

PERFORMANCE WORK STATEMENT (PWS) – Attachment #1
Business Administrative Management & Consulting Services
Defense Innovation Unit

Part 1

General Information

1. General: This is a non-personnel services contract to provide scientific and technical consulting services. The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1.1 Description of Services/Introduction: The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform Professional Services - Business Administrative Services as defined in this Performance Work Statement except for those items specified as government furnished property and services. The contractor shall perform to the standards in this contract.

1.2 Background: The Defense Innovation Unit (DIU) is a fast-moving Department of Defense organization that contracts with commercial companies to solve national security problems. In July 2015, Ash Carter, Secretary of Defense issued Department of Defense (DoD) Directive 5105.85 to establish DIU.¹ Under Directive 5105.85, five main mission areas, were established to support the advancement of technology for DoD, Artificial Intelligence; Human Systems; Autonomy; Information Technology; and Space. Since then our Information Technology portfolio evolved into our Cyber portfolio and in October 2020, DIU launched a sixth technology portfolio: Advanced Energy and Materials (AE&M).

Our mission is twofold: The Defense Innovation Unit (DIU) strengthens our national security by accelerating the adoption of leading commercial technology throughout the military and by growing the national security innovation base (NSIB). During a year of challenging economic circumstances across the United States and the globe, it has become even clearer that the health and strength of our economy is essential to our prosperity as a nation and to our national security. The startups, established companies, venture capital firms, investors, and traditional defense contractors that DIU works with to deliver the best commercial technology to the Department of Defense (DoD) are not only fundamental sources of dual-use technologies but also the foundation of a strong U.S. economy and NSIB.

1.3 Objectives: The basic service objective is for DIU to have Professional Services/Business Administrative Services to support the six DIU portfolios (Artificial Intelligence; Human Systems; Autonomy; Cyber; Space; and AE&M) in solving national security problems.

¹ DoD Directive 5105.85 https://fas.org/irp/doddir/dod/d5105_85.pdf

1.4 Scope: The purpose of this contract is to provide the services included in MAS 541611, **Management and Financial Consulting, Acquisition and Grants Management Support, and Business Program and Project Management Services**. The services include providing operating advice and assistance on administrative and management issues. Examples include: strategic and organizational planning, business process improvement, acquisition and grants management support, facilitation, surveys, assessment and improvement of financial management systems, financial reporting and analysis, due diligence in validating an agency's portfolio of assets and related support services, strategic financial planning, financial policy formulation and development, special cost studies, actuarial services, economic and regulatory analysis, benchmarking and program metrics, and business program and project management. DIU requires non-personnel services in seven task areas (refer to PWS Section 5 for the tasks associated with the tasks):

- Task 1: Administration
- Task 2: Program Management
- Task 3: Finance
- Task 4: IT Services (ancillary)
- Task 5: Portfolio Support
- Task 6: Security & Facilities Management
- Task 7: Strategic Engagement

1.5 Period of Performance: The period of performance shall be for one (1) Base Year of 12 months and four (4) 12-month option years. The Period of Performance reads as follows:

1.6 Quality Assurance.

1.6.1 Quality Assurance Surveillance Plan. The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Contractor must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.6.2. Contractor Quality Control Plan. The contractor will be responsible for developing a Contractor Quality Control Plan, to incorporate at time of award, in order to ensure they have systematic methods to monitor performance and to identify the required documentation and the resources to be employed to meet the **Acceptable Quality Level (AQL)** as described in Technical Exhibit 1. At a minimum, the QCP must include a self-inspection plan, an internal staffing plan, and an outline of the procedures that the Contractor will use to maintain quality, timeliness, responsiveness, customer satisfaction, and any other requirements set forth in this PWS. The QCP is to be delivered within 30 days after contract award. After acceptance of the quality control plan the contractor shall receive the contracting officer's acceptance in writing of any proposed change to the QC system. **(Deliverable)**

1.6.3 Monthly Status Report: The contractor shall provide a Monthly Status Report (MSR). The MSR shall outline the most current status of the task order. The MSR shall list, the accomplishments of each active task during a reporting period. The report shall list all problem areas and items requiring Government action. The MSR shall contain a report of the costs incurred to date and whether they comply with the contract delivery schedule. The MSR format will be agreed upon by

the COR and the MSR and shall contain, but not be limited to, the below information. The MSR is due monthly, within seven (7) business day of the following month. The final MSR is due on the last day of the contract. **(Deliverable)**

- Activities to include meetings attended, results, and deliverables by task
- Travel data for trips completed and planned, to include name of traveler, trip location, purpose, estimated/actual travel costs, and dates of travel
- Meetings attended with a summary of relevant items discussed
- Proposed activities
- Open issues/problem areas
- Key personnel changes

1.6.4 Quarterly In-Process Reviews: If determined necessary by the Contracting Officer Representative, the contractor shall coordinate with the government to schedule and conduct Quarterly In-Progress Reviews (IPRs), during each period of performance to summarize status, progress, recommendations, and concerns regarding task development and/or required documentation. Presentation materials shall be prepared and provided to the COR five (5) business days prior to the IPR. The contractor shall deliver IPR minutes within five (5) business days after IPR. At a minimum, IPR meeting minutes should reflect a record of discussion activity, decisions made, date, locations, and attendees.

The contractor is responsible to ensuring all Portfolio Leads, Managers, and Executive Leadership can attend the IPR in person or via VTC. For estimating purposes, there are roughly 20 government leads that will be attending the IPR. The IPR shall be held within fifteen (15) business days after concluding a United States government fiscal year quarter.

1.7 Location and Operations

1.7.1 Place of Performance: The direct support to be performed under this contract will be performed in Government provided office space in San Francisco, CA; Boston, MA; Austin, TX and in the Washington DC National Capital Region (NCR). Remote work is a possibility in some circumstances, more information will be provided during the solicitation phase.

1.7.2 Telework. The Government may permit telecommuting (telework) to contractors when determined to be in the best interest of the Government in meeting work requirements. The DIU Government Staff Lead will approve telecommuting (telework) for contractors based on DIU requirements. Telecommuting will be at no additional cost to the Government. Prior to approving telework, contractors will be required to take Telework Fundamentals - Employee Training provided by <https://www.telework.gov/training-resources/telework-training/virtual-telework-fundamentals-training-courses/>.

