SECTION 1 Background 2
1.A. MSC Role 2
SECTION 2 Scope 2
2.A. Overview 2
2.B. Dry Cargo Time and Voyage Charters 2
SECTION 3 Task Order Proformas 2
3.A. Dry Cargo Time Charter Task Order Proforma 2
3.B. Dry Cargo Voyage Charter Task Order Proforma 2
SECTION 4 Ordering Procedures at the Task Order Level 2
4.A. Request for Quote (RFQ) 3
4.B. Task Order Evaluation 3
4.C. Task Order Evaluation Factor Criteria 3
4.D. Lowest Price Technically Acceptable (LPTA) Evaluation 5
SECTION 5 On-Ramp Of Additional Contractors 6
SECTION 6 Invoicing 6
SECTION 7 Deliverables Schedule 6
7.A. General Vessel Information 6
7.B. Task Order Deliverables 7
SECTION 8 Service Delivery Summary (SDS) 7
8.B. Quality Control, Reporting, and Records 8
SECTION 9 Security (Cyber security, Industrial security, Vendor Threat Mitigation) 9
9.A. Operationally Critical Support 9
9.B. Cybersecurity Incident Reporting 9
9.C. Cybersecurity Incident Reporting Timelines 10
9.D. Mandatory Reporting Data 10
9.E. Incident Reporting Coordination 11
9.F. Confidentiality and Non-Attribution Statement 12
9.G. Cybersecurity Material Model Certification (CMMC) 12
9.H. Industrial Security Information (Applicable Only to Task Orders Involving Classified or Sensitive Cargo) 12
APPENDIX A, GENERAL VESSEL INFORMATION 19

SECTION 1 BACKGROUND

1.A. MSC Role

1.A.1. As the Navy Component Command of the United States Transportation Command (USTRANSCOM), the Military Sealift Command (MSC) provides all strategic and maritime logistics for the Department of War (DoW). MSC operates government-owned and commercial ships to deliver equipment, fuel, and supplies to joint forces worldwide, acting as the maritime arm of USTRANSCOM.

1.A.2. MSC reports to the Navy (U.S. Fleet Forces Command) for administrative purposes, it operates under the combatant command of USTRANSCOM for transportation missions. MSC provides three main types of support to USTRANSCOM: surge sealift (moving unit equipment), prepositioned sealift (keeping supplies at sea), and sustainment sealift (resupplying forces).

SECTION 2 SCOPE

2.A. Overview

2.A.1.1. The Joint Global Sealift Charter (JGSC) contract enables MSC to fulfill its mission by providing strategic sealift to facilitate USTRANSCOM's global movement of large-volume combat forces' rolling stock and associated materials through short-term worldwide time and voyage charters. The Contractor must own or control a Roll-On/Roll-Off (RORO), multi-purpose, or vehicle carrier vessel. Additionally, the Contractor must maintain status as a Voluntary Intermodal Sealift Agreement (VISA) Participant throughout the life of the contract. A VISA Participant is defined as an entity that is a U.S.-flag vessel operator organized under the laws of a State of the United States, or the District of Columbia, that is a signatory party to VISA, including all United States subsidiaries and affiliates of the entity which own, operate, charter or lease ships and intermodal equipment in the regular course of their business and in which the entity holds a controlling interest.

2.B. Dry Cargo Time and Voyage Charters

2.B.1. These charters are short-term agreements supporting USTRANSCOM operations. The Contractor shall provide dry cargo vessels on a time or voyage charter basis to meet mission-specific requirements.

SECTION 3 TASK ORDER PROFORMAS

3.A. Dry Cargo Time Charter Task Order Proforma

3.A.1. The Contractor is required to visit the MSC website at https://www.msc.usff.navy.mil/Business-Opportunities/Contracts/ to obtain the task order proforma for Dry Cargo Time Charters.

3.B. Dry Cargo Voyage Charter Task Order Proforma

3.B.1. The Contractor is required to visit the MSC website at https://www.msc.usff.navy.mil/Business-Opportunities/Contracts/ to obtain the task order proforma for Dry Cargo Voyage Charters.

SECTION 4 ORDERING PROCEDURES AT THE TASK ORDER LEVEL

4.A. Request for Quote (RFQ)

4.A.1. The Government will award a task order resulting from each Request for Quote (RFQ) to the offeror whose technically acceptable proposal represents the lowest price to the Government.

4.A.1.1. The RFQ requirement will be sent electronically to all JGSC contractors via email.

4.A.1.2. All JGSC contractors will be provided with an equal opportunity to submit prices electronically for the specific charter within the timeframe specified in the RFQ.

4.A.1.3. Quotes received after the cutoff may be considered only if no technically acceptable quotes are received before the cutoff or if the late quote offers significant advantages to the Government. Late quotes received after the award decision has been made will not be considered under any circumstances.

4.B. Task Order Evaluation

The Government's task order evaluation will consider the following factors:

1. Classified Requirement Compliance, if applicable
2. U.S. Flag Preference
3. VISA Preference
4. RFO[1] DFARS 252.247-7026, if applicable
5. Technical Capability
6. Small Business Preference, if applicable
7. Past Performance, if applicable
8. Price

4.C. Task Order Evaluation Factor Criteria

4.C.1. Classified Requirement Compliance

4.C.1.1. The Government will evaluate proposals to verify compliance with classified requirements, if applicable.

4.C.2. U.S. Flag preference

4.C.2.1. In accordance with the Military Cargo Preference Act of 1904, the order of priority or cargo moving via ocean is as follows: U.S. Flag vessels (P1), Combination U.S./Foreign Flag vessels (P2), and Foreign Flag vessels (P3).

