PERFORMANCE WORK STATEMENT

NOVASTAR

NASIC S&TI ANALYTIC CAPABILITY SUPPORT

National Air and Space Intelligence Center (NASIC)
Wright-Patterson Air Force Base, Ohio

15 March 2021

1.0 **BACKGROUND.** National Air and Space Intelligence Center (NASIC) requires contract support for research, development, and sustainment of new and existing hardware, systems, and software capabilities enabling scientific and technical intelligence production for the United States Air Force (USAF), the Department of Defense (DoD) and National Level intelligence efforts. NASIC also requires contract support for the production of technical intelligence through collection, analysis, planning, processing, dissemination, archiving and associated activities for NASIC, the USAF, the DoD and National Level intelligence efforts. The work provides agile and innovative resource capability supporting technical analysis in the Intelligence Community, turning innovation into intelligence products, and constantly improving productivity in technical analysis product generation. NASIC's mission is to discover and characterize air, space, missile, forces, and cyber threats to enable full-spectrum multi-domain operations, drive weapon system acquisition, and inform national defense policy. Task Orders (TOs) will be awarded to perform work in and across these mission areas.

1.1 NASIC MISSIONS.

1.1.1 Air. Create foundational, predictive, integrated, scientific and technical intelligence analysis on the characteristics and performance of foreign military and civil aircraft, ground and airborne radars, directed energy weapons, integrated air defense (IADS,) and the Command, Control, Communications, Computers, Intelligence Surveillance and Reconnaissance (C4ISR) capabilities that connect the foreign Joint Force and empower its commanders at the tactical, operational, and strategic levels.

1.1.2 Space/Counterspace. Create foundational, predictive, integrated, scientific and technical intelligence analysis on foreign communications systems, navigation assets and warfare capabilities, ISR systems, and infrastructure supporting space operations to include space launch vehicle systems, and facilities to include associated telecommunications. This also includes counterspace analysis focusing on foreign space situational awareness (SSA) capabilities, cyber and electronic threats to space systems, anti-satellite missiles and directed energy weapons, along with associated couterspace command and control elements.

1.1.3 Cyberspace. Create foundational, predictive, integrated, scientific and technical intelligence analysis on foreign cyber threats to prevent technological surprise for air and space dominance. Provides characterization and performance of foreign capability as well as associated vulnerabilities critical to offensive cyber operations. Produce cyber threats analysis on foreign intent and doctrine as well as other threats related to forces, networks, and operations of US air and space systems.

1.1.4 Forces. Create foundational, predictive, integrated, scientific and technical intelligence analysis on foreign force employment, doctrine, behavioral influences, foreign denial and deception, full-spectrum campaign-level assessments, emerging and disruptive foreign technology, the foreign acquisition cycle, and threats to DoD modernization.

1.1.5 Missiles. Create foundational, predictive, integrated, scientific and technical intelligence analysis on foreign strike weapons, operations, associated C4ISR, capabilities and vulnerabilities. Analyze and assess detailed external configuration; location and performance

of internal components, technologies, and other subsystems; construction techniques and materials; guidance and control systems; propulsion systems; reentry systems, countermeasures, and ground support equipment.

1.2 NASIC DISCIPLINES

1.2.1 Geospatial Intelligence (GEOINT). Analyze, assess, and exploit imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on Earth. This includes the following GEOINT program elements/missions: Electro-Optical (EO), Synthetic Aperture Radar, Multi Spectral Imaging/Hyper Spectral Imaging (MSI/TSI), Thermal Infrared (TIR), Overhead Persistent Infrared (OPIR), Light Detection and Ranging (LIDAR), Ground Moving Target Indicator (GMTI), and Full Motion Video (FMV).

1.2.2 Measurements and Signatures Intelligence (MASINT). Analyze, assess, and exploit technically derived measurement and signatures intelligence, including radar (Line-of-Sight, Over-the-Horizon, Space Object Characterization, and Non-Cooperative Target Identification), Electro-Optical (Air-borne and terrestrial), Radio Frequency, Laser, and Bistatic, resulting in intelligence that locates, identifies, and describes distinctive characteristics of targets.

1.2.3 Signals Intelligence (SIGINT). Analyze, assess, and exploit foreign communications systems and non-communications emitters including: Data analysis, data processing, data management, analytic techniques development and implementation, system engineering, system integration and training development.

