PERFORMANCE WORK STATEMENT

Performance Work Statement

Contractor:

1.0 NATURE AND SCOPE OF THE ACQUISITION

1.1 Description of the Effort

The AN/TPS-80, Ground/Air Task Oriented Radar (G/ATOR) system, herein after referred to in this document as G/ATOR, provides capabilities in the Air Defense/Surveillance Radar (AD/SR) and Ground Weapons Locating Radar (GWLR) variants. This Performance Work Statement (PWS) is in support of the G/ATOR Secondary Reparable (SECREP) requirements to repair, test and return to service, provide engineering, failure data analysis and logistics support services.

1.2 Scope

This PWS establishes requirements, sets forth tasks, and identifies work efforts that shall be performed to repair G/ATOR SECREPs to a serviceable condition. More specifically, this PWS establishes requirements, set forth tasks, and identifies work efforts that shall be performed in support of:

1. SECREP Repairs
2. Data Analysis and Collection;
3. Engineering Services;
4. Authorization to Operate (ATO) Maintenance and Cyber Security Support;

2.0 APPLICABLE DOCUMENTS

2.1 Applicable to all Contract Line Item Numbers

2.1.1 General

The following regulations and documents form a part of this PWS to the extent specified herein. In the event of conflict between the documents referenced and this PWS, the PWS shall take precedence. Nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained. Unless otherwise stated, the following documents may be obtained from the Defense Logistics Agency (DLA) Document Services, Building 4/D, 700 Robbins Avenue, Philadelphia, PA 19111-5094 or visit https://assist.dla.mil/online/start/index.cfm.

The following documents, although not specifically identified in the PWS Section 3, shall be applied across all elements of the PWS.

Federal Acquisition Regulation (FAR) Sub part 42.501		Post award Orientation
48 CFR Part 207.106 Defense Federal Acquisition Regulation (DFAR) Supplement		Preservation of Tooling for Major Defense Acquisition Programs
Department of Defense (DoD) 5000.02T	07 April 2022	Operation of the Defense Acquisition System
G/ATOR SCG ID# 11-079.09	17 January 2023	Security Classification Guide for the Ground/Air Task Oriented Radar (G/ATOR)

2.1.2 Government and Non-Government Documents Mandatory Compliance

The following documents referenced in the PWS paragraphs shall apply and are Mandatory:

ISL 2021-02	12 August 2021	National Industrial Security Program Operating Manual (NISPOM).
Department of Defense Instruction (DoDI) 4160.28	01 December 2017	Defense Demilitarization: Demilitarization Coding Operation of the Adaptive Acquisition Framework
DoDI 5000.02	23 January 2020	
Department of Defense Manual (DoDM) 5200.01, Vol 1	28 July 2020	DoD Information Security Program: Overview, Classification, and Declassification Incorporating Change 1
DoDM 5200.01, Vol 2	28 July 2020	DoD Information Security Program: Marking Information, Incorporating Change 3

DoDM 5200.01, Vol 3	28 July 2020	DoD Information Security Program: Protection of Classified Information, Incorporating Change 2
DoDM 5200.01, Vol 4	09 May 2018	DoD Information Security Program: Controlled Unclassified Information (CUI), Incorporating Change 1
DoDI 5230.24	15 October 2018	Distribution Statements on Technical Documents, Incorporating Change 3
	07 October 2019	Cybersecurity Change 1
DoDI 8500.01		
DoDI 8530.01	25 July 2017	Cybersecurity Activities Support to DoD Information Network Operations, Incorporating Change 1
Department of Defense Directive (DoDD) 8140.01	05 October 2022	Cyberspace Workforce Management, Incorporating Change 1
DoDI 8510.01	29 December 2020	Risk Management Framework (RMF) for DoD Information Technology (IT), Incorporating Change 3
DoDI 8580.1	09 July 2004	Information Assurance (IA) in the Defense Acquisition System
DoD 8570.01-M	10 November 2015	Information Assurance Workforce Improvement Program, Incorporating Change 4
DoD 5000.04-	07 May 2021	Cost and Software Data Reporting (CSDR)
DoD 4140.01 Volume 1	13 December 2018	DoD Supply Chain Materiel Management Procedures: Operational Requirements
DoD 4160.21	02 October 2019	Defense Materiel Disposition: Disposal Guidance and Procedures

Volume 1

DODD 4151.18	31 August 2018	Maintenance of Military Materiel, Incorporating Change 1
Marine Corps Order (MCO) 4130.2	30 July 2019	Updating and Reporting Software Configuration For Fleet Maintained Systems and Equipment
MCO 4855.10C	26 January 2015	Product Quality Deficiency Report (PQDR) Program
MCSCO 5530.2A 2018	06 December 2018	Access Control Order
Systems Engineering, Interoperability, Architecture and Technology Handbook (SIAT-HDBK)-003	25 February 2014	Configuration Management Implementation Handbook
Military Handbook (MIL-HDBK)-61B	07 April 2020	DOD Handbook, Configuration Management Guidance
Military Standard (MIL-STD)-3100B	31 October 2018	DOD Standard Practice, Technical Data Packages
Military Detain (MIL-DTL)-28999C (MC)	06 February 2001	Detailed Specification, Publications, Technical, Instruction Type: Preparation of Security and Privacy Controls for Federal Information Systems and Organizations
Committee on National Security Systems Instruction (CNSSI) 1253	29 July 2022	Categorization and Control Selection for National Security Systems

NIST Special Publication (SP) 800-53 Revision 4	April 2013, Updated 22	Security and Privacy Controls for Federal Information Systems and Organizations
SECNAVIST 5239.2	January 2015	DON Cyberspace IT and Cybersecurity Workforce Management and Qualification Manual
SECNAV 5239.3	27 June 2016	Department of the Navy Cybersecurity Manual
	22 April 2022	

2.1.3 Government and Non-Government Documents Guidance

The following documents are referenced in the PWS paragraphs for which they apply and are provided as guidance:

DoD Integrated Product Support Element Guidebook updated December	01 July 2019	Integrated Product Support Element Guidebook
MIL-HDBK-338B	11 May 2012	DoD Handbook Electronic Reliability Design Handbook
DoDM 4140.01-V3	03 December 2017	DoD Supply Chain Materiel Management Procedures: Materiel Sourcing
SD-22	29 June 2016	Diminishing Manufacturing Sources & Material Shortages (DMSMS) Guidebook
MCO P12304.1 CETS Manual	25 October 1993	Contractor Engineering and Technical Services Personal Manual
Army Regulation 700-4	14 December 2011	Logistics Assistance
Marine Corps Warfighting Publication (MCWP) 4-11.4 (Formerly MCWP 4-24), Maintenance Operations	24 April 1998	Maintenance Operations
CMU/SEI-2010-TR-033	November 2010	CMMI® for Development, Version 1.3 (CMMI-DEV, V1.3)

Institute of Electrical and Electronic Engineers	September 2017	System, Software and Hardware Verification and Validation Standard
(IEEE) 1012-2016		
IEEE 12207-2017	November 2017	Systems and Software Engineering—Software Life Cycle Processes
IEEE 15288.1	15 May 2015	Standard for Technical Review and Audits on Defense Programs
Society of Automotive Engineers –Electronic Industries Alliance (SAE-EIA)-649 Rev C	February 2019	Configuration Management Standard
MIL-STD-881C	03 October 2011	Work Breakdown Structures for Defense Materiel Items
IEEE 24748-4	15 May 2016	Systems and software engineering - Life cycle management - Part 4: Systems engineering planning
Committee on National Security Systems Policy (CNSSP) No. 22	January 2012	Policy on Information Assurance Risk Management for National Security Systems.
CNSS Instruction 4009	26 April 2010	National Information Assurance Glossary

Copies of DoD documents are available online at http://quicksearch.dla.mil/or from the DLA Document Services, Bldg. 4/D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.