1.7.3 Hours of Operation. Normal workdays are Monday through Friday except US Federal Holidays. Core business hours of work are from 8:00/9:00AM to 4:00/5:00 PM daily. The government expects every contractor on site during these hours. However, due to the nature of DIU there will be times when the contractor is expected to work outside of the normal business hours in support of critical DIU requirements. For any work that deviates from the core hours, the contractor must have an email approval from the applicable DIU program manager when work is required outside of core business hours. The government will identify the DIU program managers at the contract kick-off meeting.

Notwithstanding the above, contractor personnel shall not work more than 80 hours in a two-week period and monthly invoicing will not exceed 160 hours per position. The contractor is responsible for ensuring that contractors are not exceeding 160 hours per position per month.

1.7.4 Administrative Leave. When the government grants administrative leave to government employees, or is closed as a result of inclement weather, potentially hazardous conditions, or other special circumstances, contractor personnel

working at the specific facility/location granted administrative leave may also be dismissed at the discretion of the On-site Manager to the extent that the overall performance is not adversely impacted. The contractor shall at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the government facility is not closed for the above reasons. Contractor personnel may be requested to work at the Government's alternate locations during emergencies and emergency exercises. Individual Contractor personnel may be designated as essential personnel to support contingency operations at alternate Government locations during actual emergencies and emergency exercises.

1.7.5 Contractor Schedule. When deemed necessary by the COR, the contractor shall provide the COR a current schedule for its entire staff assigned to the contract, including planned leave. This schedule shall be updated monthly and provided in the monthly status report. The contractor shall assign alternates to cover assignments of any of its staff that are absent sufficient to ensure that the services are not disrupted. The government is not responsible for tracking contractor personal or sick time off. **(Deliverable)**

1.7.6 Recognized Holidays: Contractor personnel are not required to work during Federal Holidays

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

1.8 Type of Contract: The government will award one Firm Fixed-Price order in accordance with FAR Subpart 8.405-2 – Ordering Procedures for Services Requiring a Statement of Work.

1.9 Security Requirements:

1.9.1 Clearance Type. The contractor personnel will be required to access Secret, Top Secret (TS) and TS-Sensitive Compartmented Information (TS-SCI) at time of award and throughout the performance of this contract. Specific security requirements are identified in the DD Form 254, DOD Contract Security Classification Specification. Refer to Attachment 1, DD Form 254 for additional information.

1.9.2 Security Clearance Process. The Contractor shall submit the security nomination packages for the personnel assigned to the task order no later than 3-5 calendar days following issuance of the award document.

In the event that contractor personnel cannot maintain their required clearance, as outline in Technical Exhibit 2, and another candidate cannot be staffed within 15 business days, the Government may remove the specific labor category from the contract and resolicit the labor category.

1.10 Safeguarding. The Contractor shall be responsible for safeguarding all Government equipment, information and property provided for Contractor use. At the close of each work period, Government facilities, equipment, and materials shall be secured.

1.11 Special Qualifications: Refer to Section 5 of PWS

1.12 Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the contracting officer will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

1.13 Contracting Officer Representative (COR): The (COR) will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract: perform inspections necessary in connection with contract performance: maintain written and oral communications with the Contractor concerning technical aspects of the contract: issue written interpretations of technical requirements, including Government drawings, designs, specifications: monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

1.14 Key Personnel: Key Personnel are defined as certain skilled experienced professionals and/or technical personnel essential for successful contractor accomplishment of the work to be performed under this contract. Each Key Personnel should include a resumes submitted for evaluation of the proposal. The contractor agrees that such personnel shall not be removed from the contract work or replaced without compliance with paragraphs (1.14.1) and (1.14.2) hereof. Refer to Technical Exhibit 2, for annotated Key Personnel Positions.

1.14.1 If one or more of the key personnel for whatever reason becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding thirty (30) calendar days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor shall immediately notify the Contracting Officer and shall, subject to the concurrence of the Contracting Officer or his authorized representative, promptly replace such personnel with personnel of at least substantially equal ability and qualifications.

1.14.2 All requests for approval of substitutions hereunder must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitutions. They must contain a complete resume for the proposed substitute, and any other information requested by the Contracting Officer or needed by him to approve or disapprove the proposed substitution. The Contracting Officer or his authorized representative will evaluate such requests and promptly notify the contractor of his approval or disapproval thereof in writing.

1.14.3 If the Contracting Officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated or have otherwise become unavailable for the contract work is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the services ordered, the contract may be terminated by the Contracting Officer for default or for the convenience of the Government, as appropriate, or, at the discretion of the Contracting Officer if he finds the contractor at fault for the condition, the contract price or fixed fee may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage.

1.15 Identification of Contractor Employees: All contract personnel attending meetings, answering Government telephones, and working in other situations where their Contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by Contractors are suitably marked as Contractor products or that Contractor participation is appropriately disclosed. Contractor personnel will be required to obtain, use, and display a Common Access Card in the performance of this service. The COR will provide titles during the Transition Phase. The titles shall also be included in contractor emails sent on behalf of DIU. Contractor email signatures shall be standard and consistent for current and future contractor employees.

1.16 Contractor Travel. All travel costs are in accordance with Federal Acquisition Regulation (FAR) Part 31.205-46 Travel Costs. **All travel within 50 miles of the position location, Mountain View, CA; Austin, TX, Boston, MA; or the Washington DC National Capital Region (NCR) is included in the price of this contract.** When movement of contractor personnel is required locally (i.e., Metro) costs will be borne by the contractor. **Travel requests outside of the 50-mile radius requires a Trip Authorization, which shall be submitted to the COR at least two weeks prior to the travel start date and a subsequent Trip Voucher, to be submitted with the monthly invoice. Authorizations and Vouchers shall be submitted through a Travel Management System, which is in accordance with the Federal Travel Regulation (FTR), Joint Travel Regulation (JTR) (Refer to 1.16.1).** For this contract, per FAR Subpart Part 31.205-46(a)(1), costs for transportation will be based on actual costs incurred provided the method used results in a reasonable charge, the cost a prudent person would pay. Costs for lodging, meals, and incidental expenses based on per diem. Contractor travelers are required to exercise the same care in incurring expenses that a prudent person would exercise if traveling on personal business when making official travel arrangements, and therefore, should consider the least expensive class of travel that meets their needs

1.16.1 Travel Management: The contractor is responsible for having **Travel Management Service** (e.g., Concur, TripActions, etc.) for their contractor personnel. The travel management service will require at a minimum, booking, and fulfillment of airline tickets, lodging, and car rentals, which must be in accordance with the Federal Travel Regulation (FTR), Joint Travel Regulation (JTR). The travel agent service fee should be comparable to the GSA pricing provided by Contract #: GS-33F-0022P, CW Government Travel, Inc., September 16, 2019.²

