EXHIBIT A

Technical Objectives for Request for White Papers W911SR-14-2-0001 RWP-1701

Please see EXHIBIT B for Reference Documentation on Topics #5, 6, 7 & 8.

Topic #1: Models for use in Predictive Toxicology evaluating organophosphate compounds "Funding is Subject to Availability of Funds"

The United States Department of Defense is looking for ways of screening large numbers of compounds which may pose an acutely toxic threat to the warfighter. There is currently a need for the development of models to quickly generate data on the toxicity of various commercially available compounds including those from families similar to the various classes of chemical weapons agents: nerve (organophosphates and organophosphonates), blood, blister and choking. Particularly of interest are compounds that do not require first pass metabolism for toxic effectiveness. These models can include *in vivo, in silico* and *in vitro* systems. The goal would be to generate high-throughput/high-content screening technologies to develop robust and flexible tools to screen compounds for acutely toxic effects. Data generated from these efforts could include information relating to cell toxicity (cell culture or primary cells), metabolism (Cytochrome P450 and other metabolic pathways), genotoxicity, hERG inhibition, or any other endpoint that can be used to predict acutely toxic outcomes in the warfighter. There are several areas of interest:

a. Development of high-throughput *in vitro* assays suitable for assaying acute toxicity of high-volatility compounds
b. *In vitro – in vivo* correlation and validation
c. *In vitro* and *in vivo* cross-species correlation and validation
d. *In silico – in vitro correlation and validation*
e. *In silico – in vivo* correlation and validation

Proposals should include model(s) being proposed, data to be collected, and (if applicable) how data will be analyzed to determine correlation/validation and extrapolation to the human. Proposals should have clear deliverables and describe milestones and/or metrics for measuring progress towards those deliverables. Additionally, the proposals should include clear go/no-go decision points for moving forward between tasks and/or options. Finally, offerors may submit multi-year proposals, but it should be with the understanding that if the effort is selected for funding, then only the first year of funding is guaranteed; funding for the optional years will be based on the effort's performance, the needs of the program and the availability of funds.

Technical Point of Contact: Dr. Robert Kristovich, ECBC, 410-436-4239, robert.l.kristovich.civ@mail.mil

Topic #2: Science of Chemical and Biological Protection: "Funding is Subject to Availability of Funds"

The protection of the Warfighter is critical when operating in a hazardous environment. Protective clothing, respiratory protection, and hazard mitigation processes are all components to this topic. Fundamental science in protection includes the development of novel multifunctional materials that perform multiple functions such as adsorption, catalysis and sensing. Also included is the development of advanced personal protective equipment (such as masks), novel air filtration and purification technologies, and associated enabling materials/research. New chemistries for hazardous material decontaminants are also desired as well as further elucidation of the methods and processes by which decontaminants and contaminants interact with materials.

Research areas include but are not limited to:

1. Novel filtration media
2. Integrated protective fabrics
3. Dynamic multifunctional materials
4. New decontamination formulation development
5. Reactive coatings
6. Decontamination profiles (contaminant-material-decontaminant interactions)

Technical Point of Contact: Dr. Rick Cox, ECBC, 410-436-2313,
frederick.j.cox16.civ@mail.mil

Topic #3: Science of Chemical and Biological Sensing: “Funding is Subject to Availability of Funds”

The science of CB sensing advances fundamental understanding of materials or technologies that demonstrates the capability to correctly categorize or identify CB agents. This research thrust involves exploration and exploitation technologies that are capable of detection agents in multiple states of matter (solid, aerosol, vapor, liquid) and in various areas (surface or air).

This thrust ranges from a hand held detection system that can sample air or detect threats on a surface to a network of low cost, low power detection systems that communicate with each other to a larger network, to a hand held diagnostic system that performs genetic sequencing to confirm if someone has been exposed. Discovering the enabling technologies that make these types of systems work is paramount to the advancement of CB defense. Technologies that enable a low cost all-hazard environmental collection capability are also desirable.

This thrust also involves the capability of multiple sensor information to be fused into comprehensible decision management systems. The methods may include analytical, computational or numerical, or experimental means to integrate knowledge across disciplines and improve rapid processing of intelligence and dissemination of information.

Research areas include but are not limited to:

1. Novel detection methods for chemical and biological agents
2. Miniaturization and ruggedization of detection components
3. Universal sample collection, preparation, and preservation for environmental and/or clinical applications
4. Chemical and biological diagnostics
5. Low cost long shelf life biological reagents
6. Environmental biological sensors (distinguish between biological and viral, real time low cost lightweight)
7. Mass spec for biological detection and/or diagnosis
8. Algorithm development for enhanced data fusion of detection data
9. Technologies for attribution of chemical and biological events

Technical Point of Contact: Ms. Cindy Swim, ECBC, 410-436-6626, cynthia.r.swim.civ@mail.mil

Topic #4: Smoke and Obscuration Science - "Funding is Subject to Availability of Funds"

The objective of the this topic is to develop materials and demonstrate weaponization feasibility to provide full spectrum screening (as required) to defeat or degrade threat target acquisition, ranging and marking, tracking, anti-tank guided missiles, and directed energy weapon systems. A major effort under this program involves developing the capability to provide effective obscuration in the UV, visible, IR, and microwave regions of the electromagnetic spectrum. Combinations of these four regions (multi-spectral) are also of interest.

ECBC is interested in innovative concepts to address the following areas of study: - High yield visual, IR and microwave obscurants on the battlefield; Dispersion technology for nanoparticles (conductive flakes and fibers); Improved screening material packaging, compaction, feed, and deaglomeration technologies; Visual, IR and microwave obscurants that are environmentally safer and/or less toxic than current materials; Identification of candidate multiband screening material; Improved dissemination of materials; Techniques to measure screening effectiveness and obscurant generating equipment effectiveness; Aerosolization of obscurant materials; Effects of smokes and obscurants on the battlefield; Vulnerability analysis of threat sensor systems versus obscurants; Nanoparticle obscurant candidates (ultrathin conductive flakes or submicron-diameter conductive fibers that can be aerosolized).

Technical Point of Contact: Mr. Larry Bickford, ECBC, 410-436-2231, lawrence.a.bickford.civ@mail.mil

Topic #5: Offensive Information Operations (OIO) -“Funding is Subject to Availability of Funds”

Requirements: (abbreviated; see TRADOC Pub 525-66, March 08) Force Operating Capabilities (FOCs)

TRADOC FOC –03-08- Information Operations (IO). Information Operations provides the Objective Force with the capability to degrade, deny, delay, deceive, disrupt, destroy, exploit, and/or deny an adversary’s and other’s information and Information Systems (INFOSYS) while protecting friendly information and INFOSYS. The Army requires the capability to counter (disrupt, deny, degrade, destroy, delay, deceive, target, exploit, neutralize, and influence) adversary information networks, C4 systems, and Threat Intelligence, Surveillance and Reconnaissance (ISR) systems; a.k.a. Counter C4ISR for short.

These enemy C4ISR systems may be based on proprietary (nation state military) or commercial technologies. Threat countermeasure options may vary from jamming (both broad area and/or surgical) of the electromagnetic, optic/electro-optic frequency spectrum to applied offensive CNO Tactics Techniques and Procedures (TTP) targeting C4 or ISR systems to cause denial of service effects and/or manipulation of data. TTPs employed can include the use of any technique, technology, or capability that would enable the defeat of the threat capability with the goal of maximizing efficiency, effectiveness and stealth.

Emphasis in development of Offensive IO capabilities will be place in the three general broad categories as follows:

- Surgical communications EW technologies
- Offensive CNO technologies
- EW Techniques research & development efforts

Fundamental Characteristics of New Materiel Solutions:

All newly developed materiel solutions for support of offensive information operations must have the following fundamental characteristics attributed to any modern weapon system or weapon system component, such as:

- Predictability: System will perform as intended
- Repeatability: Results are consistent and repeatable
- Containability: System will not have uncontrollable collateral effects
- Reliability: System will sustain an acceptable degree of availability
- Maintainability: System will not require excessive maintenance
- Sustainability: System will not require excessive life cycle support

Predictability, repeatability, and containability shall be addressed in any early R&D effort leading to a demonstration including breadboard and brassboard experiments. Human factors engineering and other “Ability’s” shall be addressed in connection with the development of a field demonstrable prototype proof of concept system. OIO systems under this Topic must be able to operate in urban, suburban and/or rural environments, or in environments characterized by high number of collateral signals and electromagnetic activity within the associated spectrum.

Preference will be placed on systems that are based on open designs and architectures as well as those facilitating 3rd party development, interoperability, and upgradability as new threats emerge.

Technical Point of Contact: Mr. William Taylor, william.r.taylor6.civ@mail.mil, 443-861-0742 or Mr. Giorgio Bertoli, giorgio.bertoli.civ@mail.mil, 443-861-0743

Topic #5: Sub-topic # 1 – Communications Electronic Warfare “Funding is Subject to Availability of Funds”

Communications Electronic Warfare involves the detection and transmission of RF energy with the goal of disrupting the operation of threat device communications. Communications Electronic Warfare differs from Non-Communications Electronic Warfare in that the target signals are generally transmitting longer, may be modulated in a number of ways to pass information, and may contain error correction and/or noise suppression/anti-jamming techniques enabling operations in low SNR environments that may need to be overcome.

Applications of research in this area are aimed at EW jamming of Threat communications systems (military or commercial) that could be operating in any portion of the electromagnetic spectrum; targeted communications systems could include Radio Frequency (RF) based systems, optical based systems (such a free space laser communications), or directional acoustic systems. Furthermore, target system may be primarily used for voice services, data service or both. Electronic Attack applications could include anything from conventional “barrage” or high power, broad band jamming, to more clandestine, surgical, lower power methods that may overwhelm a target’s ability to receive and/or discern viable signals.

