periods.

3.5 Office of Naval Research (ONR)

E. Requirements:

E.1 Develop software capabilities as defined in the scope of work being done and perform Software Engineering efforts that align to existing Development-Security-Operations (DEVSECOPS) platforms and policies. The contractor shall deliver software builds, test, and cyber scan in the C2X GITLAB environment or other designated DEVSECOPS environment, the Overmatch Software Armory (OSA), and post containers in the OSA Software Artifactory.

E.2 Integrate developed capabilities with the Maritime Tactical C2 (MTC2) Program of Record (PoR) to demonstrate interoperability with a CSG planning tool,

E.3 The minimum viable product (MVP) requirements include developing and containerizing capabilities and maturing the product for transition to the PoR. Containerized capabilities will need to be aligned to the CANES technology stack. A SOP procedure that moves code from the operational prototype to a productionized container will be aligned with the PMW150 S&T Facility and the Overmatch OSA environment.

E.4 Support will be required from the unclassified to the TS/SCI level as directed by relevant SCGs and Original Classification Authorities. Designated TS/SCI support will be required to obtain and maintain SCI clearances and Joint Worldwide Intelligence Communication System (JWICS) accounts to support meetings, reviews, communications, actions, and datacalls at the SCI level.

E.5 Support for software engineering and capabilities will be required from the unclassified to the TS/SCI level as directed by relevant SCGs and Original Classification Authorities.

4.0 ESTIMATED LONG DISTANCE TRAVEL (in support of above tasking / goals)

It is anticipated that the travel will originate from the contractor facility

Place	No of Personnel	No of Days	No of Trips
Base Period:			
San Diego	2	5	4
San Diego	3	5	4
Option 1:			
San Diego	2	5	4
San Diego	3	5	4
Option 2:			
San Diego	2	5	4
San Diego	3	5	4
Option 3:			
San Diego	2	5	4
San Diego	3	5	4
Option 4:			
San Diego	2	5	4
San Diego	3	5	4

Travel costs related to transportation, lodging, meals, and incidental expenses are allowable subject to the limitations described at FAR 31.205-46.

Contractor personnel must adhere to all current DoD, SECNAV, OPNAV, and NIWC Pacific instructions related to foreign travel (if foreign travel is anticipated).

In the course of performance, travel in addition to that estimated above may be required to support the scope/tasking/goals in this SOW. If additional travel is necessary, the contractor shall comply with relevant SOW addendum text(s) and clauses for domestic or foreign travel.

5.0 PROPERTY REQUIREMENTS

- Government Furnished Property (GFP): None anticipated
- Government Furnished Information (GFI): None anticipated. See applicable documents section for relevant Government information.
- Government Property (incidental): None anticipated.
- Government Furnished Facilities: None anticipated.

- Contractor Acquired Property: None anticipated.

6.0 SECURITY

The security requirement for this tasking will be up to and including TOP SECRET/SCI. Most technical personnel performing on this task must be cleared to the SECRET level with the exception of select personnel performing tasks for paragraph 3.1, 3.2, 3.4, 3.5 who will need to be cleared at the TOP SECRET/SCI level. The work performed by the contractor will include access to unclassified and up to TOP SECRET/SCI data, information, and spaces. The contractor will be required to attend meetings classified up to TOP SECRET level. The contractor will be required to access TOP SECRET COMSEC, SIPRNET and JWICS at Government locations.

Most cybersecurity efforts will be at the Secret level or below, but some components will require SCI review and/or accreditation. Contractors supporting programs with SCI components will be required to obtain and maintain an active SCI clearance and JWICS account to attend technical meetings, review classified design material, and manage cybersecurity plans and actions.

Contractor personnel assigned to this effort who require access to SCI data and spaces must possess a current SSBI/T5/T5R with ICD 704 eligibility (which replaced DCID 6/4 eligibility) and be enrolled in Continuous Vetting.

Personnel requiring privileged access to government information systems must have a favorable Tier 5 background investigation or its equivalent.

Some contractor personnel will perform non-technical, administrative duties at the Unclassified and/or Controlled Unclassified Information (CUI) level at the contractor facility. These duties do not involve a CAC for logical access to government information systems nor physical access to the base. Therefore, a Fitness Determination by NIWC PAC Personnel Security is not required.

Although there is no requirement for the contractor to access NATO on this contract per Naval Intelligence Security Policy Directive 17-008 those contractors that have SCI and those with SCI access and will need access to JWIC and SIPRNet shall be North Atlantic Treaty Organization (NATO) read-on and complete the derivative classification training is provided by the facility security officer. Specific requirements provided in the Department of Defense Contract Security Classification Specification, DD Form 254.