1.2.4 Human Intelligence (HUMINT). Analyze, assess, and exploit information gathered from human interactions including: gathering information from air shows and technology conferences and debriefing individuals who have placement and access to information on foreign threats to air, space, and cyberspace.

1.2.5 Open Source Intelligence (OSINT) Analyze, assess, and exploit unclassified data (to include translation of foreign material) with intelligence requirements referred to as Publically Available Information, or PAI. PAI include academic journals, foreign news media, social media, and other web-based sources.

1.2.6 Technical Intelligence (TECHINT). Analyze, assess, and exploit foreign material, technology, and scientific information enabling the understanding of the capabilities, limitations, vulnerabilities, and performance of foreign assets enabling customers to build countermeasures, develop new technologies, and enhance force protection to prevent technological surprise and neutralize an adversary's advantage. This includes the following TECHINT program elements/missions: overall weapon system analysis and characterization, software exploitation, Field-Programmable Gate Array/Complex Programmable Logic Device (FPGA/CPLD) Exploitation, Printed Circuit Board (PCB) Exploitation, Binary Extraction of Embedded Devices, Computer Forensics, Cyber Vulnerability Analysis, Anti-Tamper Identification and Analysis, Tool Development in Support of Weapon System Exploitation, Digital Signal Measurement and Analysis, Radio Frequency (RF) System Characterization, RF Signal Measurement and Analysis, RF Signature Prediction Support, Electro-Optical/Infrared

(EO/IR) Signature Prediction Support, Computer-aided Design (CAD) Modeling, and Material Properties Measurement and Analysis. Additional support may be required to enable TECHINT including the following: Information Technology, Cybersecurity, Safety, Facility Maintenance, Physical Security, and Inventory Control.

1.2.7 Intelligence Analysis. Analyze, assess and fuse multiple sources of intelligence to create actionable intelligence to support full-spectrum multi-domain operations, drive weapon system acquisition, and inform national defense policy. This includes multiple sources of intelligence from the following mission areas: System Analysis, Force Analysis, Modeling and Simulation, Electronics Analysis, Engineering Analysis, Air & Cyberspace, Integrated Command, Control, Communications, Computers, Intelligences, Surveillances, and Reconnaissance (C4ISR), and Information Warfare. Utilize multiple sources of intelligence to create scientific and technical intelligence on foreign space systems focusing on, but not limited to, space-enabled services & operations, developing capabilities, enhanced situational awareness to/from space, risk & vulnerability assessments of space-related systems and architectures, global commercialization trends, and dual-use technologies.

2.0 SCOPE OF WORK

2.1 Overview. Provide intelligence support and perform scientific and technical intelligence analysis across NASIC missions (Air, Space, Cyber, Forces, Missiles) and disciplines (GEOINT, MASINT, SIGINT, HUMINT, OSINT, TECHINT) for strategic and operational planners, tactical operators, the acquisition community and policymakers through collection, analysis, planning, processing, dissemination, archiving and associated activities for NASIC, the USAF, the DoD and National Level intelligence efforts. These requirements support the creation, evaluation and analysis of intelligence data on foreign developments in current and future weapon systems, subsystems, and technologies.

2.2 Research. The contractor shall conduct and apply research techniques to determine solutions to NASIC requirements. The contractor shall research capabilities, developments, event phenomenology, sensor responses, technologies, and process algorithms to enhance the NASIC scientific and technical intelligence analysis.

2.2.1 Investigation. The contractor shall hypothesize and investigate possible solutions to requirements. The contractor shall support and conduct field collections.

2.2.2 Prototyping. The contractor shall analyze assigned topics and generate prototypes as possible solutions.

2.2.3 Verification. The contractor shall evaluate solutions to verify proper implementation and compliance with study requirements and design.

2.2.4 Validation. The contractor shall evaluate solutions to confirm accurate results.

2.2.5 Documentation. The contractor shall report the outcome of research conducted and identify and recommend solutions for transition to development.

2.3 Development. The contractor shall apply knowledge and understanding to develop solutions for NASIC requirements. The contractor shall plan, organize, coordinate, and execute system engineering actions designed to develop new and modified capabilities. The contractor shall support all phases of development including requirements derivation, design, implementation, system test, acceptance test, documentation, and delivery of hardware and/or software.