1.16.2 All travel request shall be submitted to the COR via their **Travel Management Service** in accordance with the provisions of the Federal Travel Regulation (FTR), Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. Each travel request shall include:

Trip Authorization: The government will reimburse the contractor for all other travel outside the 50-mile limitation that was authorized in advance by the Contracting Officer Representative, for reasonable travel related expenses. Each Trip Authorization shall include:

- Contractor Contact Information
- Date and place (city, town, or other similar designation) of the expenses
- Detailed purpose of the trip
- Estimated Expenses
- Travel Costs
- Lodging Costs

² CW Government Travel, Inc. https://www.gsaadvantage.gov/ref_text/GS33F0022P/0V9MP9.3QZZO0_GS-33F-0022P_CWTTSSCATALOG03302020.PDF

Trip Voucher: The contractor shall be reimbursed for actual allowable, allocable, and reasonable travel costs incurred during performance of this effort in accordance with the Federal Acquisition Regulation (FAR) Part 31.205-46 Travel Costs. The trip vouchers shall be submitted with the monthly invoice using the Invoice, Receipt, Acceptance, and Property Transfer (iRAPT) application, part of the Wide Area Workflow e-Business Suite. Each Trip Voucher shall include receipts for expenses over \$75.00, including Hotel, Airline, and Rental Car Receipts

1.16.3 Monthly Travel Report (Deliverable)

A monthly Travel Report is required to document the travel performed by the contractor. The COR will work with the Contractor PM to determine the best data to include at the kick-off meeting.

1.17 Other Direct Costs: Travel. Refer to PWS 1.6.13 and Technical Exhibit 2

1.18 Data Rights. The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the Contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.19 Organizational Conflict of Interest: Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI. **Disclosure of Information:** Information made available to the contractor by DIU for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer. (KO) The contractor agrees to assume responsibility for protecting the confidentiality of DIU records, which are not public information. Each contractor or employee of the contractor to whom information may be made available or disclosed shall be notified in writing by the contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

1.20 Contract Management

Refer to Program Manager Role (Section 5 of PWS)

1.21 Phase in Phase Out Period Transition (Deliverable)

The Government is not funding a separate phase-in period but expects the incumbent Contractor and incoming Contractor to work together to ensure a smooth transition.

Phase-in: The contractor shall adhere to the detailed transition plan submitted as part of their proposal. At a minimum, the contractor shall include start-up activities that may have to transition to full operational capability upon conclusion of the transition period. The contractor will be required to provide a Phase-in Transition Plan Report from their proposal 20 calendar days after award.

- Provide a detailed transition methodology in logical sequence to ensure a smooth transition of all tasks/subtasks of the contract without interruption or degradation of service levels
- Provide a timeline for completion
- Identify associated risks and issues and risk mitigation strategies

Phase-out plan will include, but is not limited to, the items listed below. The contracting officer or COR will notify the contractor within 5 business days after receipt of a complete phase-out plan of the acceptability of the proposed phase-out plan. The contractor shall overlap with incoming Contractor during transition for 30 calendar days and will work with government personnel and the incoming contractor to transfer knowledge, information, and documentation for all projects and tasks related to this contract. The information and documentation to be transferred includes but is not limited to:

- Current and on-going work products (emails, briefings, papers)
- Point of Contact information required for day-to-day business purposes
- Comprehensive historical summaries of each portfolio
- Comprehensive current state-of-play summaries for each portfolio
- White papers outlining suggested next steps for all portfolios.

Note: All automated data files in the possession of the contractor are the property of the government and shall be turned over to the contracting officer or COR at the completion or termination of the contract. And all records related to the execution of the contract shall be returned to the government as electronic copies that are readable and accessible by the government

1.22 Onboarding Contractor Personnel

1.19.1 All contractor personnel will be required to complete the Cyber Awareness Challenge **once per year**. <https://public.cyber.mil/training/cyber-awareness-challenge/>. Further, prior to approving telework, contractors will be required to take Telework Fundamentals - Employee Training provided by <https://www.telework.gov/training-resources/telework-training/virtual-telework-fundamentals-training-courses/>. Lastly, there may be additional training after a contractor is onboard, which is directed by Office of the Secretary of Defense (OSD). If OSD directs any training, contractors will be required to take the training in order to continue working for DIU.

1.19.2 Onboarding procedures will be provided by the DIU Human Resources team. In addition to the onboarding program HR will provide, prior to starting with DIU, Contractors will be required to sign the following forms:

- DIU Acceptable Use Policy

- Nondisclosure Agreement and Conflict of Interest
- Disqualification Statement

DRAFT

PART 2

DEFINITIONS & ACRONYMS

2. Definitions and Acronyms:

2.1. DEFINITIONS: *[List any terms used within the PWS that require further definition. At a minimum, insert the definitions provided below].*

2.1.1. CONTRACTOR. A supplier or vendor awarded a contract to provide specific supplies or service to the government. The term used in this contract refers to the prime.

2.1.2. CONTRACTING OFFICER. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.

2.1.3. CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.4. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.5. DELIVERABLE. Anything that can be physically delivered, but may include non-manufactured things such as meeting minutes or reports.

2.1.6. KEY PERSONNEL. Contractor personnel that are evaluated in the technical review process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.7. PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

2.1.8. QUALITY ASSURANCE. The government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.9. CONTRACTOR QUALITY CONTROL PLAN (CQCP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.10. QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.11. SUBCONTRACTOR. One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.1.12. WORK DAY. The number of hours per day the Contractor provides services in accordance with the contract.

2.1.12. WORK WEEK. Monday through Friday, unless specified otherwise.

2.2. ACRONYMS: *[List all acronyms used in the PWS and what they represent. At a minimum, insert the acronyms provided below].*

ACOR	Alternate Contracting Officer's Representative
BCTF	Boards, Commissions, and Task Forces
CFR	Code of Federal Regulations
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-the-Shelf
DD Form 254	Department of Defense Contract Security Requirement List
DFARS	Defense Federal Acquisition Regulation Supplement
DMDC	Defense Manpower Data Center
DOD	Department of Defense
EM	Enterprise Management Directorate
FAR	Federal Acquisition Regulation
HIPAA	Health Insurance Portability and Accountability Act of 1996
KO	Contracting Officer
OCI	Organizational Conflict of Interest
OCNUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QC	Quality Control
QCP	Quality Control Program
TE	Technical Exhibit
WHS	Washington Headquarters Services

PART 3

GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED ITEMS AND SERVICES: The contractor will be responsible for tracking GFE, for each contractor on the contract. An ad hoc report for the equipment assigned to each contractor will be required when the COR deems necessary. The report should include at a minimum, name of contractor, the equipment assigned to the contractor and the date of when the equipment was acquired and a date when the equipment was returned. **(Deliverable)**

3.2 Facilities: DIU will provide the necessary workspace for the Contractor staff to provide direct support outlined in the PWS to include desk space and/or allow telework or remote work.

