[redacted]

STATEMENT OF WORK
FOR
LOW SPEED VEHICLE (LSV) PREVENTIVE MAINTENANCE
[redacted]

1.0 SCOPE

The Naval Surface Warfare Center Panama City Division (NSWC PCD) requires Contractor support to provide routine preventive maintenance and repair support on low speed vehicles (LSV's) currently in use as well as vehicles that will be procured for use on NSWC PCD. Preventive maintenance shall be performed once per year to ensure equipment is running properly, avoiding costly downtime and extending the life cycle of the equipment. The following equipment shall be maintained:

MAKE	MODEL	VIN	S/N	CODE	LOCATION
DEFENDER	CAN-AM 6X6	TBD	TBD	107	B100
DEFENDER	CAN-AM 6X6	TBD	TBD	107	B100
DEFENDER	CAN-AM 6X6	TBD	TBD	107	B100
DEFENDER	CAN-AM MAX	TBD	TBD	107	B100
DEFENDER	CAN-AM PRO	3JB7KAX42LK001223	TBD	E31	B657
KAWASAKI		JK1AFCG106B511749	TBD	E42	B91
KAWASAKI	RED	JK1AFCJ157B512552	TBD	E41	B316
KAWASAKI	GREEN	FJ400DE054505	TBD	E41	B316
KAWASAKI	MULE PRO DXT	JKADTCC19SB505373	TBD	TBD	B316/B581
KUBOTA	RTV	A5KC2GDBLPG078276	TBD	E50	B100
KUBOTA	RTV	A5KC2GDBEPG079012	TBD	107	B100
KUBOTA	RTV	A5KC2GDBAKG050842	TBD	107	B100
KUBOTA	RTV	A5KC2GDBKPG050842	TBD	107	B100
KUBOTA		3JB7KAX42LK001223	TBD	1021	B49
KUBOTA		A5KC2GDBLRG086526	TBD	1021	B49
KUBOTA	RTV	A5KC2GDBPRG091927	TBD	E50	B79
KUBOTA	RTV	A5KCGDBKRG091332	TBD	E50	B79
KUBOTA	RTV	A5KC2GD8CRG092623	TBD	107DH	B100
KUBOTA	RTV	A5KC2GDPRG096934	TBD	107BH	B100
KUBOTA	RTV	TBD	TBD	E50	MOCOM
KUBOTA	RTV	TBD	TBD	E50	MOCOM
POLARIS	RANGER	3NSM4A578PE277965	TBD	TBD	B582
POLARIS	RANGER	3NSM4E575LE764171	TBD	1021	B110
POLARIS	RANGER	3NSM4A573LE762749	TBD	107	B100
POLARIS	RANGER	3NSCDA570LE092346	TBD	S31	B436
POLARIS	RANGER	3NSCDA576LEO093825	TBD	X11	B316
POLARIS	RANGER	3NSCDA574LE093824	TBD	X11	B316
POLARIS	RANGER	3NSM4A572NE550606	TBD	A14	B607

MAKE	MODEL	VIN	S/N	CODE	LOCATION
POLARIS	RANGER	3NSMAA578NE552238	TBD	A14	B608
POLARIS	RANGER	3NSM4A577NE314243	TBD	A22	B323
POLARIS	RANGER	3NSMAA572NE311274	TBD	A22	B323
POLARIS	RANGER	4XAT6E993M8013348	TBD	E13	B581
POLARIS	RANGER	3NSRDA574KE749478	TBD	X11	B581
POLARIS	RANGER	3NAM4A579NE314244	TBD	TBD	B460
POLARIS	RANGER	4XAT6A99XM8406935	TBD	1021	B110
POLARIS	RANGER	3NSMAA575LE769078	TBD	E20	MOCOM
POLARIS	RANGER	3NSM4A572LE092921	TBD	E20	MOCOM
POLARIS	RANGER	4XARSE995L8051202	TBD	E50	MOCOM
POLARIS	RANGER	4XAWH76AXD2294830	TBD	E40	B431/B147
POLARIS	RANGER	4XAXT9EA2DF250572	TBD	E40	B91
POLARIS	RANGER	4XAWHZ6AC2703395	TBD	E40	B582
POLARIS	RANGER	3NSM4A574LE767507	TBD	107	B110
POLARIS	RANGER	4XATAE999M8406057	TBD	X13	B581
POLARIS	RANGER	4XARSE992M8062918	TBD	S10	B582
POLARIS	RANGER	3NSM4U574RE007393	TBD	TBD	B490
POLARIS	RANGER	3NSM4U576RE007962	TBD	TBD	B493
POLARIS	RANGER	3NSM4U571RE007402	TBD	TBD	B493
POLARIS	RANGER	3NSM4A57XSE079929	TBD	TBD	B608
POLARIS	RANGER	3NSM4A577SE079936	TBD	TBD	B608
YAMAHA	BLUE RHINO	5Y4J34Y18A000993	TBD	E42	B91
YAMAHA	WOLVERINE	5Y4AJ34Y18A000993	TBD	S22	B581