2.3.1 Systems/Software Engineering. The contractor shall conduct systems engineering activities as the basis for developing capabilities. The contractor shall design, develop and acquire system/software components with no proprietary, intellectual property or other caveats limiting the Government's rights or use. The contractor shall employ and leverage existing software tools and standards to allow for maximum interoperability and reuse.

2.3.2 Analysis. The contractor shall review and refine Task Order requirements. The contractor shall incorporate solution specific requirements that characterize and specify the functions and performance of the selected design solution. The contractor shall analyze needs and document requirements to support data analysis.

2.3.3 Design. The contractor shall develop system/software-level designs. The contractor shall expand system-level design to include detailed designs for all levels of the selected design. The contractor shall ensure that all designs are consistent and compatible with intelligence community tradecraft standards.

2.3.4 Development. The contractor shall implement the selected design through system/software development activities, acquisition, or modification of existing Research and Development solutions. The contractor shall convert the approved designs into a functioning system through software code development and the acquisition of hardware and software required to operate the system. The contractor shall develop, version control, and store all code within a government provided code repository. If the government does not provide a code repository, then approved centralized code repositories will be provided to the contractor. All developed code will follow the Software Development Life Cycle standards which will be provided by the Government.

2.3.5 Integration. The contractor shall assemble and incorporate lower-level elements and components into higher-level system/software elements. The contractor shall assemble and incorporate higher-level system elements into the final system.

2.3.6 Testing. The contractor shall conduct testing required during development and integration to demonstrate the engineering design and development process is complete. The contractor shall demonstrate that the developed system/software conforms to requirements specified in requirements analysis and system design documents.

2.3.7 Installation/Deployment. The contractor shall install the developed system/software into a production environment and resolve problems identified in the Integration and Testing phases.

2.3.8 Documentation. The contractor shall document all solutions developed, including source code.

2.3.9 Training. The contractor shall design, develop and conduct training for new or modified capabilities when requested.

2.4 Sustainment. These requirements enhance and sustain analytic tools, capabilities, and knowledge databases consistent with NASIC corporate strategies through the application of technical knowledge and processes. The contractor shall plan, organize, coordinate, and execute systems engineering actions designed to sustain systems/software supporting NASIC requirements. The contractor shall support all phases of sustainment including: problem identification, analysis, design, implementation, system test, acceptance test, documentation, and delivery of updated hardware and software.

2.4.1 Adaptive Maintenance. The contractor shall operationally align analytic tools and systems including hardware and software to remain operational in a changing Information Technology (IT) environment.

2.4.2 Corrective Maintenance. The contractor shall conduct corrective maintenance of existing systems to solve hardware and software bugs discovered after initial delivery to the Government.

2.4.3 Preventative Maintenance. The contractor shall conduct scheduled maintenance of existing systems to sustain operations of existing hardware and software and keep systems functioning to support intelligence production during and outside normal business hours. Requirements for support outside of normal business hours will be communicated in each task order performance work statement.

2.4.4 Emergency Maintenance. The contractor shall conduct unscheduled emergency maintenance of existing systems to sustain operations of existing hardware and software and keep systems functioning to support intelligence production during and outside normal business hours. Requirements for support outside of normal business hours will be communicated in each task order performance work statement.

2.5 Production. The contractor shall perform intelligence production activities at NASIC or another cleared facility, with the potential for support at other CONUS and OCONUS locations. These requirements include obtaining data, performing technical analysis, developing assessments, evaluations, and predictions of capabilities; designing and assessing current, developmental and projected threat systems; providing reports related to worldwide developments. Production support may be required outside of normal business hours. Requirements for this additional level of support will be communicated in each task order performance work statement.

2.5.1 Tasking and Collection. The contractor shall perform a variety of functions identified in the Task Orders to support intelligence collection, production, research and development activities. The contractor shall identify and use the appropriate data sources, types, and formats with applicable tools to discover and retrieve data. The contractor shall manipulate and operate databases and other tools to track, query, archive, and recall previous tasking.

2.5.2 Processing. The contractor shall convert, correct, and enhance raw data to exploitation ready formats identified in the Task Orders. The contractor shall convert received data to community standardized data formats with metadata tags. The contractor shall apply various correction factors to correct numerous phenomena and sensor related errors. The contractor shall identify exceptions, errors, and systemic problems.

