ANNEX 16 – STATEMENT OF WORK LANGUAGE IMPLEMENTING “THE DIB” MEMO

The following SOW language shall be used to supplement DFARS Clause 252.204-7012 entitled, “Safeguarding Covered Defense Information and Cyber Incident Reporting” where the Department of the Navy Program Manager, Program Executive Officer or Chief of Naval Research, in coordination with Resource Sponsor, determines that the risk to a critical program and/or technology warrants its inclusion.

1. *System Security Plan and Plans of Action and Milestones (SSP/POAM) Reviews*

a) Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor’s facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which is included in this contract. The Contractor shall fully cooperate in the Government’s review of the SSPs at the Contractor’s facility.

b) If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The contracting officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a plan of action and milestones (POAM) for the correction of the identified deficiencies. The Contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.

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

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

2. *Compliance to NIST 800-171*

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

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

(1) Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor

authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

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

(3) Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods.

(4) Audit user privileges on at least an annual basis;

(5) Implement:

i. Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POAM); and,

ii. NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program);

(6) Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.

(7) Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

3. *Cyber Incident Response:*

a) The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

b) Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx. In delivery of the incident data, the Contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

c) If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

4. ***Naval Criminal Investigative Service (NCIS) Outreach***

The Contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

5. ***NCIS/Industry Monitoring***

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

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

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