3.3 Utilities: DIU will provide the Contractor access to the applicable Local Area Network(s)

3.4 Equipment: The Government will provide, Common Access Cards (CACs), phones, computers, and multi-functional devices for daily work. Multi-functional devices will only be available at the government locations.

PART 4

CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 General: The Contractor shall furnish all supplies, equipment, facilities and services required to perform work under this contract that are not listed under Section 3 of this PWS.

4.2 Top Secret Facility Clearance: The Contractor shall possess and maintain a Top Secret facility clearance from the Defense Counterintelligence and Security Agency. The Contractor's employees performing work in support of this contract shall have been granted a Secret, Top Secret, or Top Secret/Sensitive Compartmented Information Eligibility security clearance. The Government uses the DD Form 254 to convey security requirements to contractors when contract performance requires access to classified information. Prime contractors also use the DD Form 254 to convey security requirements to subcontractors that require access to classified information to perform on a subcontract. Subcontractors may also use the DD Form 254 if access to classified information is required to convey security requirements to additional subcontractors. The DD Form 254 will be provided with the solicitation.

PART 5
SPECIFIC TASKS

5. The Contractor shall provide contractor non-personnel services to support the seven task areas detailed in this section.

- Task 1: Administration
- Task 2: Program Management
- Task 3: Finance
- Task 4: IT Services (ancillary)
- Task 5: Portfolio Support
- Task 6: Security & Facilities Management
- Task 7: Strategic Engagement

5.1 Administration

- 5.1.1 The **Executive Administration** primary roles and responsibilities include executive administrative support by conducting research, preparing statistical reports, handling information requests, and performing clerical functions such as preparing correspondence, receiving visitors, arranging conference calls, and scheduling meetings. Tasks include:
- 5.1.1.1 Provide information, recommendations, and documentation in support of various office functions and special projects.
 - 5.1.1.2 Provide administrative support including but not limited to research and preparation of graphic presentations; word-processing, proofreading, filing, and database management; compile data of operating unit programs, policies, and procedures. Operating of the reception area, escorting guests, and visitors, creation of travel authorizations and vouchers using the authorized government travel system, and disbursement and collection of security badges. Input of time and attendance after receipt of Government employee timesheets, in the authorized government time and attendance system to be certified by a Government official.
 - 5.1.1.3 Develop reports and correspondence containing decisions of designated managers; assist in coordination and management with DIU's internal conference rooms, and supply management; perform office management functions to include program deal flow.
 - 5.1.1.4 Review and track action items as delegated.
 - 5.1.1.5 Compile reports and memorandum in support of the DIU office and executives
- 5.1.2 The **Human Capital Management** primary roles and responsibilities will be to provide mid-level clerical and administrative support for the Defense Innovation Unit. It is essential that the contractor have the ability to work in a fast paced environment, to provide administrative support to manage projects; prepare and edit correspondence; prepare reports and presentations; coordination and assist in preparing official government travel using the Defense Travel System (DTS) and knowledge of the Joint Travel Regulation (JTR); organize and maintain files and records; mail processing; office and facility space management; act as the activity security representative (ASR) and monitor the Correspondence and Task Management System (CATMS) tracking. Additionally, the contractor will support the areas of Human Resource and Military Personnel Management. Must know how to write Standard operating procedures. Tasks include:
- 5.1.2.1 Preparation of Correspondence and Reports.
 - 5.1.2.2 Coordinate office administrative functions including office security administration, processing security clearance and visit requests for DIU personnel and visitors, scheduling office events and ordering supplies.
 - 5.1.2.3 Assist with coordination and documentation of DIU physical space to ensure DIU requirements are captured to optimize the physical placement of the offices to ensure the efficient operation of the entire group.
 - 5.1.2.4 Maintain electronic copies, and paper as directed by the Government, of files of all office documents including

letters, memos, reports, and briefings. Maintain accountability of files and correspondence in the office, both in electronic and in paper form IAW WHS Administrative Instruction (IA) 15. Prepare and process Standing Operating Procedures (SOP).

- 5.1.2.5 In accordance with the Joint Travel Regulation (JTR), Defense Travel System (DTS) and R&E guidelines, assist in creating and amending authorizations (orders), and assist in vouchers (local and non-local) in DTS; Monitor submission of travel vouchers NLT 5 days after client return from travel;
 - 5.1.2.6 As required, maintain a travel tracker that includes the program supported for the trip, description of the purpose of travel, destination, departure/return dates, authorization Centrally Billed Account (CBA) and per diem estimates, final voucher amounts, and when a voucher is paid. This includes invitational orders. Travel being funded by an external organization must also be tracked. This report shall be frequently updated to maintain currency and should include forecasted travel for the duration of the current fiscal year.
 - 5.1.2.7 Assists in the maintenance of the DIU manpower rosters, phone rosters and space allocations.
 - 5.1.2.8 Monitor due dates and status of Active duty and Reserve personnel performance reports and award packages. Create and maintain a tracking system for all office tasking (both internal and external) and upcoming personnel changes. Assist Active Duty and Reserve personnel to identify/satisfy any required DoD-related training. Collect inputs from Active Duty and Reserve personnel.
- 5.1.3 The **Advisor to the Director** of DIU primary roles and responsibilities include reviewing and tracking the Director's organizational priorities and coordinating and/or managing execution amongst appropriate stakeholders to ensure they are achieved on schedule. Tasks include:
- 5.1.3.1 Oversee the Director's executive assistant to prioritize the Director's meeting, engagements, and travel schedule
 - 5.1.3.2 Reviewing and tracking the Director's organizational priorities and coordinating and/or managing execution amongst appropriate stakeholders to ensure they are achieved on schedule
 - 5.1.3.3 Reviewing and tracking daily action items for the Director and his direct reports as delegated
 - 5.1.3.4 Drafting correspondence, including email, letters, memoranda, personnel evaluations, etc. on
 - 5.1.3.5 behalf of the Director
 - 5.1.3.6 Reviewing and editing formal and official DoD documents as necessary
 - 5.1.3.7 Providing strategic support for public speaking roles, engagements, meetings, etc. by coordinating opportunities, proposing topics and remarks, and drafting agendas, read-aheads, and meeting materials with multiple stakeholders
 - 5.1.3.8 Preparing presentation slides for briefings and engagements with high-level stakeholders
 - 5.1.3.9 Providing information, recommendations, and documentation in support of various office functions and special projects
 - 5.1.3.10 Completing additional ad hoc assignments as required
 - 5.1.3.11 Managing All Hands programming
 - 5.1.3.12 Assisting with the annual leadership onsite, all DIU onsite, and Dining Out programming
 - 5.1.3.13 Collaborate with the Director of Organization Development, Director of Future Capabilities, and Director of Operations to implement implementing DIU's values and cultural aspirations
 - 5.1.3.14 Collaborate with the Strategic Engagement Team, Director of Future Capabilities, and Director of Policy to develop an action plan to prioritize and execute DIU's strategic vision
 - 5.1.3.15 Assisting with cross-functional capabilities as required, such as the development and implementation of a customer relationship management system