Application for copies of American Society of Mechanical Engineers (ASME) Y14.100-2013 and ASME Y14.34M should be made to the American Society of Mechanical Engineers at (800) 843-2763 or Infocentral@asme.org.

Application for copies of NAS 411 should be addressed to the Aerospace Industries Association of America, 1250 Eye Street, NW, Suite 1200, Washington, DC 20005-3924 or visit www.aia-aerospace.org.

Application for copies of ANSI documents should be addressed to American National Standard Institute Inc., 25 West 43rd Street, New York, NY, 10036 or visit www.ansi.org.

Application for copies of IEEE standards should be addressed to the Institute of Electrical and Electronics Engineers, PO Box 1331, 445 Hoes Lane, Piscataway, NJ 08855-1331 or visit www.ieee.org.

ASE documents may be obtained from www.sae.org or SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001

2.1.4 Forms

DD Form 1586	August 1996	Contract Funds Status Report
DD Form 254	April 2018	DoD Contract Security Classification Specification
DD Form 2794	April 2007	Cost and Software Data Reporting (CSDR) Plan

Copies of DD forms are available online at: http://www.dtic.mil/whs/directives/infomgt/forms.

3.0 REQUIREMENTS

3.1 Sustaining Engineering and Logistics Support Program Management

The Contractor shall manage the Sustaining Engineering and Logistics Support Indefinite Delivery-Indefinite Quantity (IDIQ) Contract and the associated task orders in accordance with the requirements of Paragraph 3.1 and its subparagraphs. The Contractor shall manage the individual task orders in accordance with Paragraph 3.1 as tailored to meet the specific requirements of the task order.

3.1.1 Assignment of Responsibility and Authority

The Contractor shall designate a primary representative to represent the Government for the Task Orders. The Contractor's representative shall be responsible for organizing, planning, scheduling, implementing, controlling, analyzing, and reporting on all elements of the task orders. The Contractor shall provide the resources necessary for successful execution of the task orders. Additionally, the Contractor's representative shall be cognizant of all activities and shall be prepared to present and discuss the status of task orders and associated issues with the LOGCOM Representative, the Contracting Officer and the Contracting Officer's Representative (COR). The Contractor's representative shall coordinate all conferences and meetings with the Government.

3.1.2 Task Planning and Schedule

The Contractor shall use a structured approach in planning and scheduling. The Contractor shall plan the execution of each task order tailored to the unique characteristics of the task order requirements. The Contractor shall plan and schedule each task order execution by identifying discreet measurable tasks with start and finish dates for each task, the resources assigned, deliverable development, quality assurance, and review time with key technical and program review of milestones, and deliverable development that provides effective monitoring and control.

3.1.3 Organization

The Contractor shall provide and assign personnel with the commensurate repair, analytical, maintenance, operational, and technical skills to perform the requirements of the task order and to complete the required assignments to meet the performance objectives at the established cost.

3.1.4 System Security

The use and distribution of classified material is anticipated under this effort. All classified material shall be handled, stored, and destroyed in accordance with the DoD Directive 5220.22-M.

3.1.4.1 Security Requirements

This contract will require the Contractor to have a Secret Facility Clearance and will require certain contractors to obtain and maintain classified access eligibility. The Contractor shall have a valid Secret Facility Clearance and a Secret Safeguarding Level prior to classified performance at the Contractor's facility. The prime Contractor and all sub-contractors (through the prime Contractor) shall adhere to all aspects of 32 CFR Part 117 NISPOM. All personnel identified to perform on this contract shall maintain compliance with Department of Defense, Department of the Navy, and Marine Corps Information and Personnel Security Policy to include completed background investigations (as required) prior to classified performance. The Facility Security Officer (FSO) is however required to establish, populate, and own the DISS record of every Contractor processed for and/or issued a Common Access Card (CAC). This contract shall include a DoD Contract Security Classification Specification (DD-254) as an attachment.

In accordance with DoDI 5200.48 - Controlled Unclassified Information (CUI), all contractors supporting Marine Corps Logistics Command (MARCORLOGCOM) who receive, store, or generate CUI are required to take the DoD Mandatory CUI Training, available on the Security Awareness Hub at: https://securityawareness.usalearning.gov/cui/index.html. Per DoDI 5200.48 and pursuant to contractual requirements, DoD contractors require initial CUI training and annual CUI refresher training. Additional MARCORLOGCOM specific CUI training and guidance can be attained by contacting the MARCORLOGCOM Security Manager Information & Personnel Security Program Office at 229-639-5155/5155 or smb_logcom_sec_mgr@usmc.mil.

While performing aboard NAVY/USMC sites, the Contractor shall comply with the provisions of DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," SECNAVINST 3070.2A, "Operations Security," MCSCO 3070.1B, "Operations Security Program," Marine Corps Order 3070.2A, "The Marine Corps Operations Security (OPSEC) Program," and the MARCORSYSCOMO P5510.2C, "Security Manual," at all other sites the Contractor shall comply with the local command and/or program OPSEC plan. 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 Subcontractors) shall supplement their current security practices by requiring any personnel involved in executing this contract to complete Government-sponsored and administered OPSEC training.

3.1.4.1.1 System Security Plan and Plan of Action and Milestones Reviews

Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s)) for its covered Contractor information system(s) available for review by the Government at the Contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting, which is included in this contract. The Contractor shall fully cooperate in the Government's review of the SSPs at the Contractor's facility. If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS 252.204-7012, then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The contracting officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a Plan of Action and Milestones (POA&M) for the correction of the identified deficiencies. The Contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POA&M.

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

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

3.1.4.1.2 Compliance to National Institute of Standards and Technology (NIST) 800-171'

- The Contractor shall fully implement the CUI Security Requirements and associated Relevant Security Controls in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish an SSP(s) and POA&Ms that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered Contractor information systems affecting this contract.

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

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

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

- Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods;
- Audit user privileges on at least an annual basis;
- Implement:
  - i Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e., FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POA&M); and,
  - ii NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program);
- Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POA&M for implementation, which shall be evaluated by the Navy for risk acceptance;
- Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation, which can be evaluated by the Government Program Manager for risk to the program.

3.1.4.1.3 Cyber Incident Response

- The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.
- Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx. In delivery of the incident data, the Contractor shall, to the extent practical, remove Contractor-owned information from Government covered defense information.
- If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

3.1.4.1.4 Naval Criminal Investigative Service Outreach

The Contractor shall engage with Naval Criminal Investigative Service (NCIS) industry outreach efforts and consider recommendations for hardening of covered Contractor information systems affecting Department of Navy (DoN) programs and technologies.

3.1.4.1.5 NCIS/Industry Monitoring

In the event of a cyber-incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the NCIS, which may include cooperation related to: threat indicators; pre-determined incident information derived from the Contractor's infrastructure systems; and the continuous provision of all Contractor, subcontractor or vendor logs that show network activity, including any additional logs the Contractor subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

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

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

3.1.4.3 Defense Biometric Identification Card

Certain Contractor personnel may require the issuance of a Defense Biometric Identification (DBID) card to gain access to Marine Corps and/or Army bases/stations. The COR will identify and approve only those Contractor employees performing on this contract that require a DBID card to perform their job function aboard the base. All Contractor personnel requiring access to Government facilities shall comply with applicable Marine Corps installation access control policies, including MCO 5530.13, *Marine Corps Site Perimeter Access Control*, and all applicable installation access procedures governing enrollment in DBIDS.