Enabling technologies where R&D emphasis in this area would be of interest could include (but would not be limited to) the following:

- Improved Hardware to include
- Next generation DSP / FPGA Software Defined Radio platforms
- Increased RF front end frequency coverage and Instantaneous BW
- High power and high efficiency amplifiers
- High efficiency RF couplers and combining circuits
- Smart Antenna applications that enable precision application of jamming energy
- Wide RF bandwidth array antennas and amplifiers that enable a single antenna to cover a broad portion of the RF spectrum
- Small, high efficiency lasers operating in optical communications wavelengths
- Precision optical or acoustic aiming or pointing techniques

Technical Point of Contact: Mr. William Taylor, william.r.taylor6.civ@mail.mil, 443-861-0742 or Mr. Giorgio Bertoli, giorgio.bertoli.civ@mail.mil, 443-861-0743

Topic #5: Sub-topic # 2 – Cyber Electronic Warfare "Funding is Subject to Availability of Funds"

This topic differs from Communications Electronic Attack in that the methods and techniques that are of interest predominantly make use of information, protocols, standards, or the logical structure of the signals from which to base an exploitation or attack beyond traditional physical layer EA methods. The environment from which operations could occur ranges from the conventional battlefield, to operations in an urban setting characterized by numerous RF sources and significant numbers of non-combatants, to subterranean locations where RF signal propagation is generally limited. The capabilities include being able to conduct successful operations against a selectable set of threat targets where threat signals, personnel, and equipment may be co-located with non-combatants.

This Sub-topic encompasses –

1. Traditional electromagnetic communications and computer networks and their components
2. Non-traditional electromagnetic non-communications networks; examples may include supervisory control and data acquisition systems and free-space optical communications systems
3. Non-traditional electromagnetic communications networks; examples may include information networked over high voltage power lines
4. Logical information system networks and their components
5. Virtual information networks and their components
6. Traditionally non-radiating cabled communications networks
7. Potential threat operations using commercially available communications and networked systems from within a conventional non-combatant setting (an asymmetric threat)
8. Blue force intelligence support to IO
9. IO support to blue force intelligence operations to include target development, targeting, battle damage assessment and reconstitution operations.
10. IO support to blue operations across the full range of operations and the entire peace-to-war-to-peace continuum

Research and Develop proof of concept capabilities and / or improving existing capabilities to:

- Detect, identify, locate, and map potential adversary (a.k.a. Threat) Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems and nodes and other battlefield communications and non-communications systems, in any operating environment
- Development of capabilities to distinguish threat systems and nodes from non-threat systems and nodes that may be co-located, particularly those in an urban environment
- Locate logical network components associated with critical communication nodes whose geo-locations may or may not be known
- Determine the nature and geo-location of components, systems, or users that may be communicating over a broader backbone communications system

- Surgically destroy, disrupt, deny, deceive, degrade, delay, target, neutralize or influence threat information systems, networks and their components, and threat C4-ISR systems and nodes and other battlefield communications and non-communications systems
- Accomplish surgical Radio Frequency (RF) jamming
- Exploit C4-ISR systems or networks to manipulate data, conduct ES functions, and/or conduct Denial of Service (DoS) attacks
- Operate against C4-ISR systems or networks to manipulate data and/or conduct denial of service, *without direct intrusion into the threat system or network*
- Defeat optic and electro-optic based communications systems

Technical Point of Contact: Mr. William Taylor, william.r.taylor6.civ@mail.mil, 443-861-0742 or Mr. Giorgio Bertoli, giorgio.bertoli.civ@mail.mil, 443-861-0743

Topic #5: Sub-topic # 3 - Computer Network Operations "Funding is Subject to Availability of Funds"

In general, the Intelligence and Information Warfare Directorate (I2WD) wants to obtain expert support for Computer Network Operations (CNO) which is comprised of Computer Network Defense (CND), Computer Network Exploitation (CNE) and Computer Network Attack (CNA). CND is the protection against the enemy's Computer Network Exploitation (CNE) and Computer Network Attack (CNA) and incorporates hardware and software approaches alongside people based approaches. CNE is the ability to gain access to information hosted on or about information systems and the ability to make use of the system itself. CNA is the use of novel approaches to enter computer networks and attack the data, the hardware and the software applications of prime interest. Areas of interest include full spectrum Information Operations (IO) support for the tactical Warfighter, his computer communications interfaces to higher, lower and adjacent commands employing both legacy technology and objective (future force) technologies. Also of interest are long-range visions of the planning, development, implementation and testing of the tactical warfighter's vulnerability and protection concerns in the areas of CND, CNA, CNE, Information Assurance and IO.

CND support shall include but not be limited to:

- Tools, techniques, and procedures to protect against enemy's CNE and CNA
- Perimeter defenses including firewall, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Honeypots, chameleon technologies, and antivirus
- Network integrity systems to ensure that bandwidth is available for mission-critical applications
- Detection, reaction, and restoration capability

CNE and CNA support shall include but not be limited to:

- Network discovery and mapping tools capable of operating in a relatively low bandwidth tactical environment and avoid or circumvent network/host-based IDS
- Destroy, disrupt, deny, deceive, degrade, delay, target, neutralize, or influence threat information system networks and their components, and Threat C4-ISR systems and nodes and other battlefield communications and non-communications systems
- Understand various types of tactics, technologies, and tools used to perform CNO.
- Vulnerability identifications and testing of both wired and wireless networks
- Techniques that can be used to find and route communications data through predefined path (accessible route) or to a particular location (cooperative node)
- Methods for performing both distributed and coordinated CNO missions
- Non-Access dependent CNO technique R&D
- Identification, capture and manipulation techniques for data in transit.
- Stealthy, real time, precise (within one meter) geographic location and mapping of Threat/adversary logical networks and their components. This includes, but is not limited to the following:
    - Individual work stations, terminals, and/or PCs, either networked or stand alone
    - Computer networks of any scale (both wired and wireless)
    - Virtual Private Networks (VPNs) (both wired and wireless)

  - Computer network components (local and/or backbone)
  - Displays PCS and other commercially available wireless device types
  - Government owned or managed private communications networks (military or non-military)
  - Trunked Mobile systems or other networked commercially available communications systems
  - Telecommunications equipment (e.g., Private Branch Exchange (PBXs), corded and cordless phones)
  - Cryptographic components
  - Other peripheral components

- Stealthy, non-cooperative access to logical networks and their components, that overcome threat/adversary best attempts to protect such networks and components. Proposals submitted under this sub-topic shall specify both hardware and software protection measures forming the basis of the target network environment.
- Stealthy, non-cooperative access to RF devices, communications networks and their network components, non-communications networks and their components, and other RF-centric networks and their components, to develop revolutionary TTPs that overcome threat/ adversary best attempts to protect such networks and components. Proposals submitted under this sub-topic shall specify both the hardware and software protection measures forming the basis of the target network environment.
- Stealthy, non-cooperative network discovery software tools, countermeasure capabilities and TTPs that overcome threat/adversary best information assurance/protect measures. Proposals submitted under this sub-topic shall specify both hardware and software protection measures forming the basis of the target network environment.
- Stealthy, non-cooperative network characterization tools and TTPs that overcome threat/adversary best information assurance and protection measures. Proposals submitted under this sub-topic shall specify both hardware, software, and protocol or transmission protection measures forming the basis of the target network environment.
- Stealthy logical network exploitation and/or countermeasure software schemes and TTPs capable of surgically inserting intelligent software agents into threat/ adversary logical networks, regardless of protocols in use or available.
- Stealthy intelligent software agents and TTPs for exploitation and countermeasures of threat/adversary logical networks, and other network-centric networks and their components, and/or Command and Control networks and their components.
- Stealthy component mapping of logical networks and location data correlation and deconfliction with other all-source intelligence data.

Collection, Fusion and overlay of data from, or through the use of other intelligence disciplines (SIGINT, IMINT, counterintelligence CI/Human Intelligence (HUMINT) and/or MASINT) may be required to accomplish any or all of these requirements. If so, Research and Development of TTPs to accomplish this collection, fusion and overlay of pertinent data shall be required.

Technical Point of Contact: Mr. William Taylor, william.r.taylor6.civ@mail.mil, 443-861-0742 or Mr. Giorgio Bertoli, giorgio.bertoli.civ@mail.mil, 443-861-0743

Topic #5: Sub-topic # 4 – Software Agent Technologies "Funding is Subject to Availability of Funds"

The U.S. Army has a requirement to research, develop, test, evaluate, and demonstrate software agents that can be shown to contribute to military operations such as:
Software agents are discrete bundles of computer code that go out onto and into the network environment to perform functions in accordance with their design.
Computer Network Operations (CNO) is comprised of three sub-components that are Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Defense (CND).

- Computer Network Operations2
- Information Operations
- Battle Damage Assessment
- Intelligence and cooperation

Principal topics of interest include but are not restricted to the following:

- agent communication languages and protocols
- agents and complex systems
- agent architectures: perception, action and planning in agents
- agents and cognitive models
- agent-based deployed applications
- agent programming languages and environments
- artificial social systems: conventions, norms, institutions; trust and reputation; privacy and security
- autonomous agent behavior controls for high consequence environments
- coalition formation; teamwork; coordination; middle agents
- evolution, adaptation, and learning
- logics & formal models of agency and multiagent systems: computational complexity
- mobile agents
- multi-agent simulation & modeling
- negotiation and argumentation
- ontologies for agents
- scalability and performance issues: robustness, fault tolerance, and dependability
- synthetic agents: human-like, lifelike, and believable qualities
- theories of agency and autonomy

Technical Point of Contact: Mr. William Taylor, william.r.taylor6.civ@mail.mil, 443-861-0742 or Mr. Giorgio Bertoli, giorgio.bertoli.civ@mail.mil, 443-861-0743

Topic #6: Sub-Topic #1: Radar Technologies and Techniques "Funding is Subject to Availability of Funds"

Requirements: (Abbreviated; see TRADOC Pamphlet 525-66, revised 7 March 2008)
TRADOC FOC-05-01: LOS/BLOS Lethality. Fires are categorized as LOS, BLOS, or NLOS. Engagement range is not directly tied to the definitions of LOS, BLOS, and NLOS fires. Thus, the method used, rather than the range, determines the type of engagement. However, as a general guideline, LOS engagements occur at a maximum range of 5 km, BLOS engagements occur up to 16 km. Some future Modular Force combat systems may have the ability for more than one method (such as LOS and BLOS). Fire control and distribution requires responsiveness with fires on demand to engage complex and simultaneous target sets executed as preplanned or opportunity engagements. Future Modular Force combat systems must be capable of automated precision engagements, with automated fire control, and distribution and clearance procedures with a manual backup. Future Modular Force combat systems must be capable of precision, cooperative, and autonomous/designate LOS and BLOS; and be able to defeat helicopters and UAS.