1.1 Acronym List

Following is a list of acronyms used in this Statement of Work.

CDRL	Contract Data Requirements List	COR	Contracting Officer's Representative
CUI	Controlled Unclassified Information	DoW	Department of War
FAR	Federal Acquisition Regulation	FOUO	For Official Use Only
FOIA	Freedom of Information Act	GFE	Government Furnished Equipment
GFI	Government Furnished Information	GFM	Government Furnished Material
GFP	Government Furnished Property	HAZMAT	Hazardous Material
HM/HW	Hazardous Materials/Hazardous Waste	IT	Information Technology
NSA PC	Naval Support Activity Panama City	ODC	Other Direct Cost
OEM	Original Equipment Manufacturer	OPSEC	Operations Security
OSHA	Occupational Safety and Health Administration	PCO	Procuring Contracting Officer
PII	Personally Identifiable Information	PMS	Planned Maintenance System
PPE	Personal Protection Equipment	QASP	Quality Assurance Surveillance Plan
QMS	Quality Management System	SDS	Safety Data Sheet(s)
USN	United States Navy		

2.0 APPLICABLE DOCUMENTS

The following documents, of the exact issue shown, form a part of this SOW to the extent specified herein. In the event of conflict between the documents referenced and the contents of this SOW, the SOW shall take precedence. Second tier and lower references, (i.e., those referenced in the primary references) shall be used for guidance only.

2.1 Military Specifications: None

2.2 Military Standards: None

2.3 Other Documents: None

3.0 REQUIREMENTS

All LSV work shall be performed at the Contractor facility. The LSV shall be tracked via DD 1149's. The Technical Point of Contract (TPOC) for this effort shall be Christopher Owens, with the alternate being Cyril Gazagnaire. The TPOC shall be the only personnel authorized to call for troubleshooting and/or maintenance calls. The TPOC shall also be responsible for maintaining the list of equipment and service schedule.

3.1 Inspection and Maintenance Support

3.1.1 The Contractor shall provide routine preventive maintenance for the equipment listed in SOW paragraph 1.0. As part of each maintenance visit, the contractor shall conduct an inspection of each piece of equipment once per year. The inspection and maintenance shall consist of the following:

(a) Structure – Inspect for corrosion, cracks, distortion, damage, loose and missing fasteners, defective sealant and seals.

(b) Mechanical Linkages and Actuating Mechanisms – Inspect for cracks, corrosion, evidence of improper alignment and/or worn parts that could lead to equipment failure.

(c) Electrical cables and Cable Connectors – Inspect for corrosion, fraying, chafing, kinks, untwisting, broken strands/wires, damaged pins (when disconnected); evidence of improper alignment.

(d) Flexible Hoses – Inspect for fraying, chafing, twisting, deterioration, proper routing and security; and evidence of leakage.

(e) Tubing and Ducting - Inspect for cracks, corrosion and security; evidence of leakage; and fittings and clamps for security and proper installation.

(f) Electrical/Electronic Equipment – Inspect for evidence of overheating; corrosion, proper bonding and security; defective vibration dampeners; corroded, damaged pins (when disconnected), terminals and connectors.

(g) Wiring and Wiring Components – Inspect for evidence of overheating, chafing, fraying, deterioration, fluid damage and proper routing. Inspect splices and terminals for corrosion and security; connectors for security, damaged pins and deteriorated potting (when disconnected).

(h) Instruments – Inspect for evidence of overheating of electrical units; damaged faceplates, interference with moving parts, security of units and attached wiring, hoses and tubing.