5.2 The **Program Management** primary roles and responsibilities will be to provide program management support services. Tasks include:

- 5.2.1 Complete responsibilities associated with phase in, phase out transition periods, on and off boarding, invoicing, security, travel, personnel time off request, etc.
- 5.2.2 Compile the contractor's staffing plan and update as necessary.

- 5.2.3 Conduct contractor personnel recruitment as necessary to attract, select, hire, and retain qualified personnel capable of successfully meeting the PWS requirements, to minimize any impact on contract performance.
 - 5.2.4 Compile executive summaries of events for distribution, monthly status reports of contract team's work, and schedule/coordinate ad hoc meetings
 - 5.2.5 Maintain familiarity with all Federal and Department policies with comprehensive knowledge of commonly used management methods, practices, procedures, regulations, policies, and processes.
- 5.3 **The Finance/Budget Analyst** primary roles and responsibilities include analyzing budget proposals, determining funding allocations, defending budget recommendations against various stakeholders, and forecasting future financial requirements. Tasks include:
- 5.3.1 Creating funding documents, including Purchase Requests and Military Interdepartmental Purchase Request (MIPRs)
 - 5.3.2 Working with DIU portfolios to formulate budgets for current and future years
 - 5.3.3 Work with the Agreements Officers to coordinate their approval of Other Transaction invoices
 - 5.3.4 Assist in managing the Operations and Maintenance budget
 - 5.3.5 Assist in managing the Research Development Test & Evaluation (RDT&E) budget
- 5.4 **Information Technology Services**
- 5.4.1 **Compliance analyst** primary roles and responsibilities include providing ongoing life cycle Assessment & Authorization (A&A) and Risk Management Framework support to Defense Innovation Unit (DIU). Tasks include:
- 5.4.1.1 EMASS entry, creation or updating of required artifacts, and coordinating validation efforts to support an Authorizing Official (AO) decision.
 - 5.4.1.2 The candidate will also assist with for multiple duties within the Plans, Programs, and Readiness (PPR) domain. This includes, but is not limited to, sustainment/onboarding activities, policy development, program/project management, and Configuration Control within the DIU and DIU's CSSP.
 - 5.4.1.3 Assist in the Risk Management Framework (RMF) process from both a packet preparation and assessor perspective; experience with eMASS, DITPR, and PPSM for population, tracking, and Plan of Action & Milestones (POA&M) staffing;
 - 5.4.1.4 Assist with the CSSP sustainment/onboarding requirements and processes; experience performing Information System Security Audits, Information System Security Assessments, developing Risk Management Plans, and assessing security architectures; experience with STIGs and justifying the technical need for applying each setting;
 - 5.4.1.5 Assist performing periodic auditing and continuous monitoring tasks to maintain security compliance;
 - 5.4.1.6 Assist with sponsorship for FedRAMP and DISA IL designation.
- 5.4.2 The **Cyber Security Network** support primary roles and responsibilities will be protecting DIU networks from cyber threats by actively monitoring for security anomalies, performing vulnerability assessments, and balancing security with business rules/needs. Tasks include:
- 5.4.2.1 Provide understanding of the cyber security environment, common network and host-based attacks, attack methods, and network defense architecture; in addition, have previous experience working in a security operations environment, preferably in defense-related organizations. Applicants must also be familiar with Department of Defense (DoD) cyber security service provider (CSSP) requirements and their implementation.
 - 5.4.2.2 Apply a variety of technical skills which include security event log analysis, endpoint forensic analysis, and vulnerability analysis. You will be accountable for conducting information risk assessments and audits to ensure that information systems and data are adequately protected and meet DoD cyber security requirements. In order to be effective, you will need to leverage knowledge and comprehensive understanding in using vulnerability scanners (Nmap/Nessus), intrusion detection systems (FireEye), firewalls (Palo Alto Networks), SEIM (Splunk or other) or other information security products.
 - 5.4.2.3 Work with vendors, outside consultants, and other third parties to improve information security within the organization. You will also create dashboards and deliver metrics related to information security and cyber

security operations.