TRADOC FOC-05-02: NLOS Lethality. Extended range NLOS lethality overmatch is a key component required for all potentially hostile operations, and provides the means to achieve decisive operations, freedom of maneuver, and FP in highly volatile, distributed environments. Capabilities for NLOS fires and effects must extend seamlessly, from tactical to operational levels, with no gaps in coverage, or loss of timeliness. Advanced, automated fire control and distribution means must sort out HPTs and the most dangerous targets rapidly in depth, amongst the vast array of threat intelligence.

TRADOC FOC-07-02: Protect Physical Assets. The continuous and cyclical nature of protecting critical assets is described by the interaction of the force operations activities related to sensing, understanding, deciding, and executing the tasks necessary to ensure attacks on critical assets are avoided. The future Modular Force must be able to monitor, detect, track and engage adversary actions against critical facilities and infrastructure in sufficient time and distance to enable protection activities execution (adequately protecting these facilities and infrastructure and allowing time to assess the effectiveness of protection measures, and provide for sufficient mitigation and negation of these attacks through active and passive measures). Sensing physical attacks, such as air and missile attacks, cyber attacks, and sub-surface attacks against critical facilities will require pulling together multiple sensing capabilities and information input sources.

TRADOC FOC-08-02: Enable Theater Access. Enabling theater access provides proactive means to ensure forces can deploy, and freely enter the theater of operations, by enhancing entry capabilities and infrastructure, mitigating adverse effects of the environment (terrain, weather, enemy action, infrastructure, industrial hazards, and local population), and protecting/facilitating multiple ports of debarkation, LOC, and theater entry points. Once the foothold is established, the focus of enable theater access changes to continuing the flow into, and out of, the theater, as well as enabling 'in-theater access' in support of operational maneuver.

Objectives:
The Intelligence and Information Warfare Directorate (I2WD) seeks innovation in the areas of radar technology development, radar system development, and radar modeling and analysis. The objective of this sub-topic is to provide I2WD with capabilities focused in the following areas:

1. Research, development, test and evaluation (RDT&E) of technologies and techniques which can affordably be inserted into existing and/or developmental ground based radar programs to improve performance and functionality. Possible areas of investigation may include, but are not limited to:

- semiconductor devices, circuit designs, and/or transmit/receive module packaging concepts for providing higher power, improved efficiency and improved reliability over current designs
- beamforming techniques for improved performance: digital beamforming, adaptive beamforming
- multi-static sensor surveillance, both active and passive
- wide-band/multi-band antennas for multi-mission or adaptive-mission capabilities
- improved clutter handling algorithms, improved clutter modeling, adaptive clutter cancellation

2. Research, development, test, evaluation and/or technical analyses of existing, developmental and/or future radar systems to determine methods of or achieving full objective performance against identified capability gaps in the areas of indirect fire weapons location, air surveillance and air defense. This may include design, development and demonstration of prototype radar systems or sub-systems, modeling and simulation, test and/or demonstration of capabilities using developed or existing radar systems. Focus areas may include, but are not limited to:

- achieving full hemispherical surveillance coverage, target tracking and location of a variety of conventional and non-conventional threats (indirect fire weapons, direct fire weapons, top attack, air breathing targets, etc) to support missions such as sense and warn and counterfire target acquisition
- high accuracy tracking to support accurate launch-point-location and/or impact point prediction of indirect fire weapons and cueing to support hand-off to weapons engagement systems
- methods of achieving improved situational awareness through integration, networking and/or cooperative control/cueing of multiple radar systems, or through integration of additional intelligence sources to assist in base and area defense
- multiple-mission capabilities to simultaneously support air surveillance, air defense and aviation requirements
- performance capabilities of existing systems while under varying levels of electronic attack, and countermeasures which can be inserted into existing systems to improve performance while under those levels of attack

Technical Point of Contact: Mr. Jonathan Corriveau, jonathan.p.corriveau.civ@mail.mil, 443-861-1411 or Mr. Joseph Deroba, joseph.c.deroba.civ@mail.mil, 443-861-1516

Topic #6: Sub-topic # 2 – Radar Applications "Funding is Subject to Availability of Funds"

Requirements: (Abbreviated; see TRADOC Pamphlet 525-66, revised 7 March 2008)
TRADOC FOC-02-02: The Ability to Observe and Collect Information Worldwide a. Capstone Capabilities. Observe and collect information worldwide is the ability to detect, identify, characterize, and track items, activities, conditions, and events worldwide of interest to commanders and decision-makers. This capability includes persistent observation, reconnaissance, and information collection from both open and clandestine sources. The following contributing capabilities are critical for observation and collection: ready access by friendly forces, broad area surveillance, focus/stare on targets of interest, and measure and monitor environmental conditions.

TRADOC FOC-03-02: Operations in Urban and Complex Terrain a. Capstone Capabilities. The U.S. military structure, organization, doctrine, and technical capabilities are subjects of study by most nations of the world. These nations understand how our forces will fight, and what type of environments our forces are best suited. Using this knowledge, future opponents will seek to avoid operations in environments for which our forces are optimized. Thus, our adversaries will seek cover and concealment in complex terrain and urban environments, to offset standoff of U.S. forces, and exploit the reduced inter-visibility ranges, to negate technological overmatch of standoff reconnaissance, surveillance, and target acquisition (RSTA) and lethal effects.

TRADOC FOC-04-03: Reconnaissance, Surveillance and Target Acquisition (RSTA) and Attack Operations a. Capstone Capabilities. Conduct RSTA missions in worldwide conditions, day and night in adverse weather to locate targets. Aviation attack assets that can rapidly and precisely engage and destroy/neutralize threats. Threats include fixed and mobile infantryman up to heavy armor and structural targets, such as bunkers or buildings.

TRADOC FOC-05-02: NLOS Lethality Extended range NLOS lethality overmatch is a key component required for all potentially hostile operations, and provides the means to achieve decisive operations, freedom of maneuver, and FP in highly volatile, distributed environments. Capabilities for NLOS fires and effects must extend seamlessly, from tactical to operational levels, with no gaps in coverage, or loss of timeliness. Advanced, automated fire control and distribution means must sort out HPTs and the most dangerous targets rapidly in depth, amongst the vast array of threat intelligence. Aerial platforms add an accurate and immediate third-dimensional sensor and shooter capability to the building fight.

TRADOC FOC-05-01: LOS/BLOS Lethality. Fires are categorized as LOS, BLOS, or NLOS. Engagement range is not directly tied to the definitions of LOS, BLOS, and NLOS fires. Thus, the method used, rather than the range, determines the type of engagement. However, as a general guideline, LOS engagements occur at a maximum range of 5 km, BLOS engagements occur up to 16 km. Some future Modular Force combat systems may have the ability for more than one method (such as LOS and BLOS). Fire control and distribution requires responsiveness with fires on demand to engage complex and simultaneous target sets executed as preplanned or opportunity engagements. Future Modular Force combat systems must be capable of automated precision engagements, with automated fire control, and distribution and clearance procedures with a manual backup. Future Modular Force combat systems must be capable of precision, cooperative, and autonomous/designate LOS and BLOS; and be able to defeat helicopters and UAS.

TRADOC FOC-06-01: Enable Freedom of Maneuver a. Capstone Capabilities. The mobility of the future Modular Force is critical, to maintain the high tempo, and operate over the extended distances dictated by this concept. Enabling freedom of maneuver is one of several key MS enablers of the future Modular Force, and must be developed to its full potential. Enabling freedom of maneuver extends the concept of air corridor suppression of enemy air defense, to ground mobility routes, or corridors. A blanket of sensor coverage will encompass the selected COA, allowing assured route mobility. Sensors will maintain current, updated SU, and sensor-effects links will preclude the enemy from modifying the current mobility situation. The current operational pictures will be fed continuously to JFCs, and area denial systems will prevent enemy alteration. Future requirements for the ISR system include sensors that can distinguish between friendly, enemy, and civilian activities; integration of battlefield sensors; mobility decision aids; and denying enemy forces the opportunity to apply countermobility and surveillance measures.

TRADOC FOC-06-06: Understand the Operational Environment a. Capstone Capabilities. The OE includes physical, informational, and human dimensions. These dimensions are dynamic; they change over time, often in difficult to predict ways. Understanding the OE is real time understanding of the environment (space, air, water, ground, subterranean), including terrain, weather, infrastructure, hazards, populations, and their interaction, impact on operations, and options to leverage or mitigate effects, tailored to the commander's needs. The five basic functions required to fully understand the physical dimension of the OE are: data acquisition, data exploitation, data management, data representation, and data dissemination. Required capabilities include: • Locate and Map Tunnels. Collection, generation and fusion of high-resolution geospatial data, and comprehensive operational environment information, that includes real time collection of new data, as well as supplementing existing data sets with more detail, to Include civil and cultural data. • Exploitation of the full range of sensors (including humans) to gather required operational environment and timely fusion of this data into actionable information. For example, Civil Affairs Team, Civil Liaison Teams, and Civil Affairs Functional Experts collect civil data for project assessments. Accurate, timely, current, relevant and scalable operational environment data that is compatible with the network-centric environment.

TRADOC FOC-07-02: Protect Physical Assets. The continuous and cyclical nature of protecting critical assets is described by the interaction of the force operations activities related to sensing, understanding, deciding, and executing the tasks necessary to ensure attacks on critical assets are avoided, neutralized, or mitigated. The force operations activities and how they are mapped to physical asset protection are as follows: (1) Detect. The future Modular Force must be able to monitor, detect, track and engage adversary actions against critical facilities and infrastructure in sufficient time and distance to enable protection activities execution (adequately protecting these facilities and infrastructure and allowing time to assess the effectiveness of protection measures, and provide for sufficient mitigation and negation of these attacks through active and passive measures).