2.5.3 Analysis and Exploitation. The contractor shall analyze data to create information, characterize events and activities, and discover relationships and trends. The contractor shall produce descriptive and predictive analyses and document results in intelligence community-compliant formats identified in the Task Orders. The contractor shall evaluate tools and customized methodologies and applications.

2.5.4 Dissemination. The contractor shall distribute the products resulting from intelligence production via electronic dissemination systems and written, visual, and oral methods identified in the Task Orders. The contractor shall archive data, products, data reports, and intelligence reports.

3.0 GENERAL REQUIREMENTS

3.1 Non-Personal Services. The Government shall neither supervise contractor employees nor control the method by which the contractor performs the required tasks. The Government shall not, under any circumstances, assign tasks to, or prepare work schedules for individual contractor employees. The contractor shall manage its employees and guard against any actions that are personal services, or give the perception of personal services. If the contractor believes that any actions constitute or are perceived to constitute personal services, the contractor shall notify the Procuring Contracting Officer (PCO) immediately.

3.2 Inherently Governmental Functions. The contractor shall not perform any inherently governmental functions as defined by FAR Subpart 7.5. All program decisions shall be the sole responsibility of the Government. The contractor shall not counsel, mentor, make judgments and/or discretionary decisions or perform any other activities related to supervision of Government personnel. If the contractor believes that any actions constitute or are perceived to constitute inherently governmental functions, the contractor shall notify the CO immediately.

3.3 Rehabilitation Act Compliance (Section 508). Unless otherwise exempt, all services and/or products provided in response to this requirement shall comply with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR part 1194.)

3.4 Privacy Act Information. The provisions of the Privacy Act of 1974 protect information, and, therefore all contractor personnel and any subcontractors assigned to this contract shall take the proper precautions to protect the information from unauthorized disclosure.

3.5 Operational Security (OPSEC). Critical Information (CI) associated with any Task

Order shall be protected to prevent un-authorized collection and exploitation. The contractor shall implement security requirements as directed by the Government's OPSEC Plan including initial training and reoccurring training, which shall be provided as Government Furnished Information (GFI).

3.6 Information Technology-Development. These requirements include the use of DevSecOps, Agile software methodologies in on premises, cloud, and/or hybrid architectures to develop and maintain resilient and flexible analytic tools to support all aspects of NASICs mission. NASIC is implementing a DevSecOps environment coupled with Agile methodologies to achieve results through automation, continuous capability enhancements and robust feedback loops. The Government wants to provide the option of a shared, collaborative environment among the development, testing, quality assurance, cybersecurity and operations teams. The contract scope encompasses requirements to provide the development, implementation, enhancements, and maintenance services required to successfully implement and sustain applications in the context of this environment. All IT technical tasks will be performed in accordance with the latest technologies and methodologies of large scale fault-tolerant systems using Agile methodologies in an evolving DevSecOps environment. The application lifecycle environment will enable the Government to provide an environment to automate building, testing and deploy applications.

3.7 Advisory and Assistance. The contractor shall not perform advisory and assistance work for the Government in the same mission or discipline areas outlined in this PWS. If the contractor begins this type of work, they must inform the CO or COR immediately and explain how they will avoid, neutralize, and mitigate any organizational conflicts of interest

3.8 Environmental Requirements Performance. The contractor shall use the existing infrastructure when performance is on a Government site. The contractor will not perform construction or modification of buildings, operation of heavy equipment/machinery or otherwise disturb the natural environment already in place. The contractor will not require authorization to use ozone-depleting chemicals and substances. The contract shall observe considerations for pollution prevention/control as well as the drug-free workplace policies for Air Force contracts. The contractor shall adhere to the requirements in FAR Part 23 (and its supplements) entitled Environment, Energy, and Water Efficiency, Renewable Energy Technologies, Occupational Safety, and Drug-Free Workplace.

3.9 Business Relations. The contractor shall ensure the professional and ethical behavior of all contractor personnel.

3.10 Contract Management. The contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to each Task Order. The contractor shall maintain continuity of operations between the Government and the contractor’s corporate offices.

3.11 Contract Administration. The contractor shall establish processes and assign appropriate resources to effectively administer task efforts. The contractor shall respond to Government requests for contractual actions in a timely fashion. The contractor shall designate a single point of contact between the Government and Contractor personnel assigned to support contracts or Task Orders. The contractor shall assign work effort and maintain proper and accurate time keeping records of personnel assigned to work on the requirement.