4.C.2.2. In compliance with Cargo Preference, the Contracting Officer may elect to only evaluate U.S. Flag vessels, to include current U.S. Flag vessels and vessels to be U.S. Flag upon delivery.

4.C.3. VISA preference

4.C.3.1. The VISA preference will be applied as detailed below:

[1] A citation of "RFO" indicates the reference cited is derived from the Revolutionary Federal Acquisition Regulation (FAR) Overhaul (RFO) in effect at the time of solicitation issuance.

4.C.3.1.1. Vessel offered is enrolled in VISA.

4.C.3.1.2. U.S. Flag vessel capacity operated by a Participant.

4.C.3.1.3. Combination U.S./Foreign Flag vessel capacity operated by a Participant.

4.C.3.1.4. U.S.-owned or operated foreign flag vessel capacity.

4.C.4. RFO DFARS 252.247-7026 Evaluation Preference for Use of Domestic Shipyards

4.C.4.1. If the RFQ includes RFO DFARS 252.247-7026, then the evaluation scheme is as follows: If 50% or more of the cost of overhaul, repair, and maintenance work of an offeror's "covered vessel[s]" (see definition at RFO DFARS 252.247-7026(a)) has been conducted within a U.S. shipyard during the period covering the current calendar year through the date of proposal submission, plus the preceding four calendar years, then the offeror is in "Category 1." All other offerors are in "Category 2."

4.C.5. Technical Evaluation for Voyage and Time Charters (only one applies).

4.C.5.1. Voyage Charter Technical. The offeror's proposal will be evaluated based on technical capability of the vessel(s) proposed per the requirements outlined in Part I, DRYVOY Boxes 1 through 7 of the voyage charter proforma, as referenced in Section 3.B.1 above. Owner/Offeror shall address all technical items in Boxes 1 through 7 for evaluation purposes.

4.C.5.2. Time Charter Technical. The offeror's proposal will be evaluated based on technical capability of the vessel(s) proposed per the requirements outlined in Part I, DRYTIME Boxes 1 through 6 of the time charter proforma, as referenced in Section 3.A.1 above. Owner/Offeror shall address all technical items in Boxes 1 through 6 for evaluation purposes.

4.C.6. Small Business Preference, if applicable

4.C.6.1. A small business preference may be applied to task orders where at least two technically acceptable small businesses submit quotes in response to the RFQ and meet the highest applicable VISA preference among the quotes received.

4.C.7. Past Performance, if applicable

4.C.7.1. If included as an evaluation factor in the RFQ, past performance will be evaluated on an acceptable/unacceptable basis. Offerors without relevant past performance history will receive a neutral rating, which is considered acceptable.

4.C.8. Price Evaluation for Voyage and Charter (only one applies).

4.C.8.1. Voyage Charter Price. The evaluated price will be computed based on the lump sum freight rate plus one day demurrage plus any other costs set forth in the offer. The proposed price must be determined to be fair and reasonable.

4.C.8.2. Time Charter Price. The offeror's price proposal will be evaluated based on the value of the charter hire rate(s) offered for the entire charter period of (a)__days, price for fuel, and any other pricing elements set forth in the offer. For evaluation purposes, the period of performance will consist of (b) _____ days. Fuel calculations will be based on:

(c) ____days underway laden at the speed specified in the individual solicitation, using fuel consumptions provided in DRYTIME Boxes 68 and 70;

(d)____days underway ballast at the speed specified in the individual solicitation, using fuel consumptions provided in DRYTIME Boxes 69 and 70; and

(e)____ days in port idle, using the fuel consumption provided in DRYTIME Box 71.

4.C.8.3. This will represent the overall price to the Government. The proposed price(s) must be determined to be fair and reasonable.

4.C.8.4. Fuel consumption calculations will be made using the following Defense Logistics Agency Energy (DLA-E) standard prices and appropriate fuel conversion factors. The rate(s) to be used will be identified in the RFQ. All fuel consumption will be based on MGO/MDO prices.

4.C.8.5. Fuel conversion factors are as follows:

MGO/MDO: 7.507 barrels per metric ton
LSFO: TBD

4.D. Lowest Price Technically Acceptable (LPTA) Evaluation

4.D.1. The Government will conduct an LPTA evaluation to determine the award of the task order. Offers will first be evaluated for Classified Requirement Compliance on an Acceptable/Unacceptable basis, if applicable. Offers that do not meet the classified requirements of the RFQ will be deemed unacceptable and will not be considered further.

4.D.2. Next, offers that meet the classified requirement compliance will be prioritized based on the following hierarchy:

4.D.2.1. U.S. Flag Preference - Offers will be evaluated based on their service priority as outlined in paragraph 4.C.2.

4.D.2.2. VISA Preference – Offers will be evaluated in accordance with the VISA preference outlined in paragraph 4.C.3.

4.D.2.3. RFO DFARS 252.247-7026 Preference - If RFO DFARS 252.247-7026 applies, offers will be evaluated as outlined in paragraph 4.C.4.

4.D.3. After offers are prioritized based on the above preferences, the Government will assess technical capability on an Acceptable/Unacceptable basis. Offers that meet the technical requirements of the RFQ will be considered acceptable, while those that do not will be deemed unacceptable. Among technically acceptable offers, the award will be made to the offeror that satisfies the highest applicable preference while also offering the lowest price.

4.D.4. A small business preference may be applied to task orders as outlined in paragraph 4.C.6.

4.D.5. Past performance may be considered in the award decision if referenced in the RFQ as outlined in paragraph 4.C.7.