.Conferences, Meetings, Formal Reviews and Audits

3.1.5.1 Agendas, Minutes and Status Reports

The Contractor shall plan, host, attend, coordinate, support and conduct meetings, formal reviews, conferences, and audits (hereinafter called "reviews") in conjunction with the Government. The reviews shall be conducted at Contractor, Online, and/or Government facilities. The Contractor shall prepare and deliver agendas for Government approval. The Contractor shall prepare presentation materials and deliver minutes and reports following each review. The Contractor shall document all action items, assign responsibility for completion, and determine due dates prior to adjournment of all reviews. The Contractor shall deliver a summary of all action items, responsible parties, and estimated due dates with the Minutes as designated in each task order. The summary shall identify the responsible party and estimated due date for each action item.

The Government reserves the right to cancel any review or to require any review to be scheduled at critical points during the period of performance (PoP). Action item documentation, assignment of responsibility for completion and due dates shall be determined prior to adjournment of all reviews.

A002 DI-ADMN-81249C, Conference Agenda A003 DI-ADMN-81250C, Conference Minutes

B001 DI-MISC-80508B, Technical Report Study/Services, Presentation Materials

3.1.6.2 Program Management Review and Task Order Review

The Contractor shall conduct Program Management Reviews (PMRs) to review the overall status of the task order. The Contractor shall focus the PMR on business and contractual issues to include how efficiently the task order is working, potential process improvements, costs, staffing, contractual issues, resources and task order status to include the number of task orders under contract and the number in process. The Contractor shall plan, host, attend, coordinate, and support PMR in accordance with a schedule mutually agreed to between the Government and the Contractor on dates and locations or by other means (e.g., teleconference) mutually agreed upon.

The Contractor shall conduct Task Order Reviews (TORs) to address the progress of the task order execution, technical problems encountered, and solutions to maintain schedule. The Contractor shall plan, host, attend, coordinate, and support TORs in accordance with a schedule mutually agreed to between the Government and the Contractor on dates and locations or by other means (e.g., teleconference) mutually agreed upon. For both the PMRs and the TORs, the Contractor shall develop an agenda for each review. The Contractor shall prepare presentation materials providing an overview of all agenda items. The Contractor shall provide and deliver an agenda and written minutes for each PMR and TOR. The Government reserves the right to cancel any review or to require any review to be scheduled at critical points during the period of performance. The Contractor shall document all action items, assign responsibility for completion, and determine due dates prior to adjournment of all reviews.

A002 DI-ADMN-81249C, Conference Agenda A003 DI-ADMN-81250C, Conference Minutes

B001 DI-MISC-80508B, Technical Report Study/Services, Presentation Materials

3.1.6.3 Status Reports

The Contractor shall deliver a monthly status report using a Government compatible Microsoft software suite that identifies the status of each task order against the initial task order plan. At a minimum, this report shall include task planning schedule, schedule with milestones, issues, risks and opportunities identification, and monthly expenditures.

A001 DI-MGMT-80368A, Contractor's Management and Status Report

3.1.7 Data Management

The Contractor shall maintain an electronic repository containing data used to produce and manage products for this contract. The repository shall be accessible and available to the Government to retrieve contract deliverables.

3.1.8 Contractor Performance Measurement

3.1.8.1 Cost Control and Accounting

The Contractor shall maintain and use, in the execution of the task order an accounting methodology which ensures compliance with DoD 5000.2-R to the extent applicable to provide the following:

3.1.8.1.1 Contractor Cost Reporting

The Contractor shall deliver cost, performance and schedule information for the effort set forth in this PWS during scheduled reviews and shall submit the DD Form 1586 Contract Funds Status Reports (CFSR**s)** to update and forecast the task order funding requirements. The Contractor shall systematically collect and report actual IDIQ and the associated task order costs for estimating future costs.

The Contractor shall report Contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the United States Marine Corps via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

W, Lease/Rental of Equipment; X, Lease/Rental of Facilities;

Y, Construction of Structures and Facilities;

D, Automatic Data Processing and Telecommunications, IT and Telecom-Telecommunications Transmission (D304) and Internet (D322) ONLY;

S, Utilities ONLY; and

V, Freight and Shipping ONLY.

The Contractor is required to completely fill in all required data fields using the following web address: www.sam.gov.

Reporting inputs shall be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at www.sam.gov.

A004 DI-MGMT-81468, Contract Funds Status Report

3.1.9 Post-Award Orientation Meeting

The Contractor shall conduct a Post-Award Conference (PAC) for the initial Task Order awarded under this contract during the applicable fiscal year, in accordance with FAR 42.501. The PAC shall be held within sixty (60) calendar days of Task Order award at a Government-approved location or by virtual means, as mutually agreed upon by the Contracting Officer (KO) and the Contractor.

The purpose of the PAC is to establish a common understanding of Task Order requirements, review contract management and execution procedures, confirm roles and responsibilities, identify key management and technical personnel, establish near-term milestones and critical

review dates, and discuss performance, reporting, communication, quality assurance and risk management processes.

The Contractor shall provide the following deliverables in accordance with the Contract Data Requirements List (CDRL):

- A002 DI-ADMN-81249C, Conference Agenda
- A003 DI-ADMN-81250C, Conference Minutes
- B001 DI-MISC-80508B, Technical Report Study/Services, Presentation Materials

3.1.10 Government-Furnished Property (GFP)

Renewed emphasis is being placed on ensuring all GFP in contractor custody is properly accounted for, reported and maintained in accordance with current DoD policy.

Effective 22 January 2024, DFARS Clause 252.245-7005, **Management and Reporting of Government Property**, consolidated and replaced the following legacy clauses:

- DFARS 252.211-7007, Reporting of Government-Furnished Property
- DFARS 252.245-7001, Tagging, Labeling, and Marking of Government-Furnished Property
- DFARS 252.245-7002, Reporting Loss of Government Property
- DFARS 252.245-7004, Reporting, Reutilization, and Disposal

The consolidated clause streamlines and clarifies contractor responsibilities when Government property is in contractor custody and requires reporting through the GFP Module. 100% Transfer of GFP using the GFP module on the Procurement Integrates Enterprise Environment (PIEE) within two (2) business days of the transfer date from the Government per Contract year. Key requirements include, but are not limited to:

- Reporting receipt, shipment, transfer, and disposition transactions through the GFP Module.
- Reporting both serially managed and non-serially managed GFP.
- Maintaining accountability of embedded serially managed components.
- Complying with Item Unique Identification (IUID) requirements, where applicable.
- Maintaining auditable records supporting GFP accountability throughout the asset lifecycle.
- Prompt reporting of GFP transfers, movements, losses, or discrepancies.

Contractor leadership shall review current GFP processes and validate compliance across all locations supporting Contract XXX (TBD). Site managers are responsible for ensuring personnel involved in receiving, shipping, inventory management, maintenance and property accountability understand and execute GFP reporting requirements.

Failure to maintain accurate GFP accountability and reporting may result in audit findings, property accountability discrepancies, contract compliance issues, and increased Government oversight.

Additional guidance and reporting expectations will be provided as necessary. Contractors should identify any known GFP reporting deficiencies, system limitations or process gaps requiring Government assistance as soon as possible.

3.2 Services for Governmental Support Activities and Fleet Marine Forces

The Contractor shall provide systems engineering and logistics support for in-service G/ATOR SECREPs in the Fleet Marine Forces (FMF) environments to ensure continued operation and maintenance of the G/ATOR SECREPs with managed risk. The Contractor's efforts shall focus on minimizing the downtime of the G/ATOR SECREP with outcomes that can encompass recommendations for weapon system design changes and modification to the integrated product support package that enhances operational readiness and reduces maintenance workload.