- 5.4.3 **ServiceNow Development** primary roles and responsibilities include will be responsible for day-to-day technical development, customization, reporting, and optimization of any new and current project implementation of the ServiceNow Platform at DIU. Tasks include:
- 5.4.3.1 Responsible for development in all ServiceNow core architecture, including Service Catalog, Event, Incident, Problem, Change, Release, Asset, CMDB, Discovery, Knowledge, SecOps, Advanced Analytics, HR, Customer Service Management, workflows, orchestrations, and Self-Service Portal.
 - 5.4.3.2 Understand the day-to day operational needs of the organization with the goal of fully capitalizing on and realizing the capabilities of the ServiceNow platform.
 - 5.4.3.3 Responsible for delivering highly automated, secure, managed, and scalable technical solutions enabling the DIU organization to focus on continually improving secure and compliant end user technology experience.
 - 5.4.3.4 Responsible for being well versed in other development languages and should be comfortable working with APIs and scripts.
- 5.4.4 **Network Support** primary roles and responsibilities include supporting and maintaining DIU's IT network to include but not limited to analyzing, testing, troubleshooting, and evaluating existing network and systems: local area network (LAN), wide area network (WAN), Internet systems or a segment of a network system. Performs network maintenance to ensure networks operate correctly with minimal interruption. Exercises technical responsibility for hardware, software, and cloud-based PaaS and SaaS applications used by DIU personnel in four locations to include. Tasks include:
- 5.4.4.1 Provide network and cloud-based services; technical and security strategy support services; client system, server, and application management support services for systems used by DIU personnel (Google Suite, Asana, ServiceNow, Slack, Box)
 - 5.4.4.2 Perform system administrative tasks to ensure optimal performance of DIU systems. Perform daily and weekly port and vulnerability scans on DIU networks. Manage software upgrades: security and virus updates, application software fixes and patches (Firewall, network switches and WiFi configuration updates)
 - 5.4.4.3 Provide customizations to meet the various needs of different software application packages (update ServiceNow workflows for requests, build self-onboarding portal, develop ServiceNow training and any other training needs for staff; NSIN and NSIC network implementation; domain migration)
 - 5.4.4.4 Perform hardware interface modifications when required.
 - 5.4.4.5 Manage user IDs, passwords, log-ons, access points and rights.
 - 5.4.4.6 Analyze network equipment and software reliability and utilization reports for complex equipment and software systems to identify and correct problem areas.
 - 5.4.4.7 Oversee configuration and installation of network equipment and changing of components of existing equipment to ensure efficient operations (daily work, monthly and annual All Hands, auditorium meetings)
 - 5.4.4.8 Liaise with Defense Information Systems Agency (DISA) and the DoD CIO's office to ensure appropriate security compliance measures have been taken with respect to DoD Cyber instructions and regulations (draft IT acceptable use policy for DIU, waiver to DoD policy for IT, build out instructional repository in ServiceNow, research network architecture for compliance, work with IT providers to get them FedRamped compliant.)
 - 5.4.4.9 Technically document physical and logical server topology for all information systems and associated applications.
 - 5.4.4.10 Troubleshoot IT/network problems, including cloud-based Platform-as-a-Service and Software-as-a-Service, to determine mission impact and take corrective actions. (ServiceNow support tickets, DIU website security fixes per OSD/JSP vulnerability reports, LastWall penetration testing, NIPR systems on Army 63rd Reserve network)
 - 5.4.4.11 Provide information, recommendations, policies interpretation, and documentation in support of various security functions and special projects. Research relevant IT security related issues with respect to the potential impact on DIU.
 - 5.4.4.12 Assist CORS in managing IT equipment inventory and contracts (option years quotes) for: servers, computers, mobile devices, data wall, network equipment, conference room equipment, Palo Alto Network firewall, Aruba

network switches, LastWall, RedLock, Splunk, Trainings, CAPS, VDSS, AWS, Thin clients. Assist COR on GPS IT purchases for accessories and app service payments (Asana, Slack, APIs)

- 5.4.4.13 Manage on premise applications including, but not limited to Traps EMS, VMWare vSphere, ServiceNow.
- 5.4.4.14 Conduct daily and weekly network and system port vulnerability scans and mitigate (manually, using Software scanning and cloud tools)

5.5 Portfolio Support

- 5.5.1 **Portfolio Analyst** primary roles and responsibilities include support the core DIU mission in acting as an interface node between the DOD, entrepreneurs, start-up firms, and commercial technology companies in Silicon Valley, California (DIU West); Boston, Massachusetts (DIU East); and other U.S. technology hubs to increase DOD access to leading edge commercial technologies and technical talent. Tasks include:
 - 5.5.1.1 Curate mission-critical problems from DOD components and use the Commercial Solutions Opening (CSO) to identify and enable the pilot of applicable solutions against those problems. Subsequently, the Contractor will track and help ensure the success of pilot deployments of solutions by maintaining close communication with the companies offering solutions and the DOD components using them.
 - 5.5.1.2 Field inbound mission-critical problems from DOD components. Conduct market research by identifying companies operating in areas of interest, and developing and maintaining relationships with them.
 - 5.5.1.3 Assist DIU in the identification and development of mission-critical problems for which the market likely has applicable solutions to DIU Partners (leadership team).
 - 5.5.1.4 Provide SME assistance in drafting language for Commercial Solutions Opening (CSO) solicitations in coordination with a member of the Engagement team and a CSO Pathfinder.
 - 5.5.1.5 Provide SME assistance in the evaluation of solutions submitted in response to those solicitations in coordination with members of the Army Contracting Command (ACC) Contracting Team.
 - 5.5.1.6 Provide SME assistance to the Government to facilitate vendor pitches for their solution or when providing more information.
 - 5.5.1.7 Provide SME assistance to ACC contracting team when the Government decides to reject company's solutions or invites companies with selected solutions to present proposals for contract negotiations of pilot projects. Drive and coordinate this process.
 - 5.5.1.8 In conjunction with the ACC contracting team, the contractor shall assist the Government in the coordination of the contracting approval processes.
 - 5.5.1.9 Track and help ensure success of the pilot deployments of solutions by maintaining close communication with the companies offering solutions and the DOD components using them.
 - 5.5.1.10 Keep members of the Strategic Engagement team fully aware of major successes to help create impact stories that highlight the value proposition of DIU.

5.6 Security & Facilities Management

- 5.6.1 **Logistics & Facilities** primary roles and responsibilities are to plan, direct, or coordinate DIU administrative and facility such as inventory records and information management, mail distribution, facilities planning and maintenance, custodial operations, and other office support services. Tasks include:
 - 5.6.1.1 Provide day-to-day facilities operational support- (may require operation of a Government vehicle proof of insurance.) Assist with Lastwall, Clear Shark and ServiceNow training, security, and compliance. Conduct daily Meeting Room check and maintenance. Create Floor plan meeting room maps. Organized Army environmental inspection of Rogue Squadron area
 - 5.6.1.2 Support office space allocation, office space renovations, and customer relocations (coordinate with Army 63rd on space allocation and cleaning services contract, remaining office construction, assist with facility restructuring project, help assess Security Guard contract value to DIU
 - 5.6.1.3 Facilitate procurement of office supplies and equipment as identified by the Government (maintain inventory management in ServiceNow, organize storage room, manage FedEx account, CAC building and DIU access system,

