STATEMENT OF WORK
FOR
SDV MK11 PILLAR STERN PLANES AND MOUNT STABILITY FINS

1.0 SCOPE

The Naval Surface Warfare Center Panama City Division, (NSWC PCD) requires contractor support to fabricate four Pillar Stern Planes and four Mount Stability Fins. The contractor shall provide all facilities, materials, and labor to accomplish Statement of Work tasking specified below.

1.1 Acronym List

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

CDRL	Contract Data Requirements List	CFR	Code of Federal Regulations
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	NATO	North American Treaty Organization
NDA	Non-Disclosure Agreement(s)	NSA PC	Naval Support Activity Panama City
ODC	Other Direct Cost	OEM	Original Equipment Manufacturer
OPSEC	Operations Security	PCO	Procuring Contracting Officer
PII	Personally Identifiable Information	PM	Program Manager
PSC	Product Service Code	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

(a) Teledyne Brown Engineering Drawing 8600006, Rev A – Pillar, Stern Plane – MK 11 SDV System (Attachment 1)
(b) Teledyne Brown Engineering Drawing 8600016 – Mount, Stability Fin – MK 11 SDV System (Attachment 2)

3.0 REQUIREMENTS

The Contractor shall provide all labor, equipment, parts, and consumables required to fabricate four Pillar Stern Planes and four Mount Stability Fins in accordance with all the Notes and requirements on Teledyne Brown Engineering Drawings 8600006 and 8600016. Any deviation without prior approval will result in rejection. Each assembly shall be individually wrapped, boxed, labeled, and shipped to NSWC PCD.

For all shipments, the Shipping customer service hours in Building 399 are:

Mon-Thurs: 0715-1430 (General Cargo)
Mon-Thurs: 0715-1200 (Classified)
Fri: 0715-1200 (General Cargo ONLY)

To make special arrangements in order to drop off outside the hours listed above, please contact the Property Management Transportation Officer.

3.1 Monthly Status Report

The contractor shall prepare a monthly status report that documents the status of contractor effort towards achieving contract objectives. The report shall identify accomplishments to date and difficulties encountered, and compare the status achieved to planned goals and the resources expended. (CDRL A001)

4.0 GOVERNMENT FURNISHED PROPERTY

4.1 Government Furnished Equipment (GFE): None

4.2 Government Furnished Information (GFI): Drawings will be provided for fabrication purposes.

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

Base Period of Performance: The items shall be delivered no later than 30 days after receipt of award.

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 DoW 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 (DoW) 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 DoWI 5200.48, DoW Information Security Program: Controlled Unclassified Information (CUI).

7.6 Security of Unclassified DoW Information on Non-DoW Information Systems (DoWI 8582.01) DoW Policy

7.6.1 DoW Policy

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

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

7.6.2 Information Safeguards

Unclassified DoW 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-DoW information system. However, all unclassified DoW information in the possession or control of non-DoW entities on non-DoW information systems shall minimally be safeguarded as follows:

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

b. Protect unclassified DoW 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 DoW 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 DoW 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 DoW 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 DoW 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 DoW 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 DoW 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 DoW 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 DOW DIRECTIVE 5230.25 AND DOW 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 DOWI 5200.48.

--- END OF STATEMENT OF WORK ---