STATEMENT OF WORK
FOR
THREAT SYSTEMS SUPPORT

1. OBJECTIVE:

The Defense Intelligence Agency/Missile and Space Intelligence Center's (DIA/MSIC) Test and Evaluation Threat Resource Activity (MSIC7) requires contractor support to accomplish diverse missions of providing threat intelligence and threat resource analysis in support of the Director, Operational Test and Evaluation's (DOT&E) Title10, United States Code (USC) responsibilities of assessing test adequacy of U.S. weapons systems. The Test and Evaluation Threat Resource Activity (TETRA) is an organizational element within DIA/MSIC and is operationally assigned to DOT&E. This Scope addresses specialized technical and programmatic support to fulfill diverse mission requirements of threat intelligence reporting, threat resource analysis and support to the DOT&E and the associated directorates (i.e. Land and Expeditionary Warfare, Naval Warfare, Air Warfare, Net-Centric, Space and Missile Defense Systems, and Live-Fire T&E).

2. REQUIREMENTS:

The contractor shall:

a) **Threat Intelligence Support and Reporting:** Provide specialized technical and programmatic support to fulfill diverse mission requirements of threat intelligence reporting support to the DOT&E. Coordinate briefing topics with the DIA ESO and provide, as required, intelligence briefings to DOT&E and other organizations as directed. Support, as required, T&E events, threat working groups, and DIA and Services Threat Steering Groups responsible for the Validated Online Lifecycle Threat (VOLT) assessment reports and System Threat Assessment Reports (STARs)) to work requirements promoting threat operational realism during T&E. Monitor, review, and report intelligence activities to provide DOT&E AOs with current threat intelligence assessments that provide the relevancy on impact to U. S. weapon system acquisition programs. Provide weekly intelligence highlights for each of the warfare directorates which support the DOT&E. Provide quick reaction on-site intelligence support to the DOT&E staff and support organizations. Document and maintain current intelligence assessments on threat topics of high interest to the DOT&E staff. Review intelligence mission data requirements (IMD) and Lifecycle Mission Data Plans for programs and action officer support. Submit COLISEUM tasks as required. Identify Foreign Material Program requirements and IMD needed for test events early in the acquisition process. Provide support to TETRA in efforts to develop DoD T&E rapid prototyping in support of operational testing.

b) **Threat Resource Analysis and Programmatic Support**: Provide specialized technical and programmatic support to fulfill diverse mission requirements of threat resource analysis and support to the DOT&E. Analyze T&E and intelligence products including:

Initial Capabilities Documents, Capabilities Development Documents, Capabilities Production Documents, Test and Evaluation Master Plans, Test Plans, models and simulation products, ITASE analysis, VOLTs, STARs, Threat Representation Validation and Certification Reports, Service Accreditation Reports, and other relevant products to determine threat resource requirements, availability, adequacy, and shortfalls. This analysis includes the assessment of threat representations (i.e. threat simulator, threat target, and threat models and simulations) current capabilities and shortfalls as related to program specific test events. Evaluate the ability of those threat representations to represent the threat as it is typically configured and deployed. Support includes the following functions or activities:

c) **Threat Modeling and Simulation (M&S) Support:** Provide oversight, technical support and guidance of threat modeling and simulation (M&S) used to support various test and evaluation (T&E) and ITASE implementations. Support for threat M&S involves interactions and understanding between intelligence community threat M&S developers, T&E facility implementers ranging from all-digital embedding of threat code to hardware-in-the-loop (HITL) labs, to open-air threat test assets, and to T&E stakeholders and resource managers at OSD and throughout the Services. Support requires knowledge for how threat M&S are modified for T&E implementations, modeled and used for ITASE analysis, model wrapping and tool development, tracking distribution, documentation, version and revision controls, problem reporting and associated management processes and procedures. Support involves coordinating and running various meetings of the Radio-Frequency (RF) and Infrared (IR) Threat T&E M&S Configuration Control Board (CCB) which prioritizes and approves threat model requests and change requests affecting threat M&S for T&E. Support wrapping, updating, and testing of models, and reporting of model site reports, followed by the recommending/implementing of model bug solutions as specified by the Government TPOC. Expand and/or reconfigure REDMINE-based website on SIPRNET and software for users of T&E threat FOM and signature models. Integrating model and model components into existing SAM, ATGM, AAM, MANPADS, and other TETRA T&E models. Models shall be tested, configuration managed, verified against the model TTMVVR, and validated against known threat data to ensure correct performance of the subsystems and the end-to-end performance of the models. Provide oversight, technical support and guidance for the TETRA led RF and IR T&E threat models Enterprise and the improvements required to meet RF electronic protection and IR countermeasure T&E needs. Enterprise support includes expanding and organizing the Subversion software configuration system, maintaining threat system and signature models through coordination with DoD test facilities and IC, distributing M&S products and documentation to TETRA customers, analyzing and correcting T&E model change requests to address shortfalls identified by the T&E community, keeping up to date and managing T&E use of M&S hardware products like LIVE, CHIMERA, & ITASE, and running an enterprise M&S Help Desk.