Objectives:
This topic is concerned with providing an initial / improved operational capability in the following areas:

- Research, development, test, evaluation and/or demonstrations of advanced radar systems. This includes the design, development and testing of prototype devices, subsystems and systems. Applications span short and extremely long ranges and include but are not limited to radar applications for mine detection, counter Explosive Devices, counter sniper, counter munitions, counter fire, combat identification, soldier cueing and protection, battle damage assessment, building penetration, buried target detection, terrain characterization/geospatial data, weapon cueing to targeting, tracking, target location, high resolution stationary and moving target imaging and surveillance, over single or multiple radar bands.
- Tradeoff and other technical analyses to determine performance requirements and/or technological risks, based on current and evolving operational requirements. These should take into account factors such as payload size, weight and power; platform characteristics and limitations, costs, data link limitations, spectrum issues, data generation and distribution timelines, and operator training levels. This can consider the integration of various sensor technologies (EO/IR, SIGINT etc) with radar, to meet user objectives/requirements.
- Analyses design, development and testing of advanced hardware technologies that may include but are not limited to, conformal/reconfigurable antenna designs, T/R modules, and advanced signal processors.
- Research, design, development and testing of advanced exploitation and signal processing techniques for use with monostatic, bistatic, multi-laterated radar. This may include, but is not limited to enhanced angle estimation, low-velocity target detection, target tracking algorithms, multi-dimensional imaging, aided/automatic
- target detection/classification/recognition/ identification, terrain characterization geospatial data, image enhancement, feature aided tracking, pattern recognition, anomaly detection, change detection, impact location, weapon location, automated system resource management/control, and clutter cancellation. Key efforts are to automate exploitation products and radar control as much as possible to minimize operator workload and training requirements.
- Research, design, development, implementation and testing of Electronic Counter Countermeasures (ECCM) for both MTI and SAR modes into existing, emerging or future radar systems. Techniques should also include the ability to precisely locate the source of the counter measure.
- Research, design development, test, evaluation and/or demonstrations of advanced multi-sensor technologies or systems. This includes radar integrated with but not limited to EO/IR and or SIGINT technologies.

Technical Point of Contact: Mr. Jonathan Corriveau, jonathan.p.corriveau.civ@mail.mil, 443-861-1411 or Mr. Joseph Deroba, joseph.c.deroba.civ@mail.mil, 443-861-1516

Topic #6: ISR Sub-topic # 3 – Fusion "Funding is Subject to Availability of Funds"

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
TRADOC FOC-04-01, Sensor Fusion. Fusion is the process in which data generated by multiple sources is correlated, to find the enemy and create information and knowledge. Fusion operates over integrated communications networks, draws relationships between source inputs and provides meaning to the information that has been acquired.

Objectives:
US Army RDECOM-CERDEC Intelligence and Information Warfare Directorate (I2WD) require the following capabilities:

- Development of Information Fusion (IF) software related to advanced IF techniques and those supporting Future Combat System (FCS). This shall include aid in developing new IF system and process software, integration of existing software in IF systems, human-computer system design, fusion visualization and supporting fusion technologies such as data base and fuzzy reasoning.
- Research, development, and maintenance of IF and support software packages and systems. This shall include R&D in the specific area of IF including all levels of IF according to the Joint Director of Laboratory data fusion model and their supporting IF technologies.
- Support of existing and planned fusion R&D activities with commercial or educational institutions. This shall include operational and performance analyses of requirements and capabilities, test and evaluation of existing software and systems, modification of existing software, design and code development of new software and test and evaluation of software and software systems. This shall also include studies & analyses of existing hardware supporting IF functions and their installation, test and maintenance.
- Support of planned and existing I2WD fusion test beds to include current and future field tests and evaluations. Test bed support includes hardware, software, maintenance, and associated supporting technologies as needed. The support shall include the study, design/redesign, and evaluation of existing and planned IF systems.
- Integration of existing IF R&D or working systems such as Defense Advanced Research Projects Agency (DARPA), Coalition, US Navy, US Air Force, Commercial, and other sources into I2WD IF developments. These integrations shall include hardware, software, networking, and associated supporting technologies such as database, visualization and ontologies.
- Support of specific Common Operating Picture (COP) IF technologies including advanced visualization hardware and software, hardware for IF processing, development of software supporting COP IF, including fusion engines, database, and the test and demonstration of these IF technologies.
- Support and create multiple, realistic scenarios for evaluating prototype IF systems, provide studies, and make recommendations as needed for these scenarios.

Technical Point of Contact: Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #6: ISR Sub-topic # 4 – Modeling and Simulation "Funding is Subject to Availability of Funds"

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
FOC-02-06: The Ability to Model, Simulate, and Forecast
Modeling, simulation and forecasting is the ability to utilize BA information to create an environment that allows for modeling, simulating, and forecasting in order to increase understanding, increase confidence, improve the planning (and execution) of COAs, and decrease risk for commanders and analysts. Modeling, simulation, and forecasting activities range from accurate and timely weather predictions through support of operational rehearsals, training exercises, and military education. The following contributing capabilities are critical for modeling, simulation, and forecasting: auto-populate models and simulations; identify enemy courses of action; and integrate cultural, social and other nonmilitary issues into predictive forecasts.

FOC-01-02: Information Operation and Decision Superiority: To achieve information and decision superiority in the future Modular Force requires the following capabilities:

- The ability to provide end-to-end protection, assurance, and validation of information and information systems.
- Oversee the rapid creation of data initialization and starting information.
- Continuously track, shift, reconfigure (for example, control) forces, equipment, sustainment and support, even en route.
- Access and integrate intelligence information and forecasts, including information on adversary, neutral, and non-combatant entities of interest.
- Distribute and update commander's intent and guidance to include commander's critical information requirements, and ensure it is understood.
- Maintain a tailored, relevant, synthesized COP that presents actionable information to promote understanding.
- Provide automated decision aids, planning tools, advanced modeling and simulation, and in-transit visibility to the operational force. Assimilate and dispense knowledge.
- Perform mission analysis across the operational environment.
- Progressive war games and exercises with realistic time constrained conditions that challenge and train commanders and staffs in the execution of effective battle command.
- Red teaming capabilities to rapidly test their plans in all environments and develop alternative approaches that are based on anticipated enemy reactions.
- Provide information delivery methods that are tailored, secure, and allow reprioritization based on mission requirements and available delivery methods.
- Battle command suites similar to today's command post of the future with expanded and updated visualization and information sharing capabilities.
- The ability to minimize communications dependencies via doctrinally appropriate processing and storage of critical/essential information locally, ensure dissemination of critical time sensitive survival information, and allow users to acquire needed information via intelligent searches.

General Description:

The Modeling and Simulation (M&S) efforts focus on the development of tools of forecasting / decision aid and automated situation awareness / understanding for intelligence analysis, influence operations and planning in all aspects of Intelligence Preparation of Battlefield, Intel Collection Planning, near real time Intel analysis and persistent surveillance and automated scenario generation for red, blue, green side experimentation. These include the integrated modeling of strategic / operational / tactical planning and operation and development of a near real-time operational capability to provide the users a set of scalable, portable and interoperable planning tools and methodologies to support the diversified planning and visualization and significantly enhance the performance of simulations, scenario generation process and modeling. The typical effort may include research and advanced technology development of innovative application tools and processes for integration with command capabilities to aid military commanders and planners in plan formulation and assessment of the effects and the progress of an operation. Areas of consideration may include Intelligence Surveillance and Reconnaissance (ISR), operational ontology, data / knowledge generation, data management and collection / dissemination / visualization of data.

Objectives:

- Model development and population (auto or semi-auto desirable) for traditional and non-traditional (civic, cultural, terror cells…) scenario and data generation. Modeling for COA / forecasting support and development of applications in the PMESII (Political, Military, Economic, Social, Infrastructure, information) and HSCB (Human Social Cultural Behavior) domains. Framework and standards development for incorporation of models and System-of-System integration. Development of GUI and display tools for modeling and application utility.
- Develop new and leverage existing simulation tools for supporting application development, evaluation, experimentation, and training. Simulation of sensor and sources for traditional forces and non-traditional force / asymmetric warfare for supporting intelligence exploitation and analysis.
- M&S support in provision of sensor models, scenario generation / constructive simulation, in support of hardware in the loop testing and evaluation for supported Programs of Record.
- Leverage high performance computing for complex M&S problem solving. Investigate emerging computational platforms and architectures for bring solutions to operations.
- True 3-D geospatial simulated environment with the associated electromagnetic and material properties of the environment for high fidelity, interactive physics based M&S.
- Advanced computationally efficient strategies for near-real-time, perceived real-time interactive simulations of multi-INT sensors immersed in an electronically rich environment (e.g. urban).
- Novel, innovative concepts for simulation architectures in a distributed, interactive environment, and capable of interactive simulation with traditional simulation paradigms (i.e., HLA and DIS).

Technical Point of Contact: Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #6: ISR Sub-topic # 5 – Multi-Intelligence Analysts Functions "Funding is Subject to Availability of Funds"

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
TRADOC FOC 03-03, **Advanced Collection, Processing, Analysis, Management and Sharing of Information.** Adaptive reasoning tools that automatically collate and transform sensor data into knowledge, and support it via accessible national to tactical common databases, capable of providing tailorable intelligence products to users, at all levels. Information management tools are required, permitting the Objective Force to precisely and automatically process, fuse, focus, distribute, and display information in the form most appropriate to the user.

TRADOC FOC 03-07, Decision and Planning Support. Tools and techniques must provide an automated, running estimate of the situation. It will also provide commanders and battle staffs with automated cognitive decision aids and real-time distributed, multiechelon collaborative planning support tools, to achieve knowledge-based course(s) of action development, wargaming, and decision support. Systems must be mobile, fully interoperable in the joint, multinational, interagency operational environment, and tied into the protected, network-centric, assured communications architecture to include reach-back.

Objectives:
This topic is concerned with providing an initial/improved operational capability in the following areas Research and development (R&D) of unattended systems/subsystems that utilize Software Agent technology to provide analysis of intelligence databases with the goal of automating the processes performed by intelligence analysts, planners and data base administrators. This effort would include testing and integration of developed items.
R&D of unattended systems/subsystems that automate Intelligence (INTEL) analyst's tasks: Systems/subsystems would include means to update and/or retrain the system so it could analyze new threats. This effort would include the testing and integration of any system or subsystem.