The Contractor shall provide support to Government activities transitioning to organic G/ATOR support to Tobyhanna Army Depot (TYAD), but not limited to, Naval Surface Warfare Center, Port Hueneme Division (NSWC PHD Virginia Beach). The Contractor shall provide access to their repair, test, engineering and technical data and provide technical assistance to the Government and its vendors.

The Contractor efforts under the Contract shall utilize the guidance provided by the DoD Integrated Product Support Element Guidebook updated July 2019.

3.2.1 Sustaining Engineering and Logistics Support

3.2.1.1 Product Quality Deficiency Report and System Problem Reports

The Contractor shall provide systems engineering and logistics support for G/ATOR SECREPs delivered to and operated by the MARCORLOGCOM, Tobyhanna Army Depot, and FMF. Deficiencies relating to operation of the G/ATOR SECREP are reported via Product Quality Deficiency Reports (PQDRs) or System Problem Reports (SPRs).

3.2.1.1.1 Product Quality Deficiency Report

Deficiencies experienced relating to the operation of the G/ATOR SECREP are reported via PQDRs in accordance with MCO 4855.10C, 23 December 2014. When provided a PQDR, the Contractor shall conduct analysis, investigate the cause, and identify recommended corrective actions. The Contractor shall analyze PQDRs identified by the Government. The Contractor shall, in the analysis of PQDRs, utilize the procedures of MIL-HDBK-338B and the general guidance of IEEE 1012-2012 to provide a uniform method of determining and documenting failures, root causes, and corrective actions. The Contractor shall provide and deliver for each PQDR, selected by the Government for analysis, a PQDR Corrective Action Recommendation, level of effort, and a status report of all PQDRs analyzed. The recommended corrective action will be evaluated by the Government. If the Government determines that it is in the best interest of the Government to pursue the recommended solution, the Government may request the preparation of an ECP.

B002 DI-MISC-80508B, Product Quality Deficiency Report (PQDR)

3.2.1.1.2 System Problem Reports

Reserved

3.2.1.1.3 System Problem Reports

Reserved

3.2.1.2 Safety

3.2.1.2.1 System Safety Program

The Contractor shall execute a System Safety Program to identify all safety features of the hardware, software, and system design and to continue to identify and assess procedural, hardware and software related hazards that may be present in the system. The Contractor shall identify hazards and, in negotiations with the Government, either transfer, mitigate or accept the risks. In the event that risks are accepted, the Contractor shall develop and follow specific procedures and precautions. The Contractor shall ensure that all subcontractors meet the system safety goals in the System Safety Management Plan (SSMP). In addition, the Contractor shall identify and make recommendations applicable to hazards at the interface of the G/ATOR with other system(s).

3.2.1.2.1.1 System Safety Working Group

Reserved

3.2.1.2.1.2 Safety Review of Engineering Changes

In the event a PQDR is submitted as a Category I (critical defect that could cause death, injury, severe occupational illness, major damage to a weapon system, loss of combat readiness, or depot production-line stoppage), the PQDR shall be dispositioned in accordance with MCO 4855.10C. As part of the dispositioning of Category I PDQRs, the Contractor shall analyze the hazardous aspect of the PQDR and recommend implementation of mitigating measures to prevent or reduce operational hazards or mishaps, avoid loss of life or serious injury to personnel; prevent damage to facilities or equipment; and eliminate adverse impacts on operational and mission capability.

3.2.1.2.2 Hazardous Materials

The Contractor shall monitor any new or modified parts or material used in the system and perform an analysis to identify any materials determined to be hazardous. The Contractor shall deliver to the Government the hazardous material analysis and updated Safety Data Sheets (SDS) as required by OSHA Hazard Communication Standard code of Federal Regulations 29 CFR 1910.1200. The SDSs shall also be packaged and delivered with each system so that the using Unit will be informed.

3.2.1.2.2.1 Incident/Accident Notification/Investigations

The Contractor shall provide safety expertise to support Government conducted safety assessments and to support accident investigations involving G/ATOR SECREPs. The Contractor shall comply with DoDI 6055.07 any time the system is under their supervision. The Contractor shall immediately notify a Government representative when aware of any major accident/incident (including fire) resulting in any one or more of the following: (1) one or more fatalities or two or more disabling injuries; (2) damage of government property affecting program planning or production schedules; (3) degradation of the safety of equipment under contract, such that personnel injury or property damage may be involved; and (4) identification of a potential hazard requiring corrective action; (5) any changes to safety systems or devices; (6) unintended activation of safety system or device; and/or (7) unanticipated failure of a safety system or device.

3.2.1.3 Failure Reporting, Analysis and Corrective Action System

The Contractor shall continue managing the current G/ATOR Failure Reporting, Analysis and Corrective Action Report (FRACAS) process to provide a uniform method of determining and documenting failures, root causes and corrective actions taken for all hardware and software failures occurring in fielded systems as reported by PQDRs (SF368), SPRs, and/or Trouble Tickets. These failures shall be monitored for trends, trend failures and shall be reported. Trends are defined as three failures with the same cause. These failures will be added to the current FRACAS process. The Contractor shall notify the Government within 24 hours of any critical failure (i.e., one that prevents the system from performing its mission). The Contractor shall notify the Government of all non-critical failures within 10 working days of the occurrence. The Contractor shall notify the Government by submission of a separate FRACAS report for each failure event and PQDR, SPRs, and/or Trouble Tickets received.

The Contractor shall also prepare and deliver a quarterly Failure Summary and Analysis Report to the Government identifying any failure impacting cost, schedule, producibility, supportability, cost of ownership, or interface/performance. This report is a summary of all FACARs submitted since the last summary report. The Contractor shall assess the failure data for the identification of trends and identify those trends in the Failure Summary and Analysis Report. Each Failure Summary and Analysis Report shall identify: the root cause, degradation in reliability, , and the remedial actions taken (including parts replaced). Use MIL-HDBK-338B as a guide.

B00L DI-SESS-80255B, Failure Summary and Analysis Report

B003 DI-SESS-81927, Failure Analysis and Corrective Action Report

3.2.1.4 Monitoring of Diminishing Manufacturing Sources and Material Shortages (DMSMS)/Tech Refresh, and other Replacement Monitoring

The Contractor shall identify DMSMS issues that may result in the loss or impending loss of manufacturers of items or suppliers of items or raw materials that may cause material shortages that endanger a SECREPS's or part's development, production, or post-production support capability. When notification or information concerning a DMSMS issue is received from the manufacturer, the Contractor shall analyze its impact, investigate alternatives, validate solutions, and recommend solutions to the Government. The Contractor shall, as part of the analysis, identify the way the DMSMS part or software will be supported following the loss of the support by

the DMSMS part manufacturer. The Contractor shall notify MARCORLOGCOM Representative, the Administrative Contracting Officer and the Procurement Contracting Officer (PCO) in writing whenever the Contractor believes that one or more of the components or materials in any G/ATOR SECREP is a DMSMS component. The notice shall identify the manufacturer, part number, national stock number if applicable, nomenclature and application of each DMSMS component.

The Contractor shall maintain a database containing DMSMS notifications, alternatives, and recommended solutions. The Contractor shall ensure the database is available to the Government. The Contractor shall survey subcontractors and vendors on a quarterly basis to obtain updated status and projected life of vendor and commercial-off-the-shelf (COTS) products.