- 5.6.1.4 Assist the Government with acquisition and/or receipt of office space, furniture, entry keys, telephones, parking passes, office supplies, and other resources as required.
- 5.6.1.5 Assist in the analysis of design, construction, and other recommendations as identified by the Government (manage construction fix of SVTC room, obtain security, IT and construction quotes, obtain quotes for SCIF maintenance,
- 5.6.1.6 Provide record compliance and other record lifecycle material applicable to existing Federal record policy and pending legislation (create SOPs for facility maintenance, packaging sending/receiving, and Govt. Purchase Card procedures)
- 5.6.1.7 Maintain familiarity with all applicable Federal and Department policies and regulations and with all logistic systems used throughout WHS and OSD, utilizing them as needed.
- 5.6.1.8 Establish and maintain effective working relationships with internal and external customers
- 5.6.2 **Special Security Representative** primary roles and responsibilities are to plan, implement, upgrade, and monitor security measures for the protection of computer networks and information. Ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. Respond to computer security breaches and viruses along with the Network IT Lead. In collaboration with R&E Security, complete security handoff from WHS to R&E. Tasks include:
 - 5.6.2.1 Maintain appropriate information in security related database systems to include computerized access control system, JPAS, or successor system, and security rosters reflecting eligibility and access, including Sensitive Compartmented Information (SCI). Ensure NIPR laptop is formatted correctly.
 - 5.6.2.2 Support DIU in classifying TOP SECRET (including TOP SECRET Special Access Programs) and Sensitive Compartment Information.
 - 5.6.2.3 Provide day-to-day on-site Security support to DIU personnel.
 - 5.6.2.4 Provide information, recommendations, policy interpretation, and documentation in support of various security functions and special projects. Research relevant security related issues with respect to the potential impact on DIU. Requests will often require a review of existing records, policy research, and database queries.
 - 5.6.2.5 Provide day-to-day administrative security support including research and preparation of graphic presentations; word-processing, proofreading, filing, and database management.
 - 5.6.2.6 Compile data and develop reports on security programs, policies, and procedures.
 - 5.6.2.7 Receive, record, and respond to all customer requests for security services, to include counter-intelligence support. Keep DIU informed of progress relative to their requests. Track each request to completion and by discrete action type (SIPRNet and JWICs tokens, facility access, badge request, Visit Access Requests (VARs), Security clearance verification SAAR forms for systems access). Provide sufficient metrics or monthly report to include request volume by type task, time to complete, average time by task, trend analysis over time, status.
 - 5.6.2.8 Manage email traffic submitted to the DIU Security shared mailbox.
 - 5.6.2.9 Conduct the security portions of in and out processing of Government Civilian, Military and Contractor personnel, ensuring actions are fully tracked to completion, including entries into the Joint Personnel Adjudication System (JPAS), or successor system. Assist with the TASS process for CACs.
 - 5.6.2.10 Support R&E Security Officers in conducting inquiries/investigations into potential security incidents by aiding the Government in the establishment of interviews; preparation of reports, and end-to-end tracking of the incident.
 - 5.6.2.11 Interface, brief, and provide analysis for Government Program Leads, senior management stakeholders, and executive leadership relative to the security program. Interface with Army 63rd for building security matters.
 - 5.6.2.12 Attend various security meetings to include various DIU SO program update meetings, training sessions, focus groups, and research groups. coordinate agendas, meeting minutes, presentations, and governance with the appropriate Government Program Lead as directed.
 - 5.6.2.13 Implement security procedures, checklists, process controls, and practices including preparation of documents and destruction of records as directed by the appropriate Government Program Lead.
 - 5.6.2.14 Support the annual DIU Information Security Assistance Visit (ISAV) program in accordance with R&E SO requirements. Coordinate the annual schedule, conduct the visits, develop recommendations for

improvement, prepare the annual reports, and prepare appropriate metrics outlining results and trend analysis over time.

- 5.6.2.15 Support the security education & awareness training program and report compliance.
- 5.6.2.16 Provide country-specific risk assessments and briefings for personnel planning to travel overseas. Estimate no more than 25 per year.
- 5.6.2.17 Support the SCI and collateral facility requirements for DIU SO customers. Maintain an inventory of secure facilities, including Sensitive Compartmented Information Facilities (SCIFs). Prepare and/or update required documentation affecting procedures and secure space accreditations, to include SCIF. Conduct physical security inspections, process necessary paperwork for accreditation, identify vulnerabilities, recommend mitigation strategies, and assist customer organizations with the implementation of actions to achieve DOD compliance. Establish and reactivate JWICs and SIPR accounts. Enable SCIF use requests from non-DIU visitors/personnel and coordinate VTC use by non-DIU visitors.
- 5.6.2.18 Provide record compliance and other record lifecycle material applicable to existing Federal record policy and legislation, in accordance with the DoD Administrative Instruction 15. Provide records management support to DIU staff in developing a DIU record plan and complete an inventory of all DIU records to identify DIU permanent records for long-term storage.

5.7 Strategic Engagement

- 5.7.1 The **Engagement Analyst** primary roles and responsibilities are to engage in promoting or creating an intended public image for individuals, groups, or organizations. The contractor shall write or select material for release to various communications media; originate and prepare written material, such as scripts, stories, advertisements, and other material. Tasks include:
 - 5.7.1.1 Assist in providing recommendations and guidance to DIU on strategic communications including external and internal outreach activities to support DIU responsibilities and objectives.
 - 5.7.1.2 Support DIU leadership to manage DIU media in coordination with the Office of the Assistant to the Secretary of Defense for Public Affairs.
 - 5.7.1.3 Support participation in relevant DOD forums, as determined by the Deputy Secretary of Defense. Assist in the developing and refining of messaging for a variety of internal and external audiences.
 - 5.7.1.4 Assist in developing and executing, government lead approved, strategic communications and media outreach activities in support of the DIU.
 - 5.7.1.5 Assist in providing input to the Secretary of Defense Research and Engineering (R&E) strategic communications plan. Ensure the DIU strategic communication plan is in line with and supports the Secretary of Defense Research and Engineering strategic communications plan.
 - 5.7.1.6 Assist in leveraging existing relationships, identify and create opportunities to deliver messaging to key audiences, including: DoD Organizations; Commercial Vendors; Other Professional and Academic Organizations
 - 5.7.1.7 Participate in Organizations/Events: Participation in national and local technology-focused panels hosted by universities, media, venture capital groups (i.e., identify local Valley “garage” meetings, speaking opportunities, pop-up and Maker events).
 - 5.7.1.8 Participate in various media forums: Host round-tables and one-on-one opportunities for leadership to share DIU messaging and build relationships with new media outlets.
 - 5.7.1.9 Assist in identifying key events for attendance by DIU and DOD senior leaders to provide messaging and promote DIU activities and objectives.
 - 5.7.1.10 Assist in coordinating with Office of the Secretary of Defense for Public Affairs Office (OSD/PAO), R&E front office to review strategic external outreach opportunities. Serve as a liaison between DIU and OSD/PAO on managing media inquiries.
 - 5.7.1.11 Conduct research on reporters’ backgrounds and past stories, provide context, and propose draft responses to media inquiries.