4.D.6. A written notice of award or acceptance of an offer furnished to the successful Offeror within the time for acceptance specified in the offer shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

SECTION 5 ON-RAMP OF ADDITIONAL CONTRACTORS

5.A.1. The Government reserves the right, at its sole discretion, to add ("on-ramp") additional vendors to this contract at any time during the contract period, provided they meet the following eligibility criteria:

5.A.1.1. The contractor must be an approved Participant in the Voluntary Intermodal Sealift Agreement (VISA) program and must remain a VISA Participant throughout the duration of the contract.

5.A.1.2. The contractor must own or control Roll-On/Roll-Off (RORO), multi-purpose, or vehicle carrier vessel(s).

5.A.1.3. The contractor's vessel(s) must have transported Department of War (DoW) cargo within the two years preceding the date of request.

5.A.2. Contractors seeking to be considered for on-ramp must submit documentation demonstrating compliance with all eligibility requirements to the Contracting Officer. The Government will evaluate submissions in accordance with the procedures outlined in Solicitation HTC71126RE142. If eligibility is confirmed, the Government may immediately award a contract to the contractor under the same terms and conditions as existing awardees.

5.A.3. The Government reserves the right to modify or update the on-ramp procedures as necessary to meet mission requirements.

SECTION 6 INVOICING

6.A.1. Invoicing instructions, payment terms, and supporting documentation requirements are established in the applicable task order proforma available on the MSC website. The Contractor shall comply with all invoicing requirements specified therein. Payments will be made in accordance with Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

SECTION 7 DELIVERABLES SCHEDULE

7.A. General Vessel Information

7.A.1. The contractor shall complete and submit Appendix A, General Vessel Information for any vessel the contractor plans to use under this contract within thirty (30) calendar days after contract award. This documentation shall be updated and resubmitted every six (6) months thereafter for all vessels intended for use under this contract. The submission and periodic update of Appendix A, General Vessel Information, is intended to streamline the evaluation of vessels under this contract but does not restrict the contractor from proposing alternative vessels in response to RFQs.

7.B. Task Order Deliverables

7.B.1. All task order deliverables, including reports, are included in the task order proformas available on the MSC website. The required formatting and procedures for submission are established in the Standard Operating Manual (SOM). The contractor shall strictly adhere to these guidelines when preparing and submitting all deliverables.

SECTION 8 SERVICE DELIVERY SUMMARY (SDS)

8.A.1. The SDS summarizes desired outcomes and identifies the performance thresholds/metrics that will be tracked to determine whether the desired outcomes are being achieved. Although not all PWS requirements are listed in the SDS, the Contractor is fully expected to comply with all requirements in the PWS and elsewhere in the contract (e.g., contract clauses).

Table 1, SDS

Desired Outcome	Proforma /PWS Para	Performance Threshold (Metric)	Source of Data	How Often Collected	Calculation
Notification of Reimbursable Expense Threshold	Proforma Part IV.(l)(4)	CO is notified 100% of the time when reimbursable funding reaches 85% of the allocated amount.	Monitoring Enterprise Resource Program (ERP) funding	As needed	# of missed notifications
Expense Management	Proforma Part IV.(l)(4)	Reimbursable expenses do not exceed allocated funding 100% of the time.	Monitoring ERP funding	As needed	# of instances where reimbursable expenses exceed allocated funding.
Operational Readiness	Proforma Part IV. (i)	Vessel is Ready For Tasking (RFT) 100% of the time.	Contractor Reports, Operational Audits	As required	# of days unavailable
Provide Timely Cyber-Incident Reporting	PWS 7.A.2.	No more than one late cyber-incident report or unreported cyber-incident in a twelve (12) month period.	Table 2, Cyber Incidents	As needed	# of late or unreported cyber incidents per year.

This contract is using performance-based acquisition methods. Performance will be measured based on the successful completion of the tasks outlined in the Performance Work Statement and in accordance with the following metrics.

8.B. Quality Control, Reporting, and Records

8.B.1. The Government's process for tracking and overseeing contractor performance consists of setting acceptable standards for the contractor. The COR will evaluate contractor compliance with the standards by establishing metrics. The awardee's compliance with acceptable standards will be tracked in Contractor Performance Assessment Reports (CPARS).

8.B.2. The majority of performance monitoring under the QASP will be performed by the COR. The Government will utilize the QASP to measure the contractor's performance against defined performance thresholds included in the above chart. Additionally, the Government will utilize a variety of surveillance methods to ensure contractor compliance. Surveillance methods include but are not limited to: direct observation, periodic inspections, periodic sampling, progress meetings, analysis of contractor's reports, and performance reporting through CPARS.

8.B.3. The Government must monitor and verify that the contractor is not participating in any combatting human trafficking in persons (CTIP) prohibited activities. Contractors will be required to complete the CTIP Checklist annually for the Government to verify the contractor is not engaging in any CTIP prohibited activities.

8.B.3.1. The Government must monitor and verify that the contractor is not participating in any CTIP prohibited activities. The contractor will be required to complete the DoD COR Guidebook, dated October 2022, appendix D.7, CTIP Checklist based on the review cycle as identified in the QASP and/or when there is an indication of a trafficking in persons (TIP) violation. COR will maintain oversight for the Government to verify that contractor is not engaging in any CTIP prohibited activities. When the action includes a compliance plan, then the COR must review the plan and supporting documents to ensure the contractor is compliant and communicate findings to the Contracting Officer as outlined in RFO FAR 52.222-50.

8.B.3.2. In accordance with RFO DFARS PGI 222.17(4), the COR must immediately bring to the attention of the Contracting Officer any non-compliance with RFO FAR 52.222-50. Upon receiving information indicating that contractor, a contractor employee, a subcontractor, or a subcontractor employee has failed to comply with the requirements at RFO FAR 52.222-50, the Contracting Officer shall follow the procedures at RFO DFARS PGI 222.1704 for reporting violations.