B004 DI-MISC-80508B, Technical Report Study/Services – DMSMS Vendor Survey

3.2.2 Repairs of G/ATOR Secondary Repairables, and Test Systems

The Contractor shall maintain a repair capability sufficient to support the repair required to return failed SECREP as appropriate to its performance requirements. The Contractor shall additionally repair, as directed, complete G/ATOR SECREPs that have been accepted by the Government but not yet delivered to the warfighters.

The Contractor shall, when in receipt of GFP, comply with PWS paragraph 3.1.10, FAR 52.245-1, and Section I of the Contract. The Contractor shall repair each failed SECREP and ensure the item is brought to Condition Code A in accordance with the Acceptance Test Procedures (ATP) requirements documented in the Technical Data Package. The Contractor shall ship repaired SECREPs to Marine Corps Logistics Command (MARCORLOGCOM), or per MARCORLOGCOM instructions, to a location within Continental United States (CONUS). The Contractor shall provide fully functional SECREPs to replace failed SECREPs with an objective of a ninety (90) calendar day Turn Around Time and a best effort Turn Around Time threshold of one hundred and eighty (180) calendar days. The Repair Turn Around Time is defined as the time starting from when the Contractor receives the failed SECREP until the time the repaired SECREP leaves the Contractor possession. Repaired SECREPs completed earlier than ninety (90) days will be accepted. The Contractor, at the request of the Government, shall submit Lay In Parts recommendation to reduce Repair Turn Around Time (RTAT). When approved for procurement the Contractor shall maintain accountability of Lay In Parts including monitoring and reporting impact on RTAT.

The Contractor shall, upon receipt of a failed component, screen the failed component for warranty applicability prior to shipping to a vendor for repair or replacement. If the warranty is applicable, the Contractor shall process failed components under the warranty in all cases where the component is still under a valid warranty with the vendor. The Contractor shall review post repair documentation for failure trends that may constitute a warranty breach and shall notify the Contracting Officer's Representative (COR) upon identification. The Contractor shall produce and deliver the data required for serialized item warranty tracking.

Prior to commencing repair, the Contractor shall, within five (5) business days of receipt of a failed SECREP, begin the induction process to include inspecting, testing, and conducting an economic

analysis to determine the cost of repair. If the cost of inspection, test, and repair is equal to or greater than 75% of the Government's cost to acquire a new item; or if repair of the SECREP will not return the unit to working condition, the Contactor will notify the COR and provide a repair cost estimation that indicates the item is Beyond Economical Repair (BER) and shall request disposition instructions. The Government will have the option to approve the repair of items that exceed the BER threshold. The Contractor shall present this option and request confirmation prior to the disposal of an SECREP that is identified as BER. The Contractor shall dispose of each BER component as instructed by the COR. If the item's cost of repair is less than 65% of the cost to acquire a new item, the Contractor shall repair the SECREP in accordance with the approved component repair procedures.

All shipments must contain proper shipping documentation. Suppliers must attach in a water-resistant envelope to the exterior shipping container a copy of the DD Form 250 or Invoicing, Receipt, Acceptance and Property Transfer report or if authorized by your contract, a commercial packing list, DD Form 1348 provided by the Government or original Document Number. All documents must include at a minimum, Complete Mark For (M/F) information including TCN (when applicable), contract/order number, CLIN, National Stock Number (NSN), Part Number, Shipment Number, Condition code, quantity, and Unit of Issue. Omission of any data on your shipping documentation will cause a delay in receipt of goods and significantly delay payment.

B00H DI-MISC-80508B, Technical Report Study/Services – Record of SECREPs Received, SECREPs Repaired and Costs of Each Repair

B00U DI-MISC-80508B, Technical Report Study/Services – Warranty Tracking Report

3.2.2.1 Repair and Maintenance of Test Systems

The Contractor shall maintain a repair capability and repair Government provided Test benches, Test Systems electronics, mechanical equipment, fixtures that are utilized in the design, development, manufacture, and production of the G/ATOR SECREP, subsystem, components, subcomponents and parts.

3.2.2.2 Repairs of Secondary Repairables (LOGCOM)

The Contractor shall maintain a repair capability sufficient to support the repair required to return failed Secondary Repairable (SECREP) identified in Section J Attachment, "LOGCOM Authorized Repair List," that meet the performance requirements, utilizing LOGCOM funding. The Contractor shall repair each failed SECREP and ensure the item is brought to Condition Code A in accordance with the ATP requirements documented in the Technical Data Package.

Prior to commencing repair, the Contractor shall, within five (5) business days of receipt of a failed SECREP, begin the induction process to include inspecting, testing, and conducting an economic analysis to determine the cost of repair. If the cost of inspection, test, and repair is equal to or greater than 75% of the Government's cost to acquire a new item; or if repair of the SECREP will not return the unit to working condition, the Contractor shall notify the COR and provide a repair cost estimation that indicates the item is Beyond Economical Repair (BER) and shall request disposition instructions. The Government will have the option to approve the repair of items that

exceed the BER threshold. The Contractor shall present this option and request confirmation prior to the disposal of an SECREP that is identified as BER. The Contractor shall dispose of each BER component as instructed by the COR. If the item's cost of repair is less than 65% of the cost to acquire a new item, the Contractor shall repair the SECREP in accordance with the approved component repair procedures.

3.2.3 Engineering Services and Support

3.2.3.1 Engineering Changes

3.2.3.1.1 Engineering Change Proposals Preparation

Reserved.

3.2.3.1.2 Engineering Change Proposal Incorporation

The Contractor shall retrofit approved Class I ECPs into Government owned G/ATOR SECREP, deliver spares reflecting the new configuration, and report the installation status of each affected SECREP.

3.2.3.1.3 Diminishing Manufacturing Sources and Material Shortages/Tech Refresh, and other Replacement Incorporations

The Contractor shall, when authorized by the Government via an approved ECP, procure and install the components, subcomponents, parts, firmware and software identified for obsolescence, identified as approaching obsolescence or identified as requiring Tech Refresh. During the replacement item or software selection process, the Contractor shall ensure functional partitioning and physical modularity of G/ATOR SECREPs to facilitate the replacement without impacting other parts of the SECREP. The Contractor shall, during the selection process, encourage third-party vendors' participation. The Contractor shall, when procuring replacement items or software, schedule and integrate the procurement with each repair option where possible. The Contractor shall utilize SD-22 – *Diminishing Manufacturing Sources and Material Shortages (DMSMS)* to the extent it applies to the items identified for obsolescence, or Technical Refresh.

3.2.3.2 Logistics Element Support

3.2.3.2.1 Tech Pub Support (IETM updates)

Reserved.

3.2.3.2.1.1 Technical Data Support

Reserved.

3.2.3.2.1.2 IETM

Reserved.

3.2.3.2.1.3 Validation

Reserved.

3.2.3.2.1.4 Verification

Reserved.

3.2.3.2.1.5 Copyright Release

Reserved.

3.2.3.2.2 Updates to New Equipment Training (NET) and Training Materials

Reserved.

3.2.3.2.3 Trouble Shooting and Fault Isolation beyond Built-in Test

Reserved.

The Contractor shall provide trouble shooting and fault isolation for beyond built-in test (BIT) situations wherein the BIT does not provide the warfighter with the ability to correct problems locally and reduce the number of failed items returned for repair.

3.2.3.2.4 Field Service Representatives for CONUS and OCONUS

Reserved.

3.2.4 Field-Level Maintenance Problem Resolution

Reserved.

3.2.4.1 Over and Above Repair

The Contractor shall consider maintenance and repair actions listed below as over and above requirements and not a requirement of paragraphs 3.2.2 “Repairs that don’t meet normal wear and tear of the Secondary Repairables, in the event the following occurs and Contractor assistance is required, the Government will order and fund the effort required utilizing the task order process.