Technical Point of Contact: Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #6: ISR Sub-topic # 6 – Biometric INTEL Processing “Funding is Subject to Availability of Funds”

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
TRADOC FOC-02-03: The Ability to Collect and Manage Biometric Data
Biometric data collection, processing, and analysis are rapidly becoming a critical element in fighting the global war on terrorism. Units require the ability to identify and track individuals at standoff distances. Identification techniques must be both near real time, accurate, and take into account uncooperative individuals. There is also a requirement to track and distinguish friendly personnel from a distance.
Objectives:

- Development of Multi-modal Biometric analysis tools to improve categorization and identification of individuals. This shall include the storage, data mining and linkage / Association of Biometric data to other Intelligence events. Areas of interest are Facial recognition, Voice pattern analysis and physiological phenomena.
- Development of High performance computing / rapid processing of Biometric data. This shall include methods to quickly categorize individuals that can’t be accurately identified.
- uncooperative standoff surveillance, tracking and exploitation
- identification methods without pre-enrollment

Technical Point of Contact: Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #6: ISR Sub-topic # 7 – INTEL & Battle Command Collaboration “Funding is Subject to Availability of Funds”

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
TRADOC FOC-02-04: The Ability to Manage Knowledge
Knowledge management includes horizontal and vertical integration of information from sensors, analytic centers, and decision-makers. Given that the nature of information is both synergistic and contextual, it is critical that analysts and agents be able to access past information to derive maximum benefit from the current findings. Effective knowledge management is critical to understanding the OE to enhance maneuver support (MS).

Objectives:

- Development of algorithms that dynamically manage INTEL requirements and plans in support of Battle Command. This shall include the automated/semi-automated processing of CCIR / PIR data, Intelligent Preparation of Battle (IPB), Course of Action development, and Combat Assessment. Research shall address the dynamic nature and OPTEMPO of the battlefield environment and the collaboration required with Battle Command.
- Development of algorithms to assist the analyst in the refinement of the Enemy Situational Awareness (i.e., Red Picture) via the utilization of Blue Force Tracking data. This shall include the ability to maintain track ID given varying rates of target track updates and establish track ID confidence levels.
- Development of Collaboration services between INTEL and Battle Command for rapid decision making support.

Technical Point of Contact: Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #6: ISR Sub-topic # 8 – Collection & Sensor Management "Funding is Subject to Availability of Funds"

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
TRADOC FOC-02-05: The Ability to Execute BA Assets
The commander must be able to execute BA assets worldwide under a range of conditions. The BA structure must be modular and tailorable in order to fit with a variety of organizations across the ROMO. Examples include the capability to synchronize BA with operations, task and dynamically re-task assets, monitor/track assets and their activities.

Objective:
Development of algorithms and Services that support Sensor and Collection Management. This shall address the organic / non-organic assets and collection plans, prioritization of information requirements, dynamic tasking / re-tasking of assets and tracking of requirements status. Areas of interest are in semi-automated and automated tools, data ontology for Sensor / Collection management, and organic /non-organic asset tracking.

Technical Point of Contact**:** Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #6: ISR Sub-topic # 9 – Human Terrain (HT) / PMESII Data Exploitation and Analysis "Funding is Subject to Availability of Funds"

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
TRADOC FOC-02-01: Processing, Analysis and Reporting of Intelligence Information. Analysis of Intelligence Information is the ability to use open and protected methods to discern patterns, opportunities, and vulnerabilities, and characterize information concerning an adversary and the operating environment in order to facilitate superior decision-making. This capability is a combination of both ability to conduct detailed, in-depth analysis of very specific phenomenology and the ability to fuse information from a wide variety of sources in order to create valuable insights and actionable, relevant information.

General Description:
Human Terrain (HT) Initiative is part of socio/cultural dynamics of the Irregular Warfare Focus Area within DOD's Battlespace Awareness (BA) portfolio. Social science research of a host population produces a knowledge base which is referred to as the "Human Terrain". Human Terrain may include information about the physical security, economic security, ideology and belief systems, authority figures, and organizations relevant to major social groups in the area under study. This information comes from open source, unclassified collection and must be referenced geo-spatially, relationally, and temporally in systems by a team of personnel to enable the creation of various "maps" of the human dynamics. The aim of this field research is to provide an in-depth understanding of the highly complex local socio-cultural issues and to respond effectively to decision-makers on human terrain related Information Requirements (IR). Example of IR may include insights into issues of ethnicity, tribes, society, the political environment, micro and macroeconomics, religion, the insurgency and security at the designated regions of interest.

Objectives:

- Development of Social Science Research and Analysis (SSRA) capability at the regions of interest by conducting quantitative and qualitative research on issues in PMESII (Politics, Military, Economics, Social, Information and Infrastructure) environment within operational relevance of the Human Terrain System effort.

- Development of capabilities to aid decision-makers and planners in achieving socio-cultural understanding of the local population in tactical operational areas using HT/PMESII data generated by a combination of qualitative and quantitative (polls, focus groups and semi-structured interviews) techniques. Support of social science analysis via timeline analysis with visualization and temporal correlation across multiple domain and visual display of trends of interest and generation of automated chronology with linkages of events across topics for designated issues.

- Enhancement of tool design and development (capability, algorithms, interface, test, evaluation, etc.) with the required features (maps, link charts, timeline, visualization, reports, etc.) for exploitation and management of HT / PMESII / open source data to support unit commander's operational decision-making processes.

- Development of techniques, algorithms and framework for exploiting and tracking capabilities and trends from correlation and analysis of the HT / PMESII data**.**

- Performance of high order analysis to generate quantitative (graphical and numerical representations of the data) and qualitative (textual/descriptive) analysis of socio-cultural data.

- Leverage of the existing modeling solutions & capabilities, tools, techniques to develop Intelligence / HT / PMESII / open source data models and reasoning components to discover the dynamic relationships among individuals / organizations and identify patterns and trends in the data**.**

- Development and refinement of the trend analysis models to illustrate the predicted intents and the primary and follow-on effects of the activities of individuals and groups under various situations**.**

- Development of capability of predicting target adversary behaviors based on exploitation of patterns and trends in activities of people of interest within PMESII motivation environment from the intelligence and open source data.

- Expansion of existing intelligence / HT / PMESII data models (events, individuals, organizations, facilities, equipment, etc.) to take into account dynamic, sophisticated relationships and identify social/behavioral/functional/technical/ organizational patterns and trends in the data

Technical Point of Contact: Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #6: ISR Sub-topic # 10 – INTEL Exploitation and Analysis "Funding is Subject to Availability of Funds"

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
TRADOC FOC-02-01: Processing, Analysis and Reporting of Intelligence Information. Analysis of Intelligence Information is the ability to use open and protected methods to discern patterns, opportunities, and vulnerabilities, and characterize information concerning an adversary and the operating environment in order to facilitate superior decision-making. This capability is a combination of both ability to conduct detailed, in-depth analysis of very specific phenomenology and the ability to fuse information from a wide variety of sources in order to create valuable insights and actionable, relevant information

Objectives:

- Development of Exploitation tools to extract events, objects, and activities from intelligence data for reporting, correlation and dissemination in support of Distributed Common Ground System-Army (DCGS-A). This shall include the detection & identification of events/objects in the data, metadata tagging of the extracted information, data mining for objects/events, and the storage of the data with metadata tags. INTEL areas of interest are Full Motion Video, Imagery, Terrain data, Human reports (e.g., Situation Reports (SITREPs)) and Open Source data.

- Development of Analysis tools to detect / discern patterns and relationships between events, objects, organizations and people in support of DCGS-A. This shall include the ability to assess political, military, social and behavioral phenomena and relationships. Research shall address the ability to forecast behavior from historical information.

- Development of Exploitation tools to utilize Blue Force Tracking data to refine and improve Enemy situational awareness.

- Development of Multi-INT exploitation and analysis tools to detect patterns, characterize objects / entities, and track activities.

Technical Point of Contact: Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #7 Fusion Sub-topic # 1 – ISR Exploitation Supporting Fusion "Funding is Subject to Availability of Funds"

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
TRADOC 4-19. FOC-02-07: Fusion. Fusion is the critical technology that underpins these components and in many circles has become synonymous with BA functions. Fusion, by definition, is a series of processes to transform observable data into more detailed and refined information, knowledge, and understanding. These processes, by their very nature, involve a mixture of automation and human cognition. All of the capstone capabilities required and outlined above have one or more aspects of fusion embedded within their constructs.

Objectives:

- Develop a rigorously stated mathematical approach, which may be either statistical or deterministic in nature that would provide a commonly accepted set of metrics to identify the value of observable data provided by battlefield sensors based on the characteristics of the sensors.
- Determine whether additional data from sensors enhance or degrade the fuse solution based on the value of the observable data provided by the sensors, i.e., provide a mathematical means to determine what could be gained or lost by the use of additional sensors.
- Use the observable data as the basis for determining what information can be gleaned from the sensor(s) i.e.; what do they tell us and how?
- Determine what data is required, and what the parametric requirements of the additional sensor(s) should be in order to enhance the fused solution.

Technical Point of Contact: Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #7: Fusion Sub-topic # 2 – Predictive Analysis and Estimation "Funding is Subject to Availability of Funds"

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)
TRADOC FOC-02-06: The Ability to Model, Simulate, and Forecast
Modeling, simulation and forecasting is the ability to utilize BA information to create an environment that allows for modeling, simulating, and forecasting in order to increase understanding, increase confidence, improve the planning (and execution) of COAs, and decrease risk for commanders and analysts. Modeling, simulation, and forecasting activities range from accurate and timely weather predictions through support of operational rehearsals, training exercises, and military education. The following contributing capabilities are critical for modeling, simulation, and forecasting: auto-populate models and simulations; identify enemy courses of action; and integrate cultural, social and other nonmilitary issues into predictive forecasts.

Objective:

- Research and development in pattern analysis, modeling and prediction of Enemy Course of Action (COA) and behavior. This shall include the Political, Military, Economic and Social data to support behavioral analysis. Areas of interest are in linking people, events, organizations and activities to forecasted outcomes.

Technical Point of Contact: Mr. Alan Hansen, alan.s.hansen4.civ@mail.mil, (443) 861-0763 or Mr. Kesny Parent, kesny.parent.civ@mail.mil, (443) 861-0765

Topic #8 Title: Command and Control Protect, Network Vulnerability, C4ISR Penetration Testing and Vulnerability Analyses "Funding is Subject to Availability of Funds"

Requirements: (abbreviated; see TRADOC Pub 525-66, March 08)
TRADOC FOC –03-04 Network Operations. Network operations consists of communications and the means to effectively protect and manage the flow of information, through prevention, monitoring, detection and dynamic prioritization, allocation and response.

TRADOC FOC –03-05 Information Protection. Objective Force networks must provide Protect, Detect, and React capabilities that protect the system's integrity and confidentiality, prevent unauthorized access, and reduce the probability of intercept and exploitation by hostile forces.