8.B.4. The COR shall verify that the contractor has met and complied with contractual whistleblower requirements. The oversight of the requirement in this contract surveillance plan for whistleblower is included in the above table.

8.B.5. COR shall provide annual assessment of the above performance requirements in PIEE – SPM.

8.B.6. The COR may issue a Contract Discrepancy Report (CDR) when the Contractor fails to meet the terms and conditions of the contract. Upon request, the Contractor shall provide the

cognizant COR with a written plan of corrective action, including a proposed timeline, within 5 business days after such request. This plan shall describe proposed Contractor actions to correct the problem or deficiency and bring performance back into compliance with identified performance standards.

8.B.7. The CORs shall monitor Contractor performance and compliance with the terms and the conditions of the contract using standard techniques such as inspections, Government-generated management reports, Contractor reports and customer feedback, or as otherwise indicated herein. The Contractor shall attend periodic meetings called by the COR or the Contracting Officer to discuss operations and problem areas.

8.B.8. Retention of Records. The Contractor shall maintain and, upon request, provide to the Contracting Officer such documentation deemed relevant to performance of transportation services ordered under the terms of this contract. Records will be maintained and available to the Contracting Officer throughout the term of the contract and for three years after final payment in accordance.

SECTION 9 SECURITY (CYBER SECURITY, INDUSTRIAL SECURITY, VENDOR THREAT MITIGATION)

9.A. Operationally Critical Support

9.A.1. The services designated under this contract are "operationally critical support" as defined in RFO DFARS 252.204-7012.

9.B. Cybersecurity Incident Reporting

9.B.1. In addition to the RFO DFARS 252.204-7012 reporting requirements for unclassified systems and DoD Manual (DoDM) 5220.22, National Industrial Security Program Operating Manual (NISPOM) for classified systems, reportable cyber-incidents include, but are not limited to, the following:

9.B.1.1. Cyber-incidents as defined in Table 2

9.B.1.2. Notifications by a federal, state, or local law enforcement agency or cyber-center (i.e., National Cyber Investigative Joint Task Force (NCIJTF), National Cybersecurity & Communications Integration Center (NCCIC)) of being a victim of a successful or unsuccessful cyber-event, anomaly, incident, insider threat, breach, intrusion, or exfiltration.

Table 2, Cyber Incidents

Incident Category	Description
Root Level Intrusion	Unauthorized privileged access to an IS. Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that

	provides remote interactive control, it will be reported in this category.
User Level Intrusion	Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
Denial of Service	Denial of Service (Incident)—Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.
Malicious Logic	Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Root or User Level Intrusion incidents. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS.
Ransomware	Malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. Ransomware is a reportable incident that may be associated with multiple incident categories depending on the attack vector and execution.

9.B.2. If the cyber-incident affects a classified system, vulnerabilities associated with the incident will be classified per the current version of USTRANSCOM Instruction 31-02, Security Classification Guide.

9.C. Cybersecurity Incident Reporting Timelines

In addition to providing the notification required by RFO DFARS 252.204-7012, the contractor is required to notify USTRANSCOM as soon as practical, but no later than 72 hours after discovering a reportable cyber-incident. The reporting timeline begins when the incident is discovered or reported to the company, its employees, contractors, or cybersecurity firm responsible for providing cybersecurity and response for the company. The contractor shall contact the USTRANSCOM Cyber Operations Center (CyOC) via phone at 618-817-4222. If the contractor does not immediately reach the CyOC via phone, the contractor shall send an email notification to transcom.scott.tcj6.mbx.cyoc-dodin-operations@mail.mil.

9.D. Mandatory Reporting Data

9.D.1. The contractor shall work with the USTRANSCOM CyOC through resolution of the incident. Within 72 hours of becoming aware of a reportable cyber-incident, the contractor shall provide an initial notification of the incident, even if some details are not yet available, which includes, but is not limited to, the following information:

(a) Company Name
(b) Who will be the POC with contact information
(c) Contracting Officer POC (name, telephone, email)
(d) Overall Assessment –Description of incident, data at risk, mitigations applied
(e) Indicators of compromise
(f) Vector of attack (if known)
(g) Estimated time of attack (if known)

9.D.2. The contractor shall provide a follow-on cyber-incident report to the USTRANSCOM CyOC within 5 business days of becoming aware of a reportable cyber-incident, which includes, but is not limited to, the following information:

(a) Contractor unique Commercial and Government Entity (CAGE) code
(b) Contract numbers affected
(c) Facility CAGE code where the incident occurred if different than the prime Contractor location
(d) POC if different than the POC recorded in the System for Award Management (name, address, position, telephone, email)
(e) Contracting Officer POC (name, telephone, email)
(f) Contract clearance level
(g) DoD programs, platforms, systems, or information involved
(h) Location(s) of compromise
(i) Date incident discovered
(j) Type of compromise (e.g., unauthorized access, inadvertent release, other)
(k) Description of technical information compromised
(l) Any additional information relevant to the information compromise

9.E. Incident Reporting Coordination

9.E.1. In the event of a cyber-incident, USTRANSCOM may conduct an on-site review of network or information systems where DoD information is resident on or transiting to assist the contractor in evaluating the extent of the incident and to share information in an effort to minimize the impact to both parties. Date and time of on-site visits will be mutually agreed upon by USTRANSCOM and the contractor in advance.