3.12 Contract Personnel. The number and depth of specialized areas of these analyses require specialists of exceptionally high competence across NASIC missions and disciplines in the areas of military systems, operations, and trained to recognize subtleties in foreign developments which may directly impact current and future military operations and weapons developments.

3.12.1 Qualified Personnel. The Contractor shall employ fully qualified employees with the required knowledge and expertise. Government-unique training may be required from time to time, and will be communicated either through the PCO or Contracting Officer Representative (COR). Any such communication of training will be considered mandatory knowledge and expertise under this Task Order. If Government-unique training is required to perform contractor personnel duties, then written approval must be obtained from the CO or COR prior to attending the training.

3.12.2 Intelligence Oversight Reporting and Training Requirements. In accordance with DoDD 5148.13, Intelligence Oversight, contractor personnel are required to report any Questionable Intelligence Activity (QIA) or Significant or Highly Sensitive Matter (S/HSM) to the COR or CO. Contractors shall complete initial Intelligence Oversight training within 60 days of assignment and refresher training annually thereafter.

3.12.3 Contractor Identification. In accordance with DFARS 211.106, contractor employees shall introduce themselves or be introduced as contractor personnel. Contractor employees shall clearly identify themselves as "Contractors" at all times. This includes all communications (telephone, mail, electronic mail (email) and faxes), meetings, attendance sheets, and documents. In addition, Contractor personnel shall identify their company affiliation in email signature blocks. Contractor personnel are required to wear or prominently display installation identification badges or contractor-furnished, contractor identification badges while visiting or performing work on a Government installation. |

3.12.4 Personnel Responsibility. The contractor shall provide for employees during designated Government non-work days or other periods where Government offices are closed due to weather or security conditions. The contractor shall maintain the currency of their employees by providing initial and refresher

training as required to meet the PWS requirements. The contractor shall provide the necessary infrastructure to support both on-site (Government site) and off-site (contractor site) contract tasks.

3.12.5 Contractor Holidays. The prices/costs in the contract include holiday observances; accordingly, the Government will not be billed for such holidays. Any work to be performed on an observed holiday, shall be submitted for approval to the COR a minimum of 10 days before the work is to occur. If approved, the contractor shall only bill the Government at the established hourly rate, and not at a higher holiday/overtime rate. The following days are considered holidays: All days issued by Executive Order by The President of the United States; New Year's Day; Martin Luther King Jr. Day; President's Day; Memorial Day; Independence Day; Labor Day; Columbus Day; Veteran's Day; Thanksgiving Day; Christmas Day.

3.12.6 **Emergency and Exercise Conditions.** The contractor is expected to participate and comply with all emergency and exercise conditions at facilities where the contractor is working.

3.12.7 **Labor Categories.** The contractor shall accomplish the assigned work by employing and utilizing qualified personnel with appropriate combinations of education, training, and experience. The contractor shall match personnel skills to the work or task. The contractor shall ensure the labor categories as defined in the Labor Categories document, labor rates, and man-hours utilized in the performance of each Task Order PWS line item issued hereunder will be the minimum necessary to accomplish the task.

3.12.8 **The Use of Foreign Nationals**. A foreign national is defined as all persons not citizens of, not nationals of or immigrant aliens to the U.S. It is expected that some materials marked NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN) will be passed to the contractor in support of various tasks issued. Any Foreign National will be prohibited from reviewing material with this handling caveat. Immigrant alien is defined as any person lawfully admitted into the U.S. under an immigration visa for permanent residence.

3.12.9 **Non-Disclosure Agreement.** When specified, contractor personnel shall complete and sign a "Contractor Employee Non-Disclosure Agreement." A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the contracting officer prior to performing any work.

4.0 PROGRAM/PROJECT MANAGEMENT

4.1 Program Management. The contractor shall provide the necessary resources to plan, implement, and manage the tasks either on-site or off-site to the extent provided by the available man-hours. The contractor shall conduct management activities to accomplish the contract objectives. The contractor shall plan, organize, direct, coordinate, control and propose timely

contract actions to accomplish contract objectives. The contractor shall manage and monitor all travel.