(i) Operational tests shall be performed on each item to be repaired to validate reported discrepancies and to aid in the determination of required rework and repairs. The scope of the operational tests shall be of sufficient depth to fault isolate defective components and to verify replacement or repair.

3.1.2 The contractor shall provide annual preventative maintenance of the equipment listed in SOW paragraph 1.0. The annual preventative maintenance shall consist of the following:

(a) Blow Out Radiator
(b) Change Engine Oil and Replace All Filters
(c) Check Engine Belts for Condition and proper tensions
(d) Check Dash Gauges for Operation
(e) Check Battery and Connections
(f) Check Engine for Operation
(g) Clean Grease Fittings, Suspension Components & lube
(h) Check All Fluid Levels (where applicable)
(i) Check Steering for Operation
(j) Check Brakes for functionality and Operation
(k) Check all Lights
(l) Check Safety equipment for Correct Operation
(m) Check tires and Wheels
(n) Perform Operational check and Physical Inspection
(o) Inspect Battery and Check Electrolyte Level
(p) Top off coolant, brake, windshield wiper fluid levels.
(q) Set all tires to correct air pressure.

3.2 Repair Support

Upon notification of equipment failure by cognizant Government personnel, the contractor shall respond within 2 business days to troubleshoot the equipment by identifying the symptoms of the failure and isolating the problem to a particular component or group of components. The contractor shall then test suspected component(s) and submit a quote **(CDRL A001)** detailing the cost estimate to repair the failed

component(s). Any repairs beyond the maintenance specified in this contract shall be addressed through separate purchase orders.

3.3 Maintenance and Repair Reports

After completion of each maintenance and repair action, the contractor shall submit a Maintenance Service Report **(CDRL A002)** detailing the specifics of the maintenance and/or repair action that was completed by the contractor. The report shall contain a brief summary of all work accomplished, to include both negative and positive results including parts/components replaced and a summary of test results.

3.4 Option Year One

The list of equipment that this Contract applies to shall be updated near the end of base year with no guarantee on the minimum amount of equipment. The Vendor shall then provide a quote based upon the revised list and the Government will decide whether to proceed with the next option year (OY). The Government shall provide the updated list no later than 60 days prior to the option year. The contractor shall provide a quote for equipment maintenance and repair for the list of equipment. **(CDRL A003)** Work shall be performed per SOW paragraphs 3.1 through 3.3.

3.5 Option Year Two

The list of equipment that this Contract applies to shall be updated near the end of Option Year 1 with no guarantee on the minimum amount of equipment. The Vendor shall then provide a quote based upon the revised list and the Government will decide whether to proceed with the next OY. The Government shall provide the updated list no later than 60 days prior to the option year. The contractor shall provide a quote for equipment maintenance and repair for the list of equipment. **(CDRL A003)** Work shall be performed per SOW paragraphs 3.1 through 3.3.

4.0 GOVERNMENT FURNISHED PROPERTY

4.1 Government Furnished Equipment (GFE)

The Government will provide the equipment listed in Paragraph 1.0 for maintenance listed in this SOW.

4.2 Government Furnished Information (GFI):

GFI in the form of the operating and technical manuals for the equipment listed in SOW paragraph 1.0 shall be provided no later than five (5) days after award of purchase order. Any additional GFI will be provided no later than 3 days after formal request by the Contractor. Disposition of GFI will be made at purchase order completion.

4.3 Access to Government Facilities

The Government will provide the contractor access to Government facilities to accomplish statement of work tasking. The Contractor shall provide a list of employees who require access to these areas,

including standard security clearance information for each person, to the Procuring Contracting Officer (PCO) no later than three business days after the date of award. Access to Government buildings at Naval Support Activity Panama City (NSA PC) is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0700 to 1700, Monday through Friday. Contractor employees shall be under Government oversight at all times.

Government oversight requires that a Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this task order. Contractor personnel are not allowed to access any Government buildings at NSA PC outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO). When a Government facility is closed or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and departure directions given to Government personnel.

5.0 DATA DELIVERABLES

Data shall be provided in accordance with the Contract Data Requirements List (CDRL) DD Form 1423.

6.0 PERIOD OF PERFORMANCE

The period of performance for this purchase order shall be from date of issuance through one (1) year after date of award. This procurement includes two (2) 1-year options.

7.0 SECURITY

This task involves access to Controlled Unclassified Information (CUI). Performance under this contract shall NOT require access to nor generate CLASSIFIED information.