9.E.2. The contractor agrees to allow follow-on actions by the Government (e.g., USTRANSCOM, Federal Bureau of Investigation, Department of Homeland Security, DC3, etc.) to further characterize and evaluate the suspect activity. The contractor acknowledges that damage assessments might be necessary to ascertain an incident methodology and identify systems compromised as a result of the incident. Once an incident is identified, the contractor agrees to take all reasonable and appropriate steps to preserve any and all evidence, information, data, logs, electronic files and similar type information (reference NIST Special Publication 800-61, Computer Security Incident Handling Guide, (current version)) related to the incident for

subsequent forensic analysis so that an accurate and complete damage assessment can be accomplished by the Government.

9.E.3. The contractor is not required to maintain an organic forensic capability, but must ensure data is preserved (e.g., remove an affected system, while still powered on, from the network) and all actions documented until forensic analysis can be performed by the Government or, if the Government is unable to conduct the forensic analysis, a mutually agreed upon third party (e.g., Federally Funded Research and Development Center (FFRDC), commercial security contractor, etc.). Any follow-on actions shall be coordinated with the contractor via the Contracting Officer.

9.E.4. The contractor agrees to indemnify and hold the government harmless for following any recommendations to remedy or mitigate the cyber-incident following the actions under 9.E.1. and 9.E.2.

9.F. Confidentiality and Non-Attribution Statement

9.F.1. The Government may use and disclose reported information as authorized by law and will only provide attribution information on a need-to-know basis to authorized persons for cybersecurity and related purposes (e.g., in support of forensic analysis, incident response, compromise or damage assessments, law enforcement, counterintelligence, threat reporting, and trend analysis). The Government may share threat information with other USTRANSCOM industry partners without attributing or identifying the affected contractor.

9.G. Cybersecurity Material Model Certification (CMMC)

To comply with DFARS clause 252.204-7012, contractor is required to develop a System Security Plan (SSP) detailing the policies and procedures their organization has in place to comply with National Institute of Standards & Technology (NIST) Special Publication (SP) 800-171. The SSP serves as a foundational document for the required NIST SP 800-171 self-assessment as required by the Cybersecurity Maturity Model Certification Level 2 (Self), which applies IAW DFARS 252.204-7021.

9.H. Industrial Security Information (Applicable Only to Task Orders Involving Classified or Sensitive Cargo)

9.H.1. General Security Requirements Information/Applicability: The majority of daily work associated with this PWS is at the unclassified level, but contractor personnel may be required to access classified information/systems at the SECRET level, and/or classified areas at the SECRET level, during the performance of this contract/task order. RFO FAR Clause 52.240-92, Security Requirements, applies to the extent of this contract/task order involving access to information, areas, or material classified "CONFIDENTIAL" or "SECRET". Specific security protocols for contracted companies are outlined in 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM), identified in this section of the PWS, and the DD Form 254 (DoD Contractor Security Classification Specification).

9.H.2. Contractors who possess the appropriate security clearances may request to review the classified requirement at Military Sealift Command (MSC) associated with applicable RFQs. Contractors lacking the necessary security clearance may be disqualified from consideration for those RFQs. To initiate the review, contractors must submit a written request to the contracting officer within five business days of the RFQ's release. Once approved, the contractor is

responsible for making arrangements, at their own expense, to review the classified material at the designated location and time, which will occur prior to the RFQ response deadline. If a contractor fails to submit a timely request or misses the scheduled review, the opportunity to examine the classified requirement will be forfeited.

9.H.3. Citizenship and Clearance Requirements: All personnel that will have Information Technology (IT)/Automated Data Processing (ADP) privileged access (i.e. Privileged Users) to US Information Systems (IS), and/or classified information, classified systems, or classified areas, shall be US citizens. Foreign Nationals or Local Nationals employed by the DoD are not authorized to have privileged access to US Information Systems. Overall, all contractor's, subcontractors' and/or partner's personnel shall possess the appropriate personnel security investigation for the position(s) occupied. Contractor personnel shall be required to have a background investigation that corresponds with the sensitivity level of the tasks to be performed. Non-US citizens are not eligible for Common Access Cards (CACs) unless they meet the parameters stated in Department of Defense Manual (DoDM) 1000.13, Volume 1.

9.H.4. Information Systems (IS) Roles/Categories and Associated Suitability Requirements (Federal Investigative Standards): Contractor personnel with IA administrative privileges and/or who will monitor DoD IT systems or software as designated by DoD Instruction 8500.01 and DoD Manual 5200.02 may be rated at the various levels listed below. The IS roles/categories and the number of personnel assigned to each role is approved by the COR or the CO before the start of the contract/task order. The contractor shall comply with the appropriate provisions of applicable security regulations while assigned to this contract/task order for DOD and USTRANSCOM. The following guidance will be followed when determining background investigation levels for this contract/task order depending on requirements:

IS Role/Category	Classified Access	Required Investigation
General User (Non-Privileged Access) (IT/ADP-III, Non-Sensitive)	NO	Tier 1 (T1)
General User (Non-Privileged Access) (IT/ADP-II, Non-Critical Sensitive)	YES	Tier 3 (T3)
Privileged User (e.g. System Administrator) (IT/ADP-I, Critical Sensitive)	NO	Tier 5 (T5)
Privileged User (IT/ADP-I, Critical Sensitive)	YES	Tier 5 (T5)

NOTE1: USTRANSCOM Joint Security Office (TCCS-S) will initiate/administer Tier 1 investigations to determine CAC eligibility only, classified access will not be granted based on the Tier 1 investigation. Tier 3 and Tier 5 investigations are the responsibility of the contractor. It is incumbent upon the contractor to have the appropriate investigations completed upon the start of the contract/task order.

9.H.5. Security Clearance and Special Access Requirements: All positions on this task order, require a minimum of either an interim SECRET granted by the Defense Counterintelligence and

Security Agency (DCSA) Adjudication & Vetting Services (AVS), or a completed adjudication of SECRET granted by the DCSA AVS.