4.2 Program Management Reviews. For each Task Order, the contractor shall provide up-to-date status through quarterly Program Management Reviews (PMRs). The contractor's Program Manager shall be required to present oral program reviews as requested by the Government.

4.3 Status. The contractor shall provide up-to-date status through Monthly Status/Financial Reports. Monthly Status/Financial Reports shall be unclassified and shall include details on the following items for each previous time period: (1) Best up-to-date estimate of hours worked and expected charges, including those of subcontractors; (2) status of work performance; (3) any problems or concerns encountered that may impact cost or schedule; (4) status of open items from previous reports; (5) any suggested solutions; (6) personnel changes; (7) proposed government actions; (8) a summary chart of the current financial status broken out by contract line item numbers (CLINs) (labor, other direct costs, ODCs/travel, material, options).

4.4 Contractor Presentations. The contractor shall prepare written documentation on the results of tasking to include verbal and written comments, informational memorandums and letters, meeting minutes, specialized technical reports and papers, and final report and studies as defined in individual TOs. The contractor shall present briefings on government selected studies, models, or analyses associated with task efforts to various intelligence organizations, committees, or panels as defined in the individual TOs by the government. The contractor shall prepare and present the briefings to the government appointed experts prior to the actual presentation, to ensure content accuracy and that security considerations are properly addressed and followed.

4.5 Classified Materials. The contractor shall maintain a complete listing of classified material issued by the government and maintained at the contractor's facility in performance of this contract to include, the title of the material; the origination date; the overall classification; the type of material (i.e. report, electronic media, etc.); the number of copies held; and any other information necessary to identify the inventory. The contractor shall obtain written approval by the PCO or COR prior to the release of any classified material. The contractor shall provide the PCO or COR with a destruction certificate for all classified material that is destroyed.

4.6 Subcontractor Management. The contractor shall manage subcontractor efforts necessary to integrate work performed and shall be responsible and accountable for subcontractor performance. The prime contractor shall manage work distribution to ensure there are no Organizational Conflict of Interest (OCI) considerations. Contractors may add subcontractors to their team after notification to the PCO or COR.

4.7 CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM (CPARS) Assessment. Upon request by the Government, the contractor shall submit a self-evaluation of their performance at least annually utilizing a Government provided template. From time of Government request, the contractor shall have 9 business days (i.e. initial request due date of 1 week with an additional 2 business day follow-up) to provide input to the COR. The contractor self-assessment will then be submitted to the Government client where they will utilize this information to formulate an independent performance evaluation that will be processed through

the Contractor Performance Assessment Reporting System. The requirements of the FAR and its supplements as it pertains to CPARS reporting shall be adhered to.

4.8 Contractor Manpower Reporting Application (CMRA). The contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the United States Air Force via a secure data collection site. The contractor shall fill in completely all required data fields at http://www.ecmra.mil.

5.0 APPLICABLE DOCUMENTS

5.1 Specific documents with regards to requirements information/documentation and guidance will be determined and solicited on an individual Task Order (TO) basis.

6.0 SPECIAL INSTRUCTIONS

6.1 **Work Performance Location.** The majority of the work shall be accomplished at the contractor's facility and at NASIC, 4180 Watson Way, Wright-Patterson AFB, Ohio 45433-5648. CONUS and OCONUS work locations are possible. Additional locations will be specified in the Task Order PWS.

6.2 **Security.** All security requirements will be identified in each Task Order. Up-to TS/SCI and Special Access Program (SAP) access may be required. For classified work, the contractor shall provide sub-contract DD254s for all subcontractors.

6.3 **Travel.** Travel and Temporary Duty requirements will be established for each Task Order, as appropriate. Travel shall comply with all Joint Travel Regulation requirements and shall be approved by the CO or COR prior to incurring any travel related expenses. The Contractor may be required to travel using commercial air, Government air, and other conventional modes of transportation to Outside Continental United States and Continental United States (OCONUS & CONUS) locations.

6.4 **Facilities and Services.** The Government will provide work spaces and computer support for contractor personnel working full-time within the NASIC facility Area A, WPAFB. All contractors working within NASIC shall have the proper security clearances for these areas and equipment. In addition to standard desktop software, the Government will provide access to non-standard analysis software as required for the specific Task Order. The contractor shall provide the necessary resources to plan, implement, and manage the tasks either on-site or off-site as required in each individual Task Order to the extent provided by the available man-hours. If work cannot be accommodated at the Government facility, the contractor shall provide all labor, facilities, and non-Government Furnished Equipment (non-GFE) to successfully complete all requirements. If work cannot be accommodated at the Government facility, the contractor shall provide all labor, facilities, and non-Government Furnished Equipment (non-GFE) to successfully complete all requirements.