7.1 Release of Information

(a) Release of information shall be in accordance with Section I, DFARS Clause 252.204-7000, Disclosure of Information.

(b) All technical data provided to the contractor by the Government shall be protected from public disclosure in accordance with the markings contained thereon. All other information relating to the items to be delivered or services to be performed under this task order may not be disclosed by any means without prior approval of the appropriate NSWC PCD authority. Dissemination or public disclosure includes, but is not limited to, permitting access to such information by foreign nationals or by any other person or entity; publication of technical or scientific papers; advertising; or any other proposed public release. The contractor shall provide adequate physical protection to such information to preclude access by any person or entity not authorized such access by the Government.

7.2 Controlled Unclassified Information (CUI)

Controlled unclassified information (CUI) is official information that requires the application of controls and protective measures for a variety of reasons and has not been approved for public release, to include

technical information, proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts. CUI is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 13526, but is (a) pertinent to the national interest of the United States or to the important interests of entities outside the Federal Government, and (b) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

7.3 Minimum Requirements for Access to Controlled Unclassified Information (CUI)

Access to CUI, user level access to DON or DoD networks and information systems, system security and network defense systems, and to system resources providing visual access and/or ability to input, delete or otherwise manipulate sensitive information without controls to identify and deny sensitive information, requires security clearance eligibility, based on a Tier 3 Background Investigation, and a favorable adjudication by the Defense Counterintelligence and Security Agency, Consolidated Adjudications (DCSA CAS), or Interim/Temporary access to CUI based on a determination by the NSWC PCD Security Manager based on a favorable review of an individuals completed Electronic Questionnaire for Investigation Processing (SF 86), and favorable FBI fingerprint results. Contact NSWC PCD Personnel Security (NSWCPCD_PERSEC@us.navy.mil) for initiation of the SF86 and FBI fingerprinting, the CUI determination, and validation that employees have the required eligibility, prior to providing access to CUI.

7.4 Minimum Protection Requirements for Controlled Unclassified Information

Security classification guides and unclassified limited documents (e.g., CUI, Distribution Statement Controlled) are not authorized for public release and, therefore, cannot be posted on a publicly accessible webserver or transmitted over the Internet unless appropriately encrypted.

7.5 CUI

CUI is a designation, not a classification. CUI is used by Department of Defense (DoD) and a number of other federal agencies to identify information or material, which although unclassified, disclosure to the public of the information would reasonably be expected to cause a foreseeable harm to an interest protected by one or more provisions of the FOIA. This includes information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended. CUI must be marked, controlled and safeguarded in accordance with DoDI 5200.48, DoD Information Security Program: Controlled Unclassified Information (CUI).

7.6 Security of Unclassified DoD Information on Non-DoD Information Systems (DoDI 8582.01) DoD Policy

7.6.1 DoD Policy

Adequate security shall be provided for all unclassified DoD information on non-DoD information systems. Appropriate requirements shall be incorporated into all contracts, grants, and other legal agreements with non-DoD entities.

Information Safeguards are applicable to unclassified DoD information in the possession or control of non-DoD entities on non-DoD information systems, to the extent provided by the applicable contract, grant, or other legal agreement with the DoD.

7.6.2 **Information Safeguards**

Unclassified DoD information that has not been cleared for public release may be disseminated by the contractor, grantee, or awardee to the extent required to further the contract, grant, or agreement objectives, provided that the information is disseminated within the scope of assigned duties and with a clear expectation that confidentiality will be preserved. Examples include:

a. Non-public information provided to a contractor (e.g., with a request for proposal).

b. Information developed during the course of a contract, grant, or other legal agreement (e.g., draft documents, reports, or briefings and deliverables).

c. Privileged information contained in transactions (e.g., privileged contract information, program schedules, contract-related event tracking).