9.H.6. Facilities Clearance (FCL): The contractor must have a valid FCL at the SECRET level. FCL procedures and security guidelines for adjudicative requirements are outlined in 32 CFR, Part 117. FCLs must be awarded by the Defense Counterintelligence and Security Agency (DCSA) Entity Vetting Branch.

9.H.7. Personnel and Facilities Clearance Validation: Upon contract/task order award, the USTRANSCOM contracting team will send TCCS-S the contractor cage code for FCL verification via the National Industrial Security System (NISS). The contractor will submit names of the contractor personnel performing on the contract/task order to the USTRANSCOM contracting team, who will provide to TCCS-S for vetting through the DoD personnel security system of record to ensure investigative and clearance requirements have been satisfied. This shall be completed before the COR/Mission Partner Affiliation Sponsor (MPAS) accesses the Mission Partner Identity, Credential, and Access Management (MP ICAM) system and creates CAC applications for contractor personnel. If a contractor's employee does not have the required investigative or security clearance level based on the Government's determination, the contractor's employee will be denied the ability to work in support of this contract/task order.

9.H.8. Common Access Card (CAC) Issuance Procedures:

a) Facility Security Officer (FSO) will verify, via the DOD personnel security system of record, contractors on the contract/task order have the required background investigation to obtain a CAC and provide those names to the CO/COR. Contractors that require a Tier 3 or Tier 5 investigation are the responsibility of the contractor. Contractors that only require a Tier 1 as determined by the FSO will submit to the TCCS-S Personnel Security Program Manager (through the CO or COR) an OF Form 306 (Declaration for Federal Employment) and a MP ICAM Form 1 with Section 1 completed. TCCS-S will initiate the SF-85 (questionnaire for Non-Sensitive Positions) via the National Background Investigation Services (NBIS) for completion and submission to DCSA, for Tier 1 investigations only.

b) At the same time, the contractor company will coordinate and obtain electronic fingerprinting for their employee. The third-party company will "electronically" capture the applicant's fingerprints, using the USTRANSCOM (Submitting Office (SON), Security Office (SOI), and Agency Location Code (ALC)). Hardcopy fingerprint cards are NOT acceptable. These steps shall be completed before the COR/MPAS accesses MP ICAM to create a CAC application.

c) Basic US Citizen Contractor CAC Requirements:
    1. Requires access on a continual basis of 6 months or more.
    2. Contractor personnel require access to a DoD facility or networks, either on-site or from a remote location.
    3. Users need access to systems for platforms that requires CAC login or user authentication.

d) Basic Non-US Citizen Contractor CAC Requirements:
   1. Meet (as direct/indirect DoD hire personnel), as identified in the DoDM 1000.13, Volume 1, the investigative requirements for DoD employment as recognized through international agreements pursuant to DoDI 1400.25, Civilian Personnel Management, Volume 1231. In addition to these investigative requirements, a fingerprint check against the FBI criminal history database, an FBI investigations files (name check search), and a name check against the Terrorist Screening Database shall be required prior to CAC issuance IAW Office of Personnel Management Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12", July 31, 2008.
   2. Possess (as foreign military, employee, or contract support personnel), a visit status and security assurance that has been confirmed, documented, and processed IAW international agreements pursuant to DoDI 1400.25, *Civilian Personnel Management*.

e) CAC Applications:
   1. The CAC applications (MP ICAM Form 1 with Section 1 completed) must have an adjudication Tier 1, Tier 3, or Tier 5 background investigation posted in the DoD personnel security system of record, or
   2. An interim CAC may be approved when the contractor employee has a favorable fingerprint, name and criminal records check completed and has either a Tier 1, Tier 3, or Tier 5 background check "open" with DCSA.
   3. The MP ICAM MPAS will not approve the CAC applications in MP ICAM until that MPAS has verified, with a member of USTRANSCOM TCCS-S, one of the above requirements.

9.H.9. Access to Scott Air Force Base or USTRANSCOM Facilities: Upon receipt of the CAC, permanently assigned contractor personnel located at USTRANSCOM at Scott AFB (SAFB), IL, may obtain a USTRANSCOM Facility Access Badge if the employee will be assigned physically on SAFB in a USTRANSCOM-owned or managed facility, has a valid Visit Access Request on file, and attends Initial Security Training (IST) on-site. The Government will provide unrestricted access to facilities, consistent with security clearance eligibility and need-to-know, necessary for the on-site personnel to perform their work IAW the contract/task order. Contractor personnel assigned on-site at USTRANSCOM will wear and display the USTRANSCOM Facility Access Badge at all times while in USTRANSCOM facilities. Visits to SAFB by contractor personnel who do not possess the CAC will be facilitated by the COR/CO sponsoring the employee through the online base access system.

9.H.10. Visits by Non-Assigned Contractors to USTRANSCOM/SDDC Buildings: Any visit(s) by contractor personnel not permanently assigned to this contract/task order (i.e., company presidents, company security managers, contractor personnel not permanently assigned at SAFB, etc.) require an electronic visit access request be submitted using the DoD personnel security system of record. The DoD personnel security system of record visits can be forwarded to the Security Management Office (SMO) code: US-TRANSCOM-1. The visit access request

shall annotate the contract/task order number in the POC block of the visit access request and the name/phone number of either the functional, COR or CO in the phone number block.

9.H.11. Visits by Permanently Assigned Contractors: Permanently assigned contractor employees on SAFB will require a visit access request for the current Period of Performance (PoP) posted in the DoD personnel security system of record to SMO: US-TRANSCOM-1. The visit access request will annotate the contract number in the POC block of the visit access request and the name/phone number of either the functional, COR or CO in the phone number block.