The Contractor shall conduct repairs of the SECREPs, or components damaged due to maintenance-induced failures occurring during user repairs to installed equipment, or components resulting from user maintenance-induced over-limit power or surge conditions.

The Contractor shall conduct repairs of SECREP structure damaged due to operational events or non-operational events and perform repairs of the damaged SECREP.

The Contractor shall perform repairs due to fire or uncontrollable acts of nature, such as but not limited to windstorms or hurricane damage, hail damage, bird strikes, or lightning strikes.

In the event a damaged SECREP is beyond economical repair, the Contractor shall identify parts recommended for removal from the SECREP, giving consideration to items that are high usage, difficult to procure or have a high associated cost.

The Contractor shall demilitarize and dispose of excess or damaged material in accordance with DoDI 4160.28, DoD 4140.1 and DoD 4160.21.

3.2.4.2 Assistance to Government Activities in Standing up Organic Support

3.2.4.2.1 Far-Field Range Technical Requirements

Reserved.

3.2.4.2.2 Inspect and Repair Only As Needed (IROAN) Support

Reserved.

3.2.4.3 Product Improvement

The Contractor shall provide improvements to the G/ATOR SECREP product baseline in the areas of software enhancement, cybersecurity, technology insertion and directed capabilities, survivability, vulnerability, and protection. As requested, the Contractor shall prepare and submit ECPs in accordance with direction provided in paragraph 3.2.3.1.1. In the event developmental testing is conducted, the Contractor shall utilize FRACAS process separate and distinct from that used for failures occurring in fielded systems. The Contractor shall use the FRACAS process to provide a uniform method of documenting failures, root causes and corrective actions for all hardware/software failures.

3.2.4.3.1 Software Enhancement Support

The Contractor shall provide software enhancement support, to the extent identified in this Task Order and/or approved changes, to develop new software or modify existing software to resolve deficiencies identified in G/ATOR SECREPs delivered to and operated by the FMF.

3.2.4.3.1.1 FY26 SW Maintenance Release

Reserved.**3.2.4.3.1.2 Software Support Activity Support**

The Contractor shall support and assist the Government Software Support Activity (SSA) in software development and support activities to designated SSA. The Contractor shall perform the following efforts including, but not limited to:

a. The Contractor shall provide the Government with access to the System Problem Report (SPR) Jira database to view and write to existing SPRs to make modifications, comment, and add attachments.

b. The Contractor shall deliver the Government with regular visibility and the ability to download artifacts (e.g., JIRA, PAL).

c. The Contractor shall facilitate weekly meetings where technical information is exchanged regarding software development, test, and support activities to the SSA and Saab.

d. The Contractor shall include SSA representatives at the weekly NG SPR adjudication meetings and any other change control board that adjudicates items and issues over

products relevant to RAMS, PHM, and COMMS (RAPHCO) or Operational Command and Control (OCC).

e. The Contractor shall provide technical advice, documentation, and over the shoulder support for software bench set-up and checkout in support of conducting software testing in the SSA lab.

f. The Contractor shall provide assistance troubleshooting hardware, firmware and software configuration settings and network configuration for the RAPHCO and OCC Computer Software Configuration Items (CSCIs).

g. The Contractor shall provide assistance troubleshooting hardware, firmware and software configuration settings, and network configuration for the ITB/Test Benches at SSA.

h. The Contractor shall provide assistance with the establishment of a PCSP development environment in the SSA lab.

i. The Contractor shall provide access to system test benches at NG as needed to support testing of assigned SPRs as needed.

j. The Contractor shall provide technical advice and guidance related to any SPR assigned to the SSA for either investigation or implementation.

k. The Contractor shall facilitate peer reviews of investigations or proposed design proposals performed by SSA personnel for SPRs assigned to the SSA.

l. The Contractor shall deliver to the SSA source code drops monthly or as the SW is changed for the PCSP variant of the GITD according to SSA's CM process.

m. The Contractor shall deliver to the SSA executables drops and associated support/bench tools, monthly or as the SW is changed for the NG maintained CSCIs to support software development.

n. The Contractor shall deliver proposed Interface Design Document (IDD) and Interface Description Language (IDL) updates upon assignment to an SSR to support Enhanced Radar Data Display System (ERDDS) development.

o. The Contractor shall deliver technical advice and assistance setting up cybersecurity per DoDI 8510.01 at the SSA.

p. The Contractor shall include SSA Test Personnel during SSR testing on site at NG.

The Contractor shall provide this support for all applicable CSCIs and shall include support and advisory services from the Subcontractor, and that support shall continue with transition of RAPHCO and OCC CSCIs to the SSA.

3.2.4.3.2 Cybersecurity Support

Reserved.

3.2.4.3.2.1 Cybersecurity

The Contractor shall ensure system cybersecurity program adheres to DoD, DoN, USMC and National Institute of Standards and Technology (NIST) approved cyber security, information assurance (IA) architecture, policies, programs, standards, and guidelines. The Contractor shall implement and maintain a cybersecurity program for the system, subsystems, components and support systems and equipment in accordance with the current DoDI 8500.01, DoDI 8510.01, and DoDI 8580.1.

The Contractor shall identify, manage, and verify cybersecurity requirements in the same manner as all other system requirements. The Contractor shall identify cybersecurity requirements that are security critical and identify and implement corresponding RMF security controls for these requirements. The Contractor shall securely configure the system while maximizing the system functionality and minimizing system cybersecurity risk as described in SECNAV M-5239.1. The Contractor shall ensure that cybersecurity risks are identified and managed as a part of the overall program risk management process. The Contractor shall ensure that the cybersecurity risk management activities are consistent with guidance provided in Committee on National Security Systems Policy (CNSSP) No. 22. The Contractor shall ensure that the cybersecurity risk management activity reexamines threats, exposure, and vulnerabilities and assesses changes to all system architecture and design changes.

The Contractor shall ensure that COTS items are assigned an appropriate evaluation assurance level in accordance with the National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (CCEVS) for Information Technology (IT) Security Common Criteria. The Contractor shall ensure that COTS deliverable items have been certified via the CCEVS; https://www.niap-ccevs.org/. The Contractor shall conduct code scans in support of requests for addition of software to the Supported Products List (SPL) and in support of code changes to new or existing applications.

The Contractor shall document all third-party software used in the system, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed-source. The Contractor shall ensure that third-party software meets the software assurance requirements of the system and that such third-party software components come from trusted sources/suppliers.

B00N DI-MISC-80508B, Technical Report-Study/Services, Third Party Software List

The Contractor shall integrate cybersecurity into systems security engineering. The Contractor shall maintain applicable security controls through the systems engineering technical processes. The Contractor shall recommend changes to cybersecurity controls for the system via systems engineering technical processes. The Contractor shall ensure that all documentation complements the program's cybersecurity program and the system Security Plan (SP).

The Contractor shall ensure that the cybersecurity portions of the overall system design are included in systems engineering and design documents, test plans, procedures, and reports.

The Contractor shall ensure that cybersecurity boundaries (e.g., cryptographic boundary, certification boundary, classification boundary) are clearly and consistently identified in program documents and drawings. The Contractor shall allocate and implement the applicable

cybersecurity controls for the system in accordance with CNSSI No. 1253 and NIST SP 800-53. The top level of Security Requirements is the CNSS-1253 Security Controls. These controls that are selected at the beginning of the system design and are treated as security requirements that all aspects of a system must meet. The Contractor shall ensure and document bi-directional traceability between security controls and requirements.