TRADOC FOC –03-08 Information Operations. Information Operations (IO) enables the Objective Force Commander to shape adversary perceptions, reduce the effectiveness of an adversary's combat capability, reduce the ability of others to influence the success of military operation, and protect friendly and supporting C4ISR in IO system, and the information that they provide.

TRADOC FOC –10-01 Understanding the Battlespace Environment. Opponents will try to counter U.S. strengths by attacking, or exploiting, our weaknesses, especially our critical dependence on C4ISR, so vital to our synergistic, system-of-systems approach.
Notes:

1. Vulnerabilities of U.S. C2 or C4ISR systems or their components shall be classified SECRET.
2. Vulnerability assessments, penetration testing, exploitation, countermeasure development, or the development of tactics, techniques and procedures, having a focus that is Threat / adversary-based, shall not be undertaken under this topic.
3. No classified materials, software, tools, tactics, techniques or procedures shall be developed under this topic.
4. Classified tools for IO shall be developed under the IO Attack topic and sub-topics of this Topic.
5. Contractors working under this topic shall not have access to classified tools.

Objectives:
The Intelligence and Information Warfare Directorate (I2WD) wants to obtain expert support for Network Vulnerability analysis, penetration testing and vulnerability analyses of U.S. Army tactical C2 and C4ISR systems and their supporting Radio Frequency (RF) networks and logical networks. Information Assurance (IA) capabilities of U.S. Army C2 and C4ISR systems shall be characterized and evaluated, considering known or projected potential threats, within the following mission areas:

- Electronic Attack (EA),
- Signals Intelligence (SIGINT)
- Computer Network Operations (CNO) to include
    - Computer Network Defense (CND)

  - Computer Network Exploitation (CNE)
  - Computer Network Attack (CNA)

Required support shall include an analysis of fielded, soon to be fielded, or candidate / developmental U.S. Army C2 and C4-ISR systems, hardware and software to:

- identify vulnerabilities
- support system exploitation for vulnerability testing purposes
- stress Information Assurance (IA) capabilities
- gain network access
- identify high value targets
- execute attacks for penetration testing and vulnerability assessment purposes only

Publicly available unclassified tools are of particular interest due to their availability. I2WD objectives are to identify and report C2 and C4ISR network and host based vulnerabilities to the appropriate Program Executive Office (PEO) and/or Program Manager (PM).
I2WD is developing a process for conducting classified vulnerability analyses and is interested in acquiring and integrating hardware/software tools that are –

- freely and openly available
- Commercial Off-The-Shelf (COTS)
- Government Off-The-Shelf (GOTS)

Acquired and integrated tools shall be used to conduct vulnerability analyses and exploitations of U.S. Army C2 and C4-ISR systems. The rules of engagement for vulnerability assessments are according to a strictly adhered to four-step process. One is not permitted to omit or skip steps. The four-step process is:

1. Gain network access
2. Identify high value targets
3. Identify vulnerabilities
4. Execute attacks

Network access - Network access must be obtained in-order to execute a CNA on a target system or host. Gaining access can be a particularly challenging task in a stand-alone network. Systems that have connectivity to external networks typically have security architectures in place for protection. An attacker gaining access through a Radio Frequency (RF) link or through an externally connected network is commonly referred to as an “outsider”. In Army tactical networks there are likely to be several layers of protection that an outsider would need to penetrate prior to launching an attack. Tools, techniques, and procedures used to protect Army communication networks and information system networks include firewalls, routers, access control, communication security, and transmission security.

Electronic reconnaissance - Electronic reconnaissance refers to methods and tools used to inspect or explore an adversary’s communication systems and information systems networks.

- Due to the wireless nature of tactical networks, a combination of computer network discovery efforts and selected Signals Intelligence (SIGINT) data is required to develop a coherent and useful electronic reconnaissance product.

- Network discovery tools shall be capable of operating in a relatively low bandwidth tactical environment and be able to avoid or circumvent network based Intrusion Detection Systems (IDS).

Surveillance - Surveillance refers to the observation of computer network information systems for the purpose of determining high value targets.

- As with electronic reconnaissance, surveillance can be accomplished using SIGINT and computer network based data collection. SIGINT (Communications Intelligence (COMINT) and Electronic Intelligence (ELINT)) tools are used to determine emitter types, duty cycle, and technical parameters.
- Network "sniffers" and other logical networking tools are used to determine message types, traffic loads and technical parameters of logical networks. Information from each set of tools, or a combination of tools, shall provide valuable information for identifying critical nodes and high-value targets. Logical network tools must function in a relatively low bandwidth tactical RF environment.

Exploitation - Target candidates must be technically exploited prior to developing a targeting or attack strategy. Electronic Support (ES) supports electronic attack (EA). Computer Network Exploitation (CNE) supports Computer Network Attack (CNA).

Targeting - In intelligence parlance, "targeting" can refer to identifying and characterizing a critical node, determining the physical location of the critical node, then passing that data to a "shooter" or "cyber warrior" for physical or electronic attack.
In the RF world, direction finding and geo-location tools are valuable for physical targeting. CNE is an essential prerequisite for CNA targeting. Unclassified CNE and CNA vulnerability assessment tools shall be capable of operating in:

- a low bandwidth, low data rate RF digital data environment typically found at tactical levels of operation [e.g., the Single-Channel Ground and Airborne Radio System (SINCGARS) combat net radio, its interface with the Enhanced Position Location Reporting System (EPRLS) and Battlefield Functional Area host computers].
- the presence of U.S. Army host Intrusion Detection Systems (IDSs), and other hardware and software protection schemes.

Technical Point of Contact: Mr. William Taylor, william.r.taylor6.civ@mail.mil, 443-861-0742 or Mr. Giorgio Bertoli, giorgio.bertoli.civ@mail.mil, 443-861-0743

Topic #8: C2 Sub-topic #1 - Blue Attack Blue “Funding is Subject to Availability of Funds”

Under this topic I2WD is interested in assembling, fully integrating, and dynamically maintaining a world-class suite of system-of-systems unclassified and openly available COTS and GOTS, Electronic Attack (EA), CNE and CNA tools and Tactics, Techniques, and Procedures (TTPs). The purpose of these attacks is for vulnerability assessment, and penetration testing of our own, U.S., C2 and C4-ISR systems.

- Our objective is to disrupt, deny, degrade, destroy, delay, deceive, target, neutralize, or influence U.S. Army C2 and C4ISR systems, and the authorized users of those systems, using the same tools that a potential Threat / adversary could assemble, integrate, and maintain from unclassified open sources.
- I2WD assumes that a potential Threat / adversary would not have access to our (U.S. and allies) classified attack and protect tools and TTPs.
- If we possessed CNE and/or CNA tools of an actual Threat/adversary, the fact that we possessed them and the tools themselves would most likely be highly classified and perhaps compartmented. An actual adversary’s tools could be used within the context of a real world, classified war plan-driven scenario.

Technical Point of Contact: Mr. William Taylor, william.r.taylor6.civ@mail.mil, 443-861-0742 or Mr. Giorgio Bertoli, giorgio.bertoli.civ@mail.mil, 443-861-0743

Topic #9: Integrated Software Reliability Process "Funding is Subject to Availability of Funds"

Across the Department of Defense, 70 percent or more of a given weapon system's lifecycle costs are associated with product sustainment. Any shortfalls in system reliability contribute significantly to those sustainment costs. In many cases, especially in more recent times, software causes a substantial portion of system failures. Early software-focused systems engineering and testing are critical for reducing and eliminating faults. Failure reduction significantly decreases costs for the Department of Defense and increases the ability of Soldiers to execute their missions.

There are a number of software processes and models available in the general literature that have the potential to greatly increase software reliability. Examples include several reliability growth models, the AMSAA software reliability scorecard, defect containment matrices, etc. Although many processes and models exist, there is not a consistent and integrated mechanism for selecting the appropriate tools and applying them to improve a system's reliability (all through the design process and continuing up until the end of full-up system technical testing). The transition from vendor software engineering efforts to customer (e.g., Army) testing is of particular concern.

Some of the major challenges include:

1. Spiral development and/or major upgrades in existing functionality reducing overall reliability (which often violate the assumptions that reliability growth models are built upon);
2. Assessing the status of software reliability in a suitable form to provide risk assessments and support go/no-go decisions throughout development and customer acceptance testing;
3. Transitioning reliability from commercial design and development with a defect management focus to Army customer testing with a focus on operational/safety/cost impacts of observed failures; and
4. Adequate testing and assessment of software reliability in large complex software systems of systems.

Proposals should include models and processes being proposed and how those models and processes can be integrated to successfully improve software reliability throughout development and customer acceptance testing.

Proposals should have clear deliverables and define milestones and/or metrics for measuring progress towards those deliverables. Additionally, the proposals should include clear go/no-go decision points for moving forward between phases and/or options. Finally, offerors may submit multi-year proposals, but it should be with the understanding that if the effort is selected for funding, then only the first year of funding is guaranteed; funding for the optional years will be based on the effort's performance, the needs of the program, and the availability of funds.

Technical Point of Contact: Dr. David Mortin, AMSAA, 410.278.6248, david.e.mortin.civ@mail.mil

Topic #10: Advanced Materials “Funding is Subject to Availability of Funds”

The Government has the need for efforts in the development and demonstration of advanced materials for weapons and munitions applications. This shall include advanced alloy systems, polymers and composites that can reduce parasitic weight, increase performance (lethality, range, etc.), extend shelf life, reduce item costs, conserve strategic materials, or in other ways help to create or achieve the Army’s vision of the future. Materials of interest include, but are not limited to: titanium, tantalum, tungsten, steel, nickel, aluminum, magnesium, ceramics, cermets, rare earth metals, polymer-based composites, filled composite materials and metal-matrix composites. Processes and production systems to manufacture, as well as specialized tools and methodologies for characterization, testing, and analysis of these advanced materials, are desired.