9.H.12. Supplemental Notes Regarding Visit Information in the DoD Personnel Security System of Record: Personnel requiring access to Government facilities will properly complete the "Visit Information" block in the DoD personnel security system of record. Otherwise, contractor employees will be denied access to the facility and classified and/or sensitive information. Also, prime contractors will annotate their contract number and subcontractors will provide the name of their Company, with the prime contract number they are assigned to by the Prime, in the "additional information" block of the Visit table. A valid "Reason for the Visit" must be stated and the "visit access" must not exceed that of the contract.

9.H.13. Security and Emergency Operations Training: Contractor personnel physically assigned at USTRANSCOM at SAFB shall attend/complete the following training as prescribed by DoD, USTRANSCOM and Air Force Instructions: Initial Security, Workplace Violence, Annual Security Awareness, Operations Security (OPSEC), DOD Antiterrorism Level I, Active Shooter/Attacker, Emergency Operations, Combating Trafficking in Person (CTIP), Controlled Unclassified Information (CUI), Derivative Classification, and any Security Stand-down Day Training scheduled by the Commander, USTRANSCOM. Contractor personnel assigned elsewhere shall attend security training established by their respective Government security offices and/or installations.

9.H.14. Additional Security Conditions: All contractors assigned to USTRANSCOM on SAFB will complete contractor in-processing before the start of work on this or any contract/task order in USTRANSCOM. Contractors starting work on a new contract/task order will report to the Joint Security Desk, located in Building 1900 first-floor breezeway. In-processing includes the following:

- Verification of personal identification
- Verification of Visit Access Request in the DoD personnel security system of record
- Verification of the contractor's Security Clearance Eligibility in the DoD personnel security system of record
- Brief and sign the individual SF-312 (Security Agreement)
- Complete North Atlantic Treaty Organization (NATO) Indoctrination
- Review of Facility access requirements
- Issuance of a Temporary USTRANSCOM Facility Access Badge for the facility
- Creation of a personnel security file

9.H.15. Derogatory Information: Any member of the contracted company team (Program Manager, FSO, or other supervisory staff) aware of pending human resource activity of consequence (to include termination or suspension), behaviors or patterns of concern, or misconduct, to include reporting requirements in accordance with Security Executive Agent Directive (SEAD) 3 (for contractors with classified security eligibility), for any contractors supporting this contract/task order during the established period of performance, will immediately contact the USTRANSCOM Joint Security Office (TCCS-S) Attn: Industrial Security Program Manager. If the Government notifies the contractor that the employment or the continued employment of any contractor personnel is prejudicial to the interests or endangers the security of the United States of America and/or USTRANSCOM personnel, information, or assets; that employee shall be removed and barred from the worksite. This includes security deviations / incidents and credible derogatory information on contractor personnel as noted in the DoD personnel security system of record. Personnel who have incident reports posted in the DoD personnel security system of record will be denied the ability to support the contract/task order until the issues have been resolved and the incident has been removed in the DoD personnel security system of record. The contractor shall make any changes necessary in the appointment(s), at no additional cost to the Government. If any incident involves or may involve the mishandling of classified information or a potential Negligent Discharge of Classified Information, the USTRANSCOM Joint Security Office Attn: Industrial Security Program Manager, will be notified within 24 hours during the normal work week and within 72 hours if the incident occurs over the weekend.

9.H.16. Accessing NATO Information: No contractor employee will access NATO information without first being indoctrinated on NATO and having that access recorded in the DoD personnel security system of record. Any NATO information accessed will be only on SIPRNet. Senders of NATO information will ensure the receiving network is accredited and the receiving point is a Sub-Registry or authorized Control Point. No NATO information will be stored with US classified information. Access to NATO information will be based on need-to-know, appropriate access level, and training. NATO information will not be disseminated to unauthorized users. NATO information will not be printed unless authorized by a USTRANSCOM NATO – Sub-Registry person in TCCS-S. All printed NATO classified information must be strictly controlled and tracked in a NATO registry. Contact the USTRANSCOM Sub-Registry for additional control measures. In accordance with 32 CFR, part 117, NATO briefed personnel will be re-briefed on an annual basis. USTRANSCOM will indoctrinate all on-site contractor employees and document in the DoD personnel security system of record. Contractor personnel assigned to USTRANSCOM facilities will be NATO briefed and debriefed by USTRANSCOM, with appropriate annotations to the DoD personnel security system of record. Company FSOs may take responsibility for all NATO refresher briefings per 32 CFR, part 117 and record the date of the annual briefings in the contractor employee's records.

9.H.17. Security Debriefing: Contractor personnel physically working at USTRANSCOM at SAFB, IL, shall complete out-processing on the last day of the contract/task order or upon termination or reassignment from duties under the current contract/task order. The following closeout tasks will be completed, before the contractor departs:

- Review of the contractor's personnel security folder

- Review and debrief the contractor's SF-312
- Debrief anyone with NATO Access
- Update and annotate the DoD personnel security system of record reflecting the current status of the contractor at USTRANSCOM
- Surrender CAC (with copy of the revocation notice from the COR or MPAS), for those off-site CACs will be physically mailed to TCCS-S for collection and turned into Scott AFB ID office for DMDC inventory and destruction.
- Surrender the USTRANSCOM Facility Access Badge to the Joint Security Desk
- Contractor personnel shall have surrendered all Government supplies, materials, and equipment to the COR.

9.H.18. Antiterrorism/Force Protection: Contractor employees will comply with antiterrorism Force Protection conditions (FPCONs) at the location they are performing work, whether it is CONUS or OCONUS.