Note: It is recognized that adequate security will vary depending on the nature and sensitivity of the information on any given non-DoD information system. However, all unclassified DoD information in the possession or control of non-DoD entities on non-DoD information systems shall minimally be safeguarded as follows:

a. Do not process unclassified DoD information on publicly available computers (e.g., those available for use by the general public in kiosks or hotel business centers).

b. Protect unclassified DoD information by at least one physical or electronic barrier (e.g., locked container or room, logical authentication or logon procedure) when not under direct individual control of an authorized user.

c. At a minimum, overwrite media that have been used to process unclassified DoD information before external release or disposal.

d. Encrypt all information that has been identified as CUI when it is stored on mobile computing devices such as laptops and personal digital assistants, compact disks, or authorized removable storage media such as thumb drives and compact disks, using the best encryption technology available to the contractor or teaming partner.

e. Limit transfer of unclassified DoD information to subcontractors or teaming partners with a need to know and obtain a commitment from them to protect the information they receive to at least the same level of protection as that specified in the contract or other written agreement.

f. Transmit e-mail, text messages, and similar communications containing unclassified DoD information using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include

closed networks, virtual private networks, public key-enabled encryption, and transport layer security (TLS).

g. Encrypt organizational wireless connections and use encrypted wireless connections where available when traveling. If encrypted wireless is not available, encrypt document files (e.g., spreadsheet and word processing files), using at least application-provided password protected level encryption.

h. Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

i. Do not post unclassified DoD information to website pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to website pages that control access by user identification and password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies during transmission. Access control may be provided by the intranet (vice the website itself or the application it hosts).

j. Provide protection against computer network intrusions and data exfiltration, minimally including:

   (1) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

   (2) Monitoring and control of both inbound and outbound network traffic (e.g., at the external boundary, sub-networks, individual hosts), including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

   (3) Prompt application of security-relevant software patches, service packs, and hot fixes.

k. Comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, proprietary, critical program information (CPI), personally identifiable information, export controlled) as specified in contracts, grants, and other legal agreements.

l. Report loss or unauthorized disclosure of unclassified DoD information in accordance with contract, grant, or other legal agreement requirements and mechanisms.

m. Do not use external IT services (e.g., e-mail, content hosting, database, document processing) unless they provide at least the same level of protection as that specified in the contract or other written agreement.

7.7 Operations Security

Operations Security (OPSEC) is concerned with the protection of critical information: facts about intentions, capabilities, operations, or activities that are needed by adversaries or competitors to bring about failure or unacceptable consequences of mission accomplishment.

Critical information includes information regarding:

- Operations, missions, and exercises, test schedules or locations;
- Location/movement of sensitive information, equipment, or facilities;
- Force structure and readiness (e.g., recall rosters);
- Capabilities, vulnerabilities, limitations, security weaknesses;
- Intrusions/attacks of DoD networks or information systems;
- Network (and system) user IDs and passwords;
- Movements of key personnel or visitors (itineraries, agendas, etc.); and
- Security classification of equipment, systems, operations, etc.

The contractor, subcontractors and their personnel shall employ the following countermeasures to mitigate the susceptibility of critical information to exploitation, when applicable:

- Practice OPSEC and facilitate OPSEC awareness;
- Immediately retrieve documents from printers accessible by the public;
- Shred sensitive and Controlled Unclassified Information (CUI) documents when no longer needed;
- Protect information from personnel without a need-to-know;
- When promulgating information, limit details to that essential for legitimacy;
- During testing and evaluation, practice OPSEC methodologies of staging out of sight, desensitization, or speed of execution, whenever possible.

8.0 GOVERNMENT AND CONTRACTOR RELATIONSHIP

(a) The services to be delivered under this Task Order are non-personal services and the parties recognize and agree that no employer-employee relationship exists or will exist under the Task Order between the Government and the Contractor's personnel. It is, therefore, in the best interest of the Government to afford both parties a full understanding of their respective obligations.

(b) All Contractor, Subcontractor, and consultant personnel shall wear prominently displayed identification badges at all times when performing work on NSWC PCD property or attending meetings in the performance of this Task Order. The badge shall contain the individual's name, the company name and logo. When participating in such meetings (e.g., as a speaker, panel member), those individuals in Contractor employ must supplement physical identification (e.g., badges, place markers) with verbal announcements so that it is clear to the assembled group that they are employees of the Contractor, not NSWC PCD employees. In addition, when working on NSWC PCD property, all Contractor, Subcontractor, and consultant personnel shall have signs visible on their desks or at their work sites that clearly state that they are not NSWC PCD employees.

(c) The Contractor is responsible for supervision of all Contractor personnel assigned to this Task Order. The Contractor shall exercise ultimate over all aspects of Contractor personnel day-to-day work under this Task Order including the assignment of work, means and manner of Contractor employee performance and the amount of Contractor supervision provided. The Contractor shall be ultimately responsible for all aspects of performance under this Task Order including the work of its Contractor personnel.