The Contractor shall complete security requirements analysis, security design, engineering activities, software changes and modifications, security testing, and delivery of all security patch updates, in coordination with minor or major SSRs, with validated installation procedures to maintain or incrementally increase the cybersecurity posture of the system.

All Security patch updates shall be incorporated into and delivered with a System Software Release (SSR) when an SSR is to be fielded.

B00J DI-AVCS-80700 Computer Software Product End Items SSR Security Patch Updates and Installation Instructions

3.2.4.3.2.2 Cybersecurity Assessment and Authorization (A&A) Process Support

The Contractor shall provide expert technical and security services to the Information System Security Manager (ISSM) with the goal of maintaining cybersecurity acquisition milestones and Authority to Operate (ATO) of the system. The Contractor shall ensure that authorization efforts are in accordance with the DoD 8500.01, DoD 8510, FIPS 199, NIST 800-53, CNSSI 1253, and 800-53A, NIST 800-37, and any other required regulations, policies, standards, directives, laws, and Executive Orders. This task shall consist of process support, analysis support, coordination support, security assessment test support, Assessment & Authorization and cybersecurity documentation support, and system verification of implemented security controls and requirements defined in DoDI 8580.1 and DoDI 8500.01. A completed A&A package consists of addressing all applicable security controls to sufficiently provide a completed Implementation Plan, Security Assessment Plan, Continuous Monitoring Plan, System security Plan, and Plan of Action and Milestones (POA&Ms); The Contractor shall include cybersecurity RMF activities and events within the integrated master schedule and/or integrated master plan. The Contractor shall also participate in cybersecurity activities (e.g., Integrated Product Teams, coordination meetings, and Government directed sessions) and document the minutes denoting attendees, summarize discussion results, tasks, and deadlines.

The system has been assessed and authorized under the RMF. The system has been categorized as High/High/High for Confidentiality/Integrity/Availability, with the classified security control overlay being applicable. The Contractor shall be responsible for ensuring that the system meets and maintains compliance criteria for system authorization. The Contractor shall address and resolve (with Government concurrence) confidentiality, integrity, availability, authentication, and non-repudiation issues that may prevent the system from maintaining an ATO/ATC Annual Security Reviews (ASRs) and an independent Security Controls Validation (SVC) will be conducted on the system. The Contractor shall provide support, source data, and analysis required to support the Government in maintaining the system's Authority to Operate/Authority to Connect (ATO/ATC) in accordance with DoDI 8500.01, DoDI 8510.01, DoDI 8580.1, and SECMAV M-5239.1. The

Contractor shall provide a plan, to include timeline, in line with system authorization schedule, to conduct validation assessments to identify cyber security vulnerabilities on assets and information systems.

The Contractor shall verify cybersecurity controls and submit the verification results. The Contractor shall provide an update to the System Security Plan (SSP) and shall support data validation efforts during all steps of the RMF process. The team shall review system documentation (data call, diagram, etc.) prior to test activities, develop the test scope (OS, Security Technical Implementation Guides (STIGs), Ports, Protocols and Services, etc.)

Supporting documentation includes but is not limited to: Hardware/Software Lists and Matrices; Security Requirements Traceability Matrix (SRTM); Data Flow Diagrams; Interconnection and Network Diagram(s); Information Assurance Vulnerability Management (IAVM) Plan; Access Control Policy, Audit and Accountability Policy; Identification and Authentication Policy; Ports, Protocols, and Services Management (PPSM). These documents will be delivered in the format capable of being imported into the Services RMF tool.

B00M DI-MISC-80508B, Technical Report - Study/System Security Plan (SSP) with Appendices Cybersecurity Analysis Support

The Contractor shall perform cybersecurity analysis using DoD-approved tools, processes, and procedures to: maintain and improve, when applicable and as directed by the Government, the cybersecurity baseline; update the System Software Cybersecurity POA&M quarterly; and when necessary, validate changes to established security requirements. The Contractor shall recommend additional security requirements and corrections to eliminate or mitigate any cybersecurity findings. For detected vulnerabilities that could impact accreditation, the Contractor shall recommend (primarily) technical solutions, human procedures, software configuration parameters, system changes, or a combination of potential solutions to mitigate the vulnerability and maximize system functionality while minimizing cybersecurity risk. The Contractor shall analyze, through system level and regression testing, the adequacy of changes to the system and assess residual risk.

The Contractor shall conduct analysis for any COTS and/or non-developmental items (NDI) to ensure that they are appropriately configured, software/hardware/firmware is controlled, and any unique cybersecurity risks they pose are mitigated.

B00K DI-MISC-80508B, Technical Report - Study/Services – Cybersecurity Analysis and Studies for COTS and NDI (as required)

3.2.4.3.2.3 Authority to Operate (ATO) Maintenance/Quarterly Reporting

The is granted Authorization to Operate (ATO) based on the Program's ability to manage risks. Authorization is the official management decision given by the USMC Authorization Official (AO). This official authorizes operation of an IS and explicitly accepts the risk to USMC operations. The Contractor shall support, implement, and adhere to all NIST, Federal, DoD, DISA, and USMC policies, procedures, and standards regarding cyber security and the RMF. The Government does this in part by implementing an agreed upon set of security controls documenting the tasks and necessary resources to resolve SECREP deficiencies. POA&Ms are necessary to keep track of the

milestones that we will pass along the way, to hold ourselves accountable, and to let any auditors or validators know we're serious about correcting our system issues– those milestones should include estimated completion dates. The Contractor's execution of A&A requirements supports the systems adherence to FISMA. FISMA requires G/ATOR to develop, document, and implement a program to provide information security for the system. The NIST SP 800-53 outlines the specifics of Federal standards for building and running information security systems. Staying compliant with FISMA can help to ensure the implementation and maintenance with the relevant RMF guidelines.

3.2.4.3.2.3.1 Quarterly System Software Cybersecurity Plan of Action and Milestones

The Contractor shall update the System Cybersecurity POA&M on a quarterly basis with the results of the Contractor's internal quarterly assessments and results from each System Software Release (SSR). The Contractor shall conduct technical evaluations of systems to provide appropriate cybersecurity requirements and recommendations to their capabilities and potential use within the security program of the system. The Contractor shall conduct scans and evaluate the results from DoD mandated tools (i.e., Assure Compliance Assessment Solution (ACAS), STIGs, Security Content Automation Protocol (SCAP)), and perform manual compliance assessments, along with manual STIG checks. Non-compliant findings shall be documented in the System Cybersecurity POA&M on a minimum quarterly basis. The Contractor shall deliver a quarterly System Software Cybersecurity POA&M to the Government. The System Software Cybersecurity POA&M shall be based on the system's software vulnerability scans of the entire system's software inventory performed by the Contractor and serves as a tool for planning and tracking the resolution of software vulnerabilities (which is always classified when populated with vulnerabilities) The Contractor shall review the POA&Ms for adequacy and recommend status (Started, Recommend Risk Acceptance, Completed) to the Government for upload into the RMF tool. The delivered System Software Cybersecurity POA&M shall not contain unmitigated Category 1(Very High, or High) findings. Mitigated risk level must be moderate or lower. The Contractor shall participate in the IT security auditing of the system by providing remediation and an updated System Cybersecurity POA&M in conjunction with approved software releases. The Contractor shall execute an operationally viable Information Assurance Vulnerability Management (IAVM) program per CJCSI 6510.01F. The Contractor shall monitor and track new Information Assurance Vulnerability Alerts (IAVAs) and Bulletins (IAVBs), Marine Corps Enterprise Network (MCEN) Operational Directives (OPDIRS) and applicable DISA STIGs/Security Requirements Guides (SRGs) applicable to G/ATOR SECREPs. The Contractor shall determine applicability of IAVA/IAVB notices to the system and annotate on the System Cybersecurity POA&M the plan for addressing them.