Contractors performing tasks at the TS or below level without SCI access shall only receive the North Atlantic Treaty Organization (NATO) awareness brief and complete the derivative classification training prior to being granted access to SIPRnet. The facility security officer provides training. Specific requirements provided in the Department of Defense Contract Security Classification Specification, DD Form 254.

The National Industrial Security Program Operating Manual (NISPOM) 32 CFR NISPOM Rule 117.8 implements contractor reporting requirements per SEAD 3. Contractors are required to report certain events such as those that have an impact on: 1) the status of the facility clearance (FCL), 2) the status of an employee's personnel clearance (PCL); may indicate the employee poses an insider threat the proper, 3) the proper safeguarding of classified information, and 4) or an indication that classified information has been lost or compromised. Contractors working under NIWC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Defense Counterintelligence and Security Agency (DCSA) Trust Decision (Adjudications), (TDA) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under NIWC Pacific contracts.

Anti-Terrorism/force Protection **(AT/FP)** briefings are required to be completed annually for all personnel

(military, DOD civilian, and contractor). The briefing is available at Joint Knowledge Online (JKO): https://jkodirect.jten.mil (prefix): JS; course number: US007; title: Level 1 Anti-terrorism awareness training, if experiencing problems accessing this website contact the JKO Help Desk (24 hours a day/7 days a week, js.jko.helpdesk@mail.mil, 757-203-5654). The website will allow contractors who do not have a CAC to access the training. This training can also be found on the Total Workforce Management Services (TWMS) site: https://twms.dc3n.navy.mil/selfservice/. note: contractor employees must receive the AT/FP briefing annually when Commanders have granted access to their installations or separate facilities per in DoDI O-2000.16 Volume 1.

6.1 Operations Security (OPSEC).
OPSEC is a six-step continuous analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; apply countermeasures; and periodic assessment of effectiveness). Critical information is any specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. Critical information does not necessarily mean CI, but includes all CI, CUI, and certain aggregations of information that meet the definition of critical information. Examples of critical information include research and development information, proprietary operational information, personal identifiable information, and financial information associated with U.S. national security related programs and activities. All personnel working under this task may at some time handle, produce or process critical information or Critical Program Information (CPI), and therefore both Collaborators must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD 254.

Questions regarding the handling of CUI with regard to the support or performance of this Agreement may be directed to the Naval Information Warfare Systems Command (NAVWAR)/NIWC Pacific, OPSEC Manager, Code 87200.

Security programs are oriented towards protection of CI and classified material. OPSEC is an operations function, which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E, SECNAVINST 3070.2A, NAVWARINST 3432.1, Navy Tactics, Techniques, and Procedures (NTTP) Operations Security (OPSEC) Manual, the National Security Decision Directive (NSDD) Number 298, and NAVWAR/NIWC Atlantic/NIWC Pacific's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual. Note: OPSEC requirements are applicable when contract personnel handle, produce or process critical information, have access to CI, unclassified CPI, CUI, or Department of Navy (DON) networks. CDSE OPSEC Course: https://securityawareness.dcsa.mil/opsec/index.htm.

6.2 Information Security
Pursuant to DoDM 5200.01 and DoDI 5200.48, the contractor shall provide adequate security for all Controlled Unclassified Information (CUI) and Unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. If the contractor originates, adds to, or changes any of the DoD information, it must be marked in accordance with DODI 5200.48 and handled properly. The contractor shall disseminate CUI and unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking). CUI Category descriptions are located: https://www.dodcui.mil/Home/DoD-CUI-Registry/.

6.3 Contractor Requirements for Intelligence Oversight
In compliance with DoDD 5148.13 paragraph 4.1.e and SECNAVINST 3820.3F, all contractor personnel conducting Intelligence or Intelligence-related activities or supporting those efforts under Department of

Defense authorities shall report any Questionable Intelligence Activity (QIA) or Significant or Highly Sensitive Matter (S/HSM) to the Naval Information Warfare Systems Command Intelligence Oversight Program Manager or Senior Intelligence Officer.

6.3.1 Questionable Intelligence Activity (QIA):
Any Intelligence or Intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

6.3.2 Significant or Highly Sensitive Matter (S/HSM):
An Intelligence or Intelligence-related activity (regardless of whether the Intelligence or Intelligence-related activity is unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by Intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of Intelligence activities. Such matters might involve actual or potential:

- Congressional inquiries or investigations.
- Adverse media coverage.
- Impact on foreign relations or foreign partners.
- Systemic compromise, loss, or unauthorized disclosure of protected information.

7.0 DELIVERABLES

The contractor shall provide data deliverables in accordance with (IAW) the Contract Data Requirements List (CDRL). The contractor shall deliver any source code developed, along with end-user documentation IAW CDRL, as applicable. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs generated under each task. The contractor shall not develop any CDRL classified TOP SECRET with SCI.

8.0 PERFORMANCE CRITERIA

Not applicable.