Contractor personnel under this Task Order shall not:

(1) Be placed in a position where they are under the supervision, direction, or evaluation of a

Government employee.

(2) Be placed in a position of command, supervision, administration or control over Government personnel, or over personnel of other Contractors under other NSWC PCD contracts, or become a part of the Government organization.

(3) Be used in administration or supervision of Government procurement activities.

(4) Have access to proprietary information belonging to another without the express written permission of the owner of that proprietary information.

(d) Employee Relationship:

(1) The services to be performed under this Task Order do not require the Contractor or its personnel to exercise personal judgment and discretion on behalf of the Government. Rather the Contractor's personnel will act and exercise personal judgment and discretion on behalf of the Contractor.

(2) Rules, regulations, directives and requirements that are issued by the U.S. Navy and NSWC PCD under its responsibility for good order, administration, and security are applicable to all personnel who enter the Government installation or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with non-personal services Task Order.

(e) Inapplicability of Employee Benefits: This Task Order does not create an employer-employee relationship. Accordingly, entitlements and benefits applicable to such relationships do not apply.

(1) Payments by the Government under this Task Order are not subject to the Federal income tax withholdings.

(2) Payments by the Government under this Task Order are not subject to the Federal Insurance Contributions Act.

(3) The Contractor is not entitled to unemployment compensation benefits under the Social Security Act, as amended, by virtue of performance of this Task Order.

(4) The Contractor is not entitled to workman's compensation benefits by virtue of this Task Order.

(5) The entire consideration and benefits to the Contractor for performance of this Task Order are contained in the provisions for payment under this Task Order.

(f) Notice. It is the Contractor's, as well as, the Government's responsibility to monitor Task Order activities and notify the Contracting Officer if the Contractor believes that the intent of this clause has been or may be violated.

(1) The Contractor should notify the Contracting Officer in writing promptly, within three (3) calendar days from the date of any incident that the Contractor considers to constitute a violation of this clause. The notice should include the date, nature, and circumstances of the conduct, the name, function and activity of each Government employee or Contractor official or employee involved or knowledgeable about such conduct, identify any documents or substance of any oral communication involved in the conduct, and the estimate in time by which the Government must respond to this notice to minimize cost, delay or disruption of performance.

(2) The Contracting Officer shall promptly, within five (5) calendar days after receipt of notice,

respond to the notice in writing. In responding, the Contracting Officer will either:

(i) confirm the conduct is in violation and when necessary direct the mode of further performance,

(ii) countermand any communication regarded as a violation

(iii) deny that the conduct constitutes a violation and when necessary direct the mode of further performance; or

(iv) in the event the notice is inadequate to make a decision, advise the Contractor what additional information is required, and establish the date by which it should be furnished by the Contractor and the date.

9.0 DISTRIBUTION LIMITATION STATEMENT

Distribution Statements and Warning Notices: *The Contractor shall place the appropriate Distribution Statement on information associated/generated with this contractual effort, per the applicable Security Classification Guide, and carry forward the markings on documents provided by the government, along with the following statements on all technical documents/media, as applicable.*

WARNING - THIS DOCUMENT CONTAINS TECHNICAL DATA WHOSE EXPORT IS RESTRICTED BY THE ARMS EXPORT CONTROL ACT (SECTION 2751 OF TITLE 22, UNITED STATES CODE) OR THE EXPORT CONTROL REFORM ACT OF 2018 (CHAPTER 58 SECTIONS 4801-4852 OF TITLE 50, UNITED STATES CODE). VIOLATIONS OF THESE EXPORT LAWS ARE SUBJECT TO SEVERE CRIMINAL PENALTIES. DISSEMINATE IN ACCORDANCE WITH PROVISIONS OF DOD DIRECTIVE 5230.25 AND DOD INSTRUCTION 2040.02.

DESTRUCTION NOTICE - CLASSIFIED INFORMATION, DESTROY IN ACCORDANCE WITH SECNAVINST 5510.36, (DON INFORMATION SECURITY PROGRAM) OR NISPOM RULE. UNCLASSIFIED LIMITED DOCUMENTS, (E.G., CUI, DISTRIBUTION STATEMENT CONTROL) DESTROY PER DODI 5200.48.

--- END OF STATEMENT OF WORK ---