- 5.7.1.12 The contractor shall provide strategy development support services. The contractor shall:
- 5.7.1.13 Provide in-depth analysis and support in strategic planning, integration, and program management for DIU strategy.
- 5.7.1.14 Provide advice and support for the DIU outreach activities that help link DIU activities to key aspects of the DOD's National Defense Strategy, to include its speaker series, military visits program, events, and conferences.
- 5.7.1.15 Provide information, recommendations, and documentation in support of various DIU activities and special projects concerning linking the DIU technology investment with the most valuable outcomes for the DOD as a whole.
- 5.7.1.16 Support the conception and execution of DIU strategy, including but not limited to research regarding investment strategy and preparation of related event programs, graphic presentations, word processing, and database management functions.
- 5.7.1.17 Serve as an integral member of the DIU rapid prototype transition team and recruit additional DOD partners from across the DOD as a part of the process of taking DIU technology investments from prototypes to programs of record.
- 5.7.1.18 Coordinate with external DIU partners and stakeholders, especially those in the National Capital Region (NCR), to integrate the DIU investment strategy with key objectives of the National Defense Strategy.
- 5.7.1.19 Conduct analysis and communicate analytical findings on new and existing initiatives, projects, and programs to DOD and DIU Leadership.
- 5.7.1.20 Review and track action items associated with the DIU Strategic Communications strategy, to enable seamless linkages between innovators in the military departments and the DIU technology priorities.
- 5.7.1.21 Organize the convening of key stakeholders within DOD and relevant DIU portfolio and project managers.
- 5.7.1.22 Compile reports and memoranda in support of the DIU office, engagement program, and DIU Leadership.
- 5.7.1.23 Identify further opportunities for DIU portfolio and project management staff to engage with key stakeholder communities in the Military Departments.
- 5.7.1.24 Maintain familiarity with all Federal and Department policies that affect the ability of DIU to accelerate commercial technology to the warfighter.
- 5.7.2 The **Digital Content Manager's** primary roles and responsibilities will be to manage and support the development of content across DIU's website and social media accounts to create a cohesive, branded, and engaging digital experience. Responsibilities include maintain ownership of the quality and consistency of our web standards, content, and structure; responsible for day-to-day content management of the website and social media accounts (LinkedIn, Twitter, Facebook, and YouTube). Tasks include:
 - 5.7.2.1 Build content into our content management system (Contentful); test and deploy into production
 - 5.7.2.2 Think strategically about our users and web presence and build new features, capabilities, or pages in collaboration with external developers (when required) to support mission execution
 - 5.7.2.3 Collaborate with IT and external developers to monitor/troubleshoot the performance of the DIU website tech stack
 - 5.7.2.4 Produce and edit video, such as virtual event recordings, and podcast content for multiple channels (website, YouTube, Acast, Spotify, iTunes, etc.)
 - 5.7.2.5 Collect and analyze website (via Google Analytics) and social media performance data to ensure alignment between digital content and communications strategies and DIU business goals
 - 5.7.2.6 Track DIU's media hits, including media hits by members of the DIU team
 - 5.7.2.7 Support basic graphic design or branding requests and/or collaborate with external designers to produce new design assets as required (banners, icons, marketing collateral, templates, etc.)
 - 5.7.2.8 Take initiative to problem solve and help implement new standards and best practices for digital content and marketing strategies
 - 5.7.2.9 Utilize User Experience (UX), social media, SEO, and online lead development strategies
 - 5.7.2.10 Manage HTML, CSS, or other front-end web-related languages

PART 6

APPLICABLE PUBLICATIONS

6. The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures.
 - The Federal Acquisition Regulation, Current to: FAC 2005-99, Effective: 15 Jun 2018
 - The Defense Federal Acquisition Regulation Supplement (DFARS) Current to DPN20171228 (Effective 28 Dec 2017) Edition
 - OPM Hiring Process Model <https://www.opm.gov/policy-data-oversight/human-capital-management/hiring-reform/hiring-process-analysis-tool/>
 - DoD Handbook for Incoming Officials https://my.whs.mil/sites/default/files/IncomingHandBook_19Jan2017_WEBCAC_1.pdf
 - Defense Travel System (DTS) <https://dtsproweb.defensetravel.osd.mil/dts-app/pubsite/all/view/>,
 - Federal Travel Regulations www.gsa.gov/federaltravelregulation,
 - Joint Travel Regulations (JTR) <http://www.defensetravel.dod.mil/site/travelreg.cfm>
 - DoD Federal Privacy Rule [Part 310—DoD Privacy Program](#)
 - The Department of Defense (DD) Form 254 “Contract Security Classification Specification”³

³ <http://acqnotes.com/wp-content/uploads/2014/09/A-Guide-for-the-Preparation-of-a-DD-Form-254.pdf>

PART 7
ATTACHMENT/TECHNICAL EXHIBIT LISTING

7.1 Technical Exhibit 1 – Estimated Workload Data*

*Attached to the sources sought notice

TECHNICAL EXHIBIT 2

PERFORMANCE REQUIREMENTS SUMMARY and DELIVERABLES SCHEDULE*

Acceptable Quality Level (AQL): Refer to Table 2, for AQL related to each deliverable. For the purposes of this PWS, *Highly Satisfied* has the meaning of, the DIU customer finds the work performed to exceed their expectations, little to no changes is required and *On Time* has the meaning of, within 7 business days of the following month or as provided in more detail in Table 2.

Deliverable: A deliverable is a specific measurable, tangible, and verifiable activity, outcome, result, item, or product that the Contractor shall provide and that will require formal Government acceptance and approval. The Government will review, assess, and provide comment, as required. The Contractor shall provide deliverables as set forth in Table 2.

Inspection/Acceptance/Method of Surveillance: Unless otherwise specified in the contract, the Government will accept or reject services and materials at the place of delivery as promptly as practicable after delivery, and they will be presumed accepted 60 days after the date of delivery, unless accepted earlier. The Government will notify the Contractor of deliverable acceptance or provide comments in writing. After receipt of Government comments, the Contractor, if necessary, shall revise and resubmit the final deliverable to the Government within 5 business days of receipt of written comments.

***Acceptable Quality Level (AQL), Deliverable, and Inspection/Acceptance/Method of Surveillance will be provided at time of solicitation**

DRAFT