The Government is interested in materials that will reduce weight, improve ballistics or provide protection to extend the service life of the barrels and other components of weapon systems. These materials may be associated with coatings e.g. cold spray, plasma spray, laser deposition, high velocity oxygen fuel, laser peening, etc; surface modification i.e. superfine finishing, or material substitutions such as ceramic, polymer and/or composite materials. The behavior of materials in service conditions such as crack initiation and growth as well as fatigue behavior of materials is of interest. Additionally, nano-materials hold great promise either in themselves or in combination with other materials to increase the performance of the base materials. Processes which produce unique materials with a nano-size grain structure are of interest.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #11 Testing Methodology “Funding is Subject to Availability of Funds”

The Government has the need for efforts addressing non-destructive testing technology. This shall include efforts that advance the state of the art for performing natural and induced environmental testing of explosive and inert armaments, munitions, and fire control devices at the system and component levels, and developing and implementing new non-destructive evaluation techniques for product evaluation; dimensional analysis; joining technology; and additive manufacturing.

The Government has the need for efforts addressing advanced capabilities associated with armament system ballistic test and evaluation (T&E). These efforts shall address the complete infrastructure associated with a fully functional state-of-the-art ballistic test facility. Focus shall be on improving T&E efficiency by reducing cycle time, increasing the reliability of data capture, minimizing environmental impact, incorporating state-of-the-art instrumentation and technique and integrating virtual participation while maintaining the standards required by government regulation and licensing permits. Introduction of novel T&E equipment and methodology is encouraged.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #12 Electronics “Funding is Subject to Availability of Funds”

The Government has the need for efforts addressing fabrication technology development for micro-system chips based on the silicon, deep reactive ion etching (DRIE) process. This technology is to be utilized for miniature fuze systems. Processed chips will be applied for microelectromechanical system (MEMS) devices for Safe and Arm and micro-initiation components. The Government has the need for efforts in the development of anti-tamper systems for remote armament systems. Anti-tampering systems are needed in increasing numbers as military priority capability needs for autonomous tactical behaviors, autonomous movement and manned/unmanned lethality are growing. Solutions are being sought to protect remote armament systems on the battle field, in urban environments and in storage. The efforts developed should include a capability that tracks tampering attempts made on unmanned systems. Anti-tamper systems that are capable of deactivating battery-operated unmanned systems are needed as well. The Government has a need for efforts in the development of micro-system packaging and micro-system architecture for input into remote armament systems. Novel optical, electrical and hermetic sealing techniques and capabilities will be needed to support this effort.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #13 Manufacturing Sciences "Funding is Subject to Availability of Funds"

The Government has a need for efforts in the development and demonstration of the science behind the manufacture of quality weapon and munitions components, and the integrated data environment that will allow the process knowledge to be retained by the Army in a central repository for future use by the Army's Production Base. These efforts shall address the identification, definition and understanding of materials, equipment, processing and procedures associated with the manufacture of weapons and munitions components; and the capture of that information so that this knowledge can be readily transferred to the industrial base for use in component manufacture. Efforts shall also address the integration of the 3D-Technical Data Package philosophy in the design to manufacturing cycle, and the sharing of digital information across dissimilar systems. Efforts that enhance ARDEC's ability to understand the underlying science of component manufacture or further ARDEC's capability to document and transfer manufacturing processes are desirable. Additionally, efforts that establish manufacturing science test beds, including Additive Manufacturing, to complement ARDEC's prototyping capabilities, and those that team with ARDEC via an Integrated Data Environment are encouraged.

The Government is interested in proposals for advancing the state of the art in manufacturing and fabricating components for weapon and munitions systems. Of high interest are technologies that will extend the life of high value components, such as gun barrels. These technologies may be associated with coatings e.g. cold spray, plasma spray, laser deposition, high velocity oxygen fuel coating, laser peening, intensive quenching, etc; and surface modification, i.e. superfine finishing, or material substitutions such as ceramic materials. Also, processes that reduce weight of system components or extend performance either in terms of life, ballistics, or protection are of interest. Further, the Government is interested in manufacturing processes to reduce cost, cycle time, and fabricate parts where price is independent of quantity, examples of such processes include rapid prototyping technology, free forming technology whether laser based, plasma based, or polymer based. Our vision of the future requires a "paperless process" from designer to machine. Inherent in this process are several subsets including a "model centric" design environment, includes intelligent machining, joining, and processing. One goal is to add intelligence to machine tools to enable them to do a self assessment, self programming, self diagnostics, self scheduling, and in-process monitoring using both software and sensor tools capable of surviving in the harsh processing environment. Lastly, the Government is interested in fiber optic technology, and remote sensing or optics necessary for such systems, and technologies that instill intelligence in processes or machine tools e.g. modeling, data analysis, data fusion, etc.

The Government is interested in proposals to support our "model centric" design environment to rapidly advance the state of the art in modeling, simulation, design, manufacturing, and field support of components for weapon systems. Specifically, the government has interest in technologies that transition from development to production of advanced design methodologies and ensure that this transition occurs seamlessly and with the greatest possible understanding of manufacturing process capability in relation to design intent. It will be essential to establish process capability relative to design intent baselines and goals (i.e., Cp, CpK) and put the disciplines, methodologies, and tools in place to meet these goals. Additionally, the Government is interested in design expertise, methodologies and tools to achieve "quality" hardware from the very start of production and throughout the program production life cycle. The expertise and tools may include the capability to define and flow complex requirements at the characteristic level through multiple layers of the supply chain, simulate optimum processes and tooling for material and machined parts, and seamlessly document process capability in relation to design intent, providing for continuing improvement of both design and manufacturing processes.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #14 Modeling and Simulation "Funding is Subject to Availability of Funds"

The Government has the need for efforts in the development and demonstration of modeling and simulation as tools to assist in streamlining of the munitions manufacturing process. Processing and simulation models are needed to minimize experimental iterations required to validate advanced processes and state-of-the-art technologies that heretofore have not been used to manufacture weapons and munitions components. Additionally, efforts that use simulation to address production scenarios to minimize cost are also needed. Finally, any modeling or simulation technology that assists in extending the life expectancy of Army equipment and is seen as helping to create or achieve the Army's vision of the future is encouraged.

The Government is interested in proposals for advancing the state of the art in modeling, simulation, design, manufacturing, and field support of components for weapon and munitions systems. Predictive models and computer simulations for many advanced processes and state-of-the-art technologies are needed. Predictive and simulation models for new processes are necessary to optimize the process so that the first application (and every application thereafter) meets the specified requirements and quality specifications. Validated models are also needed to allow different production scenarios to be "enacted" through simulation and thereby minimize experimentation, design and manufacturing costs. In addition to its use as a tool to better understand and optimize performance and/or reliability of systems, simulation technology is needed to verify the correctness of designs. Another important application of simulation is in developing "virtual environments", e.g., for training. Such simulations are used extensively today to train military personnel for battlefield situations, at a fraction of the cost of running exercises involving actual personnel, tanks, aircraft, etc.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #15 Optics “Funding is Subject to Availability of Funds”

The Government has the need for efforts in the development of optics technology. This shall include efforts that advance the state of the art in performance of optical, electro-optical and laser systems. Novel optical techniques and capabilities will be needed to support efforts in fuzing, fire control and directed energy systems. Any optical technology that is seen as helping to create or achieve the Army’s vision of the future is encouraged.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #16 Biometrics “Funding is Subject to Availability of Funds”

The Government has the need for efforts in the development of biometric and identification technology. This shall include efforts that advance the state of the art in the ability to detect, identify, characterize, and track items, activities, conditions, and events worldwide which will provide direct benefit to the warfighter. The Government has the need to analyze, improve, verify and validate biometric technology supporting collect, store, match, analyze, manage, reference and share functions of the DoD’s authoritative repository and next generation tactical handheld collection devices. Current biometric technologies assist in providing these capabilities but are limited to the degree of which they can scale and meet future needs. More advanced biometric collection, storage, matching, data analysis, management, reference, and sharing systems will allow the government enhanced situational awareness, and identity superiority on the battlefield for today’s mission as well as mission requirements far into the future.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #17 Power, Energy and Environmental Management Sciences "Funding is Subject to Availability of Funds"

The Government has a need for efforts in the development and demonstration of Novel Power, Energy and Environmental Management Systems, i.e., develop and demonstrate the critical components for improved reserve batteries, hybrid power sources, and other novel power sources to include power harvesting and power distribution concepts. Fuel cell and Lithium (or Li Ion) battery research and manufacturing technology development are also possible areas for projects.

The Government is interested in proposals for advancing the state of the art in materials and technology for sustainable energy and environmental protection. Specifically, the Government is interested in materials and technology that will provide for improved energy efficiency, reduced logistics and/or weight burden, and overall sustainability of energy sources during military deployment, and with a clean environmental footprint. Technologies of interest include, but are not limited to, those for power and energy conversion, power generation, energy storage and recovery, renewable energy, and hybrid intelligent management technologies. Materials of interest include, but are not limited to, coatings/materials to improve efficiency of photovoltaic and/or thermo-electric generators, novel materials for weight reduction and improved performance in batteries, materials for forward deployable sustainable energy systems, etc. Technologies proposed should demonstrate dual-use applications and have direct application to the Warfighter. Additionally, the Government is interested in innovative research that can lead to portable, efficient, and compact power technologies that enhance the military's reach, decrease the logistical burden, and improve energy efficiency at all levels. Specific areas of interest include, but are not limited to, innovative energy conversion, energy harvesting, micro-scale power sources, storage and recovery technologies, renewable energy including solar and wind, energy harvesting/scavenging technologies, hybrid intelligent management technologies, alternative energy systems, fuel cells, and micro-grid forward deployable energy solutions. Also, the development of advanced novel electric and magnetic materials and coatings/materials that improve energy efficiency and enable sustainable power and energy technologies is of interest as well as novel coatings/materials for photovoltaic and thermo-electric generators, advanced nano-composites for turbine technology, enabling coatings/materials for advanced oil-free turbo-machinery or alternative approaches, high temperature materials to reduce weight and increase efficiency of high temperature engines, novel battery materials, etc. In addition, the Government is interested in innovative research that can lead to portable, efficient, and compact power technologies that increase our military's reach, decrease the logistics burden, and improve the overall efficiency of our war fighting forces, especially for distributed and net-centric operations.