6.5 **Government Furnished Property (GFP).** GFP will be identified in Task Order requirements. The PCO will review each Task Order to ensure appropriate actions are taken under FAR Part 45, Government Property, for accountability and responsibility,

when applicable. The Contractor shall ensure accurate control and accountability of all GFP.

6.6 **Government Furnished Information (GFI).** Documents, manuals, drawings, publications and forms and other data will be provided to the Contractor, when appropriate, and specified in each Task Order. If provided, it will be screened to ensure no classified information is released without proper authorization and security. Most GFI will reside in Government controlled facilities and be handled IAW applicable guidance. GFI that is not in Government control will be handled in accordance with the instructions specified in the Task Order DD Form 254, Contract Security Classification Specification.

6.7 **Information Technology (IT).** All IT documentation and solutions implemented at NASIC shall conform to and shall be in compliance with the NASIC Enterprise Architecture as published by the EAO and approved by the NASIC CIO. Deviations from the NASIC IT standards shall be addressed through the processes outlined in NASIC Guiding Principles, Guardrails, standards, and additional policies accordingly. All contractors and personnel requiring accounts with elevated system/network privileges shall be trained and certified in accordance with DoDD 8140.01, Cyberspace Workforce Management Program, and DFARS 252.239-7001, Information Assurance contractor Training and Certification Program. All IT solutions developed under this effort shall be fully turned over to the Government without use restriction or limitation on the Government's ability to provide the IT solution and/or source code to any other third party.

7.0 Transition. The contractor shall follow the transition plan submitted as part of the proposal for each individual Task Order and keep the Government fully informed of status throughout the transition period. Throughout the phase-in/phase-out periods, it is essential that attention be given to minimize interruptions or delays to work in progress that would impact the mission. The contractor must plan for the transfer of work control, delineating the method for processing and assigning tasks during the phase-in/phase-out periods.

8.0 Data Deliverables

A001 Presentation Material
A002 Report, Record of Meeting/Minutes
A003 Management Plan
A004 Status Report
A005 Contract Work Breakdown Structure
A006 Data Accession List (DAL)
A007 Integrated Program Management Report
A008 Implementation Plan
A009 Technical Report Study/Service
A010 Manhour Estimate, Technical Cost Proposal
A011 Contractor's Configuration Management Plan
A012 System Engineering Management Plan
A013 Interface Control Document
A014 Computer Program End Item Documentation

A015 Software Development Plan
A016 Software Installation Plan
A017 Software Transition Plan
A018 System/Subsystem Specification
A019 System/Subsystem Design Description
A020 Software Requirements Specification
A021 Interface Requirements Specification
A022 Software Design Description
A023 Interface Design Description
A024 Database Design Description
A025 Software Test Plan
A026 Software Test Description
A027 Software Test Report
A028 Software Product Specification
A029 Software Version Description
A030 Software User's Manual
A031 Software Center Operator Manual
A032 Test Procedure
A033 Security Test Plan
A034 Acceptance Test Plan
A035 Training Program Development and Management Plan
A036 Training Situation Document
A037 Instruction Performance Requirements Document
A038 Instructional Media Requirements Document
A039 Instructional Media Design Package
A040 Training Program Structure Document
A041 Course Conduct Information Package
A042 Training Conduct Support Document
A043 Training Evaluation Document
A044 Test Package
A045 Instructional Media Package
A046 Training System Support Document
A047 Web-based Course
A048 Commercial Off-The-Shelf Manuals and Associated Supplemental Data
A049 Department of Defense Modeling and Simulation Verification and Validation Plan

9.0 SERVICES SUMMARY (SS)

A Quality Assurance Surveillance Plan (QASP) will be developed by the Government which will include a Services Summary for each task order.

The contractor shall submit a Quality Control Plan to ensure that Contractor services conform to contract requirements and standards. This shall include, but not be limited to, documented procedures, inspections, tests (taken at the point of performance) and training. The Contractor shall submit the final Quality Control Plan within 30 days after contract award**.**