d) **Threat Systems Program (TSP):** TETRA coordinates the overall annual solicitation, review, and approval of threat resource efforts that investigate new technologies and

introduce innovative threat representation concepts into the T&E and training environments. These threat resource efforts promote the exchange of the latest scientific and intelligence (S&TI) information between the Intelligence Community, T&E community, training communities, and Industry to improve the fidelity of threat representations (targets, simulators, and models and simulations) resident in or being developed for hardware-in-the-loop (HITL) test facilities, installed system test facilities (ISTFs), and open air ranges (OAR) used for testing of US equipment and/or training of US warfighters. The TSP facilitates resolution of test threat resource shortfalls by sponsoring studies, analysis, technical investigations, proof of concept demonstrations, and prototype developments of threat representations. The overall objective is to reduce development risk and support the Services in their acquisition of accurate, cost-effective threat representations and to promote technical innovation to stay ahead of near peer threats. Support TSP efforts both technically and programmatically, by analyzing threat resource efforts to determine technical risk, feasibility, and applicability to test and training events including infrastructure. Provide recommendations for new threat resource efforts and focus areas, and support the financial management of threat resource efforts.

e) **Threat Representation Oversight:** Provide technical support at various validation meetings including integrated product team meetings, validation working groups, critical design reviews, internal program reviews, teleconferences, etc. Perform independent technical reviews of Service's threat representation validation reports, processes, procedures, and methodologies. Provide validation report summaries for threat resource analysis support and entry into threat databases. Validation, in this context, is defined as the process of determining the degree to which a simulator, target, model, or simulation is an accurate representation of the actual threat considering its intended use. Provide tailored briefing support related to each validation program under TETRA's oversight. Provide technical and support to TETRA oversight of ITEAMS sponsored efforts.

f) **Foreign Materiel Acquisition and Exploitation (FMA&E):** Monitor Foreign Materiel Acquisition and its availability to support testing and the TSP, and it's inclusion in threat databases (i.e. the Automated Joint Threat Systems Handbook). Coordinate T&E foreign materiel procurement requirements within the DOT&E Warfare Directorates, the Services' Operational Test Agencies, S&TI Centers, and the DIA. Gather T&E Requirements through the Test and Evaluation Subcommittee (TES) for submission to the DoD Foreign Materiel Program (FMP) Top 20 list. Research and gather information on existing acquisition and exploitation projects and determine the ability to support T&E. TETRA's responsibilities include membership and coordination with government agencies both within OSD and outside agencies (i.e. Foreign Materiel Program Board of Director's (BoD), Joint Foreign Materiel Program Committee (JFMPC), the Foreign Materiel Exploitation Working Group (FMEWG), the Foreign Materiel Acquisition Working Group (FMAWG), the Test and Evaluation Subcommittee (TES), and the Manpads Interagency Coordination Group (ICG)).

g) **Database Support:** Analyze, design, develop, test, and integrate web-based information system applications for the Threat Systems Database (TSDB), the DOT&E Database, TETRA Knowledge Online, REDMINE, CFBLnet and other areas of interest as needed. The TSDB is an interactive and classified database of threat representations (including threat simulators, foreign materiel, threat models, simulations, and targets) and test facilities and ranges. The DOT&E Database includes comprehensive program and project financial and programmatic information and other reports, as well as providing an approval mechanism for decision makers. Other areas of interest as needed may include database and web support for specific functional areas not covered by the TSDB, DOT&E Database or TETRA Knowledge Online as well as threat related topics for T&E (i.e. Land and Expeditionary, Naval, Air, Net-Centric and Space, Missile Defense, and Live-Fire T&E Warfare Directorates). Maintain configuration control of the entire product. Document all development, design, and software changes. Ensure the end-product is non-proprietary and possesses complete government rights.

h) **Cyber Threat Folders:** Design, develop, maintain, update, and distribute cyber threat folders as required. Analyze, design, develop, test, and integrate cloud-based cyber threat folder repository on JWICS, SIPRNet, and NIPRNet.

i) **Artificial Intelligence, Machine Learning, and Neural Networks:** Assist, design, develop, maintain, update, and distribute T&E specific Artificial Intelligence, Machine Learning, and Neural Networks tools as required. Analyze, design, develop, test, and integrate AI-based tools on JWICS, SIPRNet, and NIPRNet.

j) **Exercise Support Team:** Provide all-source cyber intelligence analysis in support of the DOT&E Cybersecurity Assessment Program. Provide specialized technical support to by producing, organizing, and developing cyber related intelligence products and packages to enhance the ability of DoD Certified Red Teams to represent realistic cyber adversaries during DOT&E, Combatant Command (CCMD) and Service-level Exercises. Assist in development of the assessment plan, provide on-site exercise support. After each supported exercise, provide a report that describes the realism of the cyber threat emulated. Provide deployment capability for EST and joint EST/TETRA Cyber Intelligence Team.

k) **Scientific and Technical Improvements Needed for Developing Advanced Technology Threats:** Identify potential candidate threats, technology gaps, and candidate solutions for further study. Prepare candidate project documentation suitable for entry into the Test Resource Management Center (TRMC) Test and Evaluation Science and Technology (T&E S&T). TETRA facilitates the development of new threat test assets that support operational test and evaluation. Some advanced technology threats require new and innovated methods to adequately represent those threats in a realistic operational environment.