The Contractor shall deliver the following information in the USMC approved format with each System Cybersecurity POA&M delivery (B00F):

(a) POA&M Automated Generation Engine (PAGE) parser application output;

(b) .nessus and .html files from the Assured Compliance Assessment Solution (ACAS) for each Computer Software Configuration Item CSCI and layer 3 network switches;

(c) .ckl files for each CSCI and layer 3 network switches from the DISA STIG viewer application;

(d) eXtensible Configuration Checklist Description Format (XCCDF) results with .xml files for OCC laptops and server from the Security Content Automation Protocol (SCAP) Compliance Checker (SCC) application;

(e) Security Center Test Reports as identified by the ISSM The Contractor shall prepare and deliver the following:

B00F DI-MISC-80508B Technical Report- Study/Services System Cybersecurity POA&M and Supporting Data (S)

A022 DI-MISC-82190 Quarterly System Software Cybersecurity POA&M

3.2.4.3.2.3.2 Cybersecurity Test and Evaluation Support

The Contractor shall integrate test and evaluation (T&E) of cybersecurity requirements into the overall system T&E process, to include component level testing performed by subcontractors and suppliers.

The Contractor shall provide a cybersecurity Test Plan to include, but not be limited to; Procedures, Bench Diagram, Scan Table, Items to be Scanned, and List of SPRs to be verified. The Contractor shall meet all organizational implementation mission objectives required to ensure the test and evaluation activities and program requirements are addressed and integrated.

The Contractor shall develop, maintain, and improve upon the cybersecurity test plan.

The Contractor shall implement and maintain a cybersecurity testing program as outlined in DoDI 8510.01 using the most current DoD-approved tools. Assessments shall be conducted in accordance with an ISSM-approved test plan and will include pre-test preparations such as documenting the cybersecurity assessment environment. The Contractor shall perform internal security updates on a quarterly basis, conduct a comprehensive cybersecurity assessment of the system in conjunction with each security update, and update the system POA&M. The Contractor shall adhere to the following current versions of Information Assurance Vulnerability Alerts (IAVAs), IAVMs, vendor security patches, STIGs, and Communication Task Orders (CTOs)

The Contractor shall generate change requests to track, manage, and verify vulnerabilities found during the quarterly assessments. The Contractor shall monitor, track, and communicate the remediation results with the government.

The Contractor shall notify and provide the ISSM with all cybersecurity related System Problem Report (SPR) numbers with a plan and timeline for resolution. The Contractor shall resolve cybersecurity System Problem Reports (SPRs) for inclusion in SW Maintenance release in the same manner as other SPRs.

The Contractor shall ensure SSR assessments are scheduled in coordination with the PMO ISSM/ISSO. The Contractor shall provide a cybersecurity Test Report after each cybersecurity assessment indicating all new findings and statuses of SPRs. The Cybersecurity Test Report shall be classified SECRET in accordance with DoDM 5200.01, Volume 3, with Change 2.

The Contractor shall conduct technical evaluations of systems to provide appropriate cyber security requirements and recommendations. Vulnerability scans shall be handled and transmitted in accordance with the system's classification level. Vulnerability reports shall be in a format approved by the ISSM and maintained on SIPRNet.

In accordance with the approved Cybersecurity Test Plan, the Contractor shall scan the G/ATOR system using the DoD approved vulnerability scan engine which is the Assured Compliance Assessment Solution (ACAS) with its latest plugins. The latest plugins and supporting ACAS information are found on the DISA website (https://public.cyber.mil/external-resources/ CAC Login required). The Contractor shall update the ACAS vulnerability scanner with the latest signatures and scanning engines prior to the execution of each vulnerability scan. At a minimum, vulnerability scans shall be conducted against the system, which includes all CSCIs, Operator Control Console (OCC)-M Server, OCC-Laptops, Network assets, IFF, shall be hardened or made compliant using the required and approved STIGs, SRGs, SCAP Benchmarks, and other approved hardening tools. Non-compliant and/or unmitigated STIG, SRG, SCAP Benchmark, and other unmitigated findings shall be documented by the Contractor in the System Software Cybersecurity POA&M on a minimum quarterly basis. Non-compliant findings shall be documented in the System Software Cybersecurity POA&M. Vulnerability scans shall be handled and transmitted in accordance with the system's classification level. Vulnerability reports shall be in a format approved by the ISSM and managed strictly on the classified network.

Updates to the STIGs, SRGs, and SCAP Benchmarks shall be implemented by the Contractor into the system as they are released. STIG, SRG, and SCAP Benchmark artifacts shall be provided in a format approved by the ISSM. STIG, SRG, and SCAP Benchmark artifacts shall be handled in accordance with the G/ATOR system's classification level. Updates to the STIGs, SRGs, and SCAP Benchmarks shall be planned for implementation into the system as they are released and documented with quarterly submissions to the Government. Utilize the SRTM to map system components to STIG requirements. The Contractor is responsible for verifying that the SRTM is accurate based on the currently available STIGs.

The Contractor shall prepare and deliver the following:

B00F DI-MISC-80508B Technical Report- Study/Services System Cybersecurity POA&M and Supporting Data (S)

A022 DI-MISC-82190 Quarterly System Software Cybersecurity POA&M

B00Q DI-MISC-80508B, Technical Report-Study/Services, System Requirements and Vulnerability Management

B00D DI-MGMT-81844 Cybersecurity Test Plan B00E DI-MGMT-81843 Cybersecurity Test Report

3.2.4.3.2.3.2 Quarterly Security Controls Review

Reserved.

3.2.4.3.2.4 Cybersecurity Personnel

Reserved.

3.2.4.3.2.5 System Security Enhancement (SSE) Validation and Verification (V&V) Testing

Reserved.

3.2.4.4 Studies and Analysis

The Contractor shall provide engineering analyses and studies associated with the technical performance of G/ATOR SECREPs, technological opportunities, changes in evolving threat scenarios, process improvements, operational and maintenance performance of fielded systems, and the efficiency of manufacturing, and assembly of G/ATOR SECREPs.

3.2.4.4.1 Systems Engineering Support

Reserved.

3.2.4.4.1.1 Requirements Engineering

Reserved.

3.2.4.4.1.2 Reserved.Specifications

Reserved.

3.2.4.5 Engineering Tests Support

Reserved.

3.2.4.6 Engineering Data for Provisioning

Reserved.

3.2.4.7 Non-Recurring Engineering for Emerging Engineering Requirements/DMSMS Issues

Pursuant to the Government's request, the Contractor shall perform the Non-Recurring Engineering (NRE) required to resolve specific obsolescence / DMSMS issues or to support emerging engineering requirements identified by the Government. The Contractor shall provide a Rough Order of Magnitude (ROM) cost estimate for each effort identified by the Government. The Contractor shall provide a ROM that includes all efforts required to develop, test, and certify the material solution. The Government will review each ROM and then decide whether to approve the proposed NRE. Upon Government approval and funding, the Contractor shall perform the necessary NRE work to resolve the identified problem.

B001 - DI-MISC-80508B, Technical Report Study/Services, Results of Analyses for NRE

Upon completion of the Contractor's NRE assessment, the Government may request that the Contractor coordinate with the G/ATOR PMO to develop and deliver an ECP for possible implementation.

B008 DI-SESS-80639E, Engineering Change Proposal (ECP) B009 DI-SESS-80463E, Engineering Release Record (ERR) B00A DI-IPSC-81442A, Firmware Version Description (FVD)

B00P DI-SESS-81245C Installation Completion Notice