9.H.19. NOTE TO THE PRIME CONTRACTOR FACILITY SECURITY OFFICER (FSO): The prime contractor will forward the name, address, email address and telephone number of the Company FSO and backup to the USTRANSCOM Joint Security Office (TCCS-S) at: transcom.scott.tccs.mbx.industrial-security@mail.mil

9.H.20. USTRANSCOM Joint Security Office (Industrial Security) POCs:
USTRANSCOM
Attn: TCCS-S (Industrial Security Specialist)
508 Scott Drive
Scott AFB, IL 62225
Commercial: 618-817-4078

9.H.21. USTRANSCOM TCCS-S Approval:
Dustin Castle, Acting Chief, USTRANSCOM Joint Security Office

9.H.22. USTRANSCOM TCCS-S Tracking #: TCCS-S-XXX-YYYY

APPENDIX A, GENERAL VESSEL INFORMATION

GENERAL VESSEL INFORMATION	
1. Vessel type and, if applicable, MARAD design type:	
2. Place built	3. Year built: Flag:
4. INMARSAT Ident.:	5. Vessel's e-mail/Fax:
6. Call Letters:	7. IMO number:
8. Net registered tonnage:	9. Panama Canal tonnage:
10. Gross registered tonnage:	11. Suez Canal tonnage:
12. Beam (extreme) a. (ft) b. (m)	13. Length Overall: a. (ft) b. (m)
14. Immersion (on draft in Box 36): a. (LT/in) b. (t/cm)	15. Length between perpendiculars: a. (ft) b. (m)
16. Summer mean draft: a. (ft) b. (m)	17. Deadweight capacity (on draft in Box 16): a. (LT) b. (t)
18. Displacement, loaded (on draft in Box 36): a. (LT/in) b. (t/cm)	19. Summer Load Line Freeboard: a. (ft) b. (m)
20. Shaft Horsepower/kilowatts: a. (hp) b. (kW)	21. Brake Horsepower/kilowatts: a. (hp) b. (kW)
22. Nationality of Master/Officers/Crew:	23. Number of persons other than crew that can be carried:
24. Classification society entered and class assigned:	

25. Insured value of vessel (USD):	26. Vessel's present position/destination:
27. Last dry-dock date (mm/dd/yy):	28. Next dry-dock date (mm/dd/yy):
29. MarAd subsidized vessel: Yes _____	No _____
CARGO CAPACITY (as applicable)	
30. Total grain cubic capacity (cu ft / cubic meters underdeck, exclusive of deep tanks, wing tanks, reefer spaces, and spaces fitted with cell guides):	
31. Total Bale cubic capacity (cu ft / cubic meters underdeck, exclusive of deep tanks, wing tanks, reefer spaces, and spaces fitted with cell guides):	
32. Number of tween decks:	
33. Cargo Space	
a. Square footage of cargo space (note particularly total ft^2, ft^2 with 10 ft clearance, ft^2 underdeck, Ro/Ro Space): b. Square meters of cargo space (note particularly total m^2, m^2 with 3.048 m clearance, m^2 underdeck, Ro/Ro Space):	
34. Total underdeck container capacity (TEU/FEU):	
35. Total on-deck container capacity (TEU/FEU):	
36. Total refrigerated-container capacity (TEU/FEU, including number/style of outlets):	
37. Reefer-space capacity (cu ft / cu meters):	

38. Deep-tank capacity (cu ft/cu meters/bbls):
39. Capacity of spaces fitted with cell guides (TEU):
40. Amount and location of permanent ballast carried:
41. General description of ramps (number, location, size, capacity, and type): (note particularly weight of heaviest permissible vehicle in LT or t)
42. General description of cargo spaces and special features: Decks: number, size in ft^2 and cu ft; size in m^2 and cu m; strength in psf/kPa; arrangement Holds and Hatches: number and size Hatch Covers: number, size, composition, and type Underdeck Height Restriction Description of lashing points; lashing and securing gear; type; description; and amount aboard Barge-Stowage Particulars Float-on / Float-off Particulars
43. Number/location/SWL capacity of winches, derricks, booms, and cranes:

CASUALTIES / DEFICIENCIES / WARRANTS
44. Has vessel been involved in any serious grounding or collision within twelve months from the submission date of this proposal? (include full description if "yes")
45A. Are any deficiencies lodged by any regulatory body outstanding against the Vessel? (include full description if "yes")
45B. Identify any port(s) in which you have any active arrest warrants or similar actions pending that would either delay the vessel from performing, or otherwise prevent the vessel from free entry/departure.

FUEL CONSUMPTION AT SERVICE SPEEDS	
46. Average warranted speed (knots, for laden, moderate weather):	47. Average warranted speed (knots, for ballast, moderate weather):

48. Average fuel consumption (net bbls at 60 deg F and grade(s): for laden, moderate weather passage at speed identified in Box 46):	49. Average fuel consumption (net bbls at 60 deg F and grade(s): for ballast, moderate weather passage at speed identified in Box 47):
50. Auxiliaries underway fuel consumption (net bbls at 60 deg F and grade(s), only if not elsewhere identified):	51. Idle fuel period fuel consumption (net bbls at 60 deg F and grade(s)):

FUEL CONSUMPTION AT VARIABLE SPEEDS (as applicable)

Average fuel consumption (net bbls at 60 deg F for all grades and all engines/auxiliaries utilized while underway over moderate-weather passages at the speed, ranges, and grade(s) indicated):

52: Grades Consumed:

53 A. Knots	**LADEN** Net bbls per mile	Net bbls per day	Operating Range (NM)	53 B. Knots	**BALLAST** Net bbls per mile	Net bbls per day	Operating Range (NM)
10				10			
11				11			
12				12			
13				13			
14				14			
15				15			
16				16			
17				17			
18				18			
19				19			

20				20			
21				21			
22				22			