l) **Working Groups, Specialized Studies, Analyses, and other Mission-Related Functions:** TETRA plans to use working groups to explore, study and report on specific

ways to improve threat representations used in operational test and evaluation. TETRA is working threat systems collaborative relationships with the US FVEY partners and other allies to share threat test information. Provide engineering, technical, administrative and programmatic support as needed for working group activities. Support working groups by coordinating meetings, identifying technical areas that can benefit from additional analysis, providing subject matter experts, publishing appropriate documents, and other associated duties that are critical to success. Obtain and/or provide diverse technical expertise to meet needs for specialized working groups, services, support, material, and studies to support TETRA. Obtain and/or provide diverse and flexible technical expertise, on short notice, as needed for any size task. Provide the ability to access engineers, computer scientists and other specialty disciplines from a broad range of technical experts. Expertise includes radio frequency engineers, aerospace engineers, intelligence analysts, threat representation hardware and software developers, chemical/biological specialists, Electronic Warfare specialists, Information Operation specialists, and cyber experts. Form working groups composed of outside experts, government officials, and other members to research and report on the identified issue areas as needed. Support multiple working groups at the same time, as required. Identify, organize and execute committees of experts to address a broad array of technical issues, evaluate existing policies and make recommended changes, evaluate emerging threat technologies and determine their effect on US weapon systems, evaluate proposed projects, perform special studies, and participate in working groups.

m) **Next Generation TSPI Advanced Satellite Navigation Receiver (ANSR) Support:** Provide support to T&E and TETRA efforts to develop and maintain GPS high-fidelity, high-dynamic next generation Time Space Position Information (TSPI) 6 Degrees of Freedom TSPI ASNR Support requirements reviews and engineering assessment of ASNR to include current standard & future Test and Evaluation requirements managed by the TETRA AGILE process.

n) **Next Generation Machine Learning Model, Deep Learning Model, Cyber, Space and Artificial Intelligence T&E Tools:** Provide support to T&E and TETRA efforts to develop and maintain varying-fidelity, high-dynamic Machine Learning Model, Deep Learning Model, Cyber, and Artificial Intelligence T&E Tools. Support TETRA efforts to staff and man a T&E specific Cyber and Modeling/Simulation Lab. Support TETRA efforts to grow and support IC and DOT&E efforts to improve Space and Counterspace Test and Evaluation.

3. PERIOD OF PERFORMANCE:

The period of performance is a five (5) year base period with an additional five (5) year option period that may be exercised by the Government.

4. PLACE OF PERFORMANCE:

Performance under the contract will take place either at Government and/or contractor sites. The primary Government work sites are the Defense Intelligence Agency (DIA) Missile and Space Intelligence Center (MSIC) Building Complex, Fowler Road, Redstone Arsenal, AL; the Mark

Center Building, Alexandria, VA; the JFMPO at Reston, Virginia and the Pentagon, Arlington, VA.

5. WORK SCHEDULE:
Work hours shall be the same as the Government, while performing at DIA/MSIC, Mark Center, and Pentagon facilities. Core duty hours are defined as 0700 to 1700 hours, Monday through Friday.

6. TRAVEL:
Travel to other locations may be necessary to perform mission-related work. All travel shall be approved by the Government Contracting Officer's Representative prior to travel. All travel shall be in accordance with the Joint Travel Regulations.

7. SECURITY REQUIREMENTS:
All personnel located within DIA/MSIC, Mark Center, and Pentagon office space shall maintain a TS/SCI security clearance.

8. GOVERNMENT FURNISHED EQUIPMENT:
Office space and access to required DIA/MSIC and DOT&E computers, MSICnet, IC and TMAP models, SIPRnet, JWICS, computer networks and software for use on the contract.

9. DELIVERABLES:
A monthly status report and a performance and cost report shall be required under this effort.

10. CONTRACING OFFICER'S REPRESENTATIVE (COR):
Bryan McWilliams, MSIC7, 256-313-7712 is the COR.

11. CONFLICT OF INTEREST: In that contractor personnel will have access to proprietary data and/or Government financial information, the following or similar provision is required to be signed and included in this contract. "Evaluators (contractor and/or its subcontractors) understand that they will be provided proprietary and/or financial data during the course of performance of their evaluations. It is understood that all proprietary data shall not be disclosed to other than Government officials on a "need to know" basis or persons as designated by the Contracting Officer. It is further understood that all data shall be carefully guarded and under no circumstances used for financial or personal gain by the contractor or its employees.

The contractor for the duration of this contract shall not engage in evaluation, review or other related tasks regarding Threat Systems that the contractor has developed or otherwise has a substantial financial interest in. If this situation arises, the Contracting Officer shall be notified immediately. Moreover, should a contractor and/or its subcontractor(s) determine that work under this contract may jeopardize their future interests, the Contractor and/or its subcontractor(s) shall notify the Contracting Officer for resolution."