Finally, the Government is interested in emerging technologies that can eliminate the use of Cr+6 based (hexavalent chromium) surface treatments used on weapon system components to include but not limited to gun barrels, recoil mechanisms, aircraft landing gear assemblies, etc. These processes shall be environmentally-compliant and provide equivalent, or better, performance as compared to Cr+6 -based surface treatments.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #18 Acoustics "Funding is Subject to Availability of Funds"

The Government has the need for efforts in the development of acoustic technology. Areas of interest include technologies and approaches that address, but are not limited to, the transduction process (converting energy from some other form into acoustic energy that produces the acoustic wave and the reverse process) and acoustic wave propagation. This area of interest revolves around the generation, propagation and reception of mechanical waves and vibrations in air, fluids and solids. Approaches which can help create or achieve the Army's vision of the future are encouraged.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #19 Data Fusion "Funding is Subject to Availability of Funds"

The Government has the need for efforts that address the development of Information Fusion technology that integrates the munition / launch platform with incoming intelligence. Fusion is the process in which data generated by multiple sources is correlated, to assure smart weapons systems are as precise as necessary to achieve mission success. There are several requirements for fusion. First is to gather information. The fusion process, operating over integrated communications networks, includes accepting data from all weapons systems sources. Sensors include combat platforms and soldiers, organic manned and unmanned reconnaissance and surveillance of targets and projectile trajectories to the target. The final requirement of fusion is to provide meaning to the information that has been acquired in order to direct a weapons systems to its final mission objective, thence to determine a weapons systems success by remote real time target kill assessments.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #20 Advanced Design Technologies "Funding is Subject to Availability of Funds"

The Government has the need for efforts that address the development and demonstration of Advance Design Technologies. These technologies include threat recognition, targeting, and system communication of mission commands, remotely operated platforms, weapon systems and weapon systems security, control unit systems, battlefield automation systems, software/performance analysis, emerging software technologies, embedded systems, navigational guidance platforms, integrated user interfaces and processors, computer based systems, orientation and ranging technologies, enhanced software algorithm development and software sustainment/supportability as each relates to embedded software resident in weapons, improvements to existing systems and development of new systems including the design, development, fabrication of hardware and electronics of these systems. Mission objectives are to enhance supported platforms, reliability, response time, and accuracy in meeting the Army's Vision.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #21 Sustainment, Health Monitoring and Supply Chain Management “Funding is Subject to Availability of Funds”

The Government is interested in proposals for advancing the state of the art in force sustainment capabilities, health monitoring of systems, sense and respond supply chain management technologies and methodologies that directly support the war fighter. Specifically, the Government is interested in technologies and approaches that address the planning, setup and operation of production and supply nodes, tools based on best practices to evaluate the performance of production, supply and demand nodes over the entire network, aggressive sustainment capabilities for logistical operations and to address the problem of diminishing manufacturing resources and material shortages (DMSMS) on overall responsiveness of the supply chain. Additionally, the Government is interested in pursuing technologies that provide for system health monitoring to provide early warning prior to component failures due to but not limited to high-cycle fatigue, low-cycle fatigue, abrasion, wear, thermal attack, chemical attack or any combination of these to be applied to existing and developmental systems.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

Topic #22 Technology Exploitation "Funding is Subject to Availability of Funds"

The Government is interested in efforts that exploit / leverage the existing worldwide technology base to address user requirements and operational deficiencies to minimize cost and time-to-field for next generation weapons and munitions. The Government is interested in efforts that involve the adaptation of advanced and innovative technology, processes and procedures from the private sector for military applications. Additionally, efforts that evaluate transition potential of adapting existing military technology for unique warfighter needs are encouraged. Further, prototyping efforts, including Additive Manufacturing, that assess manufacturing technologies and R&D systems at Government facilities are wanted. Finally, efforts that provide rapid response technologies to fulfill needs in critical, high priority missions are needed. This may also include coordinated efforts that evaluate operational environments and requirements in relation to a proposed technology.

Technical Point of Contact: Bill Sharpe, 973-724-7144, willliam.r.sharpe.civ@mail.mil

EXHIBIT B

REFERENCE DOCUMENT: TOPICS #5 thru TOPIC #8

The future research interest topics that apply to Intelligence and Information Warfare (I2W) can be found in the Training and Doctrine Command (TRADOC) publication of Force Operating Capabilities (FOCs).

FOCs address the pursuit of advanced warfighting capabilities and describe them in relevant operational terms. FOCs provide focus to the Army's Science and Technology Master Plan (ASTMP) and warfighting experimentation. They apply to tomorrow’s Army, conducting overmatching decisive operations on the Information Age battlefield, and beyond. United States Army TRADOC functional agencies; doctrine, training, and combat developers; as well as Army materiel developers, utilize FOCs.

FOCs are derived by an assessment of Future Force operational concepts developed by the Mission Area Assessments, Mission Needs Assessments, and Mission Solution Assessments of the Requirements Generation System. Inherent in the Future Force concepts is a full consideration of the Future Operational Environment—the threat. Each FOC includes a detailed, stand-alone narrative of the capability’s utility on the future battlefield.
The following FOCs apply to this general topic and the other research topics within these Topics:

TRADOC FOC-03-03: Advanced Collection, Processing, Analysis, Management and Sharing of Information. A layered network of advanced sensors that sense in multiple domains (e.g., radio frequency, thermal, acoustical, Electro-Optical (EO), infrared (IR), and seismic) and operate independently, or as components of other systems/platforms, including dismounted soldiers, Manned/Unmanned Ground Vehicles (M/UGVs), manned/Unmanned Aerial Vehicles (UAVs), satellites, and even cyber-based platforms. Networked ISR is linked to all shooters. The network of sensors requires an integrated system-of-systems, with scaleable on-board processors, utilizing automated/aided target recognition technology, to rapidly identify, evaluate, locate, and present targets and other streaming video and text information, to commanders and staffs. It requires adaptive reasoning tools that automatically collate and transform sensor data into knowledge, support it via accessible national to tactical common databases capable of providing tailorable Intelligence (INTEL) products to users at all levels. Information management tools are required, permitting the Objective Force to precisely and automatically process, fuse, focus, distribute, and display information in the form most appropriate to the user. Required capabilities include highly advanced information processing, employing automated filters, decision support aids, comparative analysis, and embedded modeling and simulation capability, distributed over multiple, redundant communications pathways, that enable the force to quickly turn information into knowledge, create Situational Understanding (SU), and share a Common Operating Picture (COP).

TRADOC FOC-03-05: Information Protection. The Objective Force requires information protection capabilities embedded in its Information Systems (INFOSYS), as well as its organization, doctrine, procedures, and training. Information protection must proactively provide for the continuous availability of INFOSYS, authentication of participating users, confidentiality of transmissions, and non-repudiation of transmitted or received information. The Objective Force will have the capability to guard communications, networks, and computers; detect misuse or intrusion of these systems; and rapidly restore information and INFOSYS if compromised, corrupted, or destroyed. As a subset of IO, it applies to the assurance of information against threats from a thinking enemy, actively attempting to disrupt, corrupt, or exploit the flow of friendly information. Objective Force networks must provide Protect, Detect, and React capabilities that protect the system's integrity and confidentiality, prevent unauthorized access, and reduce the probability of intercept and exploitation by hostile forces. The system must provide an automated method to protect against computer viruses, and the capability of being updated to maintain currency.

TRADOC FOC-03-06: Situational Understanding. The bottom line is to find the enemy and to understand the situation. The key enabler of the Unit of Action (UA) concept is the enhanced situational awareness that leads to actionable SU. This is achieved by fusing information obtained through a layered network of soldiers, sensors, and collection platforms, with information on friendly forces, enemy forces, and the environment, to obtain a COP that is shared across the force. Distributed analysis, conducted at all echelons, precludes single point intelligence failures and permits information to be directly and precisely delivered to commanders, shooters, Maneuver Support (MS), and maneuver sustainment forces. This information must provide a seamless, fully integrated, multidimensional, and tailorable Common Relevant Operating Picture (CROP), which integrates relevant information from all sources, and integrates reports from subordinates. Must provide precision geospatial terrain environment information layers (modifiable digital overlays), which support cognitive and dynamic mission planning/rehearsal, thus creating a real-time virtual decision-making capability, based upon the commander's and battle staff's detailed 'knowledge' of the physical environment. Accurate terrain representations must be developed with the commanders' needs in mind, and provide expert knowledge at the lowest tactical echelons, providing expert local knowledge exceeding that of the local populace.

TRADOC FOC-03-08: Information Operations. Information dominance is a core competency of the Unit of Employment (UE) that provides comprehensive SU, and generates a strategic-to-tactical infosphere. Information operations provides the Objective Force with the capability to degrade, delay, deceive, disrupt, destroy, exploit, and/or deny an adversary's and other's information and INFOSYS; while protecting friendly information and INFOSYS. Information Operations requires capabilities for blinding the enemy through use of jamming, signature reduction, deception, decoys, and pattern avoidance techniques, permitting the Objective Force to see and understand first. Information Operations (IO) elements include synchronized Computer Network Attacks (CNA)/Computer Network Defense (CND), Psychological Operations (PSYOP), military deception, Electronic Warfare (EW), Special Information Operations (SIO), physical destruction, operational security, counterpropaganda, counter-deception, physical security of Command and Control (C2), Information Assurance (IA), Counterintelligence (CI), and related activities, such as Civil Affairs (CA) and Public Affairs (PA).

Using CNA, PSYOP, military deception, EW, SIO, physical destruction, and other capabilities, IO can be used offensively to influence ideas, perceptions, beliefs, decisions, and communication of information of enemy. Using IA, CND, PSYOP, military deception, counter-deception, EW, and other capabilities, IO can be used to defend decision-making processes, by neutralizing adversary perception management and intelligence collection efforts, and attacks on our INFOSYS. IT-based tools will increase U.S. Army Commanders' IO capabilities and combat power. Examples of such tools include the Internet, global broadcast television, network attack techniques (corruption of data or Denial of Service (DoS)), electro-optic, electromagnetic, high power radio frequency, audio, and seismic weapons; special purpose/multispectral obscurants, advanced INFOSYS and network security, and 'intelligent agents'.

TRADOC FOC-04-01: Sensor Fusion. Fusion is the process in which data generated by multiple sources is correlated, to find the enemy, and create information and knowledge. The chain of command decides what information is required for tactical operations. There are several requirements for fusion. First is to gather information. The fusion process, operating over integrated communications networks, includes accepting data from all ISR sources, organic and external. Sensors include combat platforms and soldiers, organic manned and unmanned reconnaissance and surveillance platforms, and external constellations. The second requirement is to draw relationships between source inputs. Fusion ensures that information is not stovepiped, but is fully exploitable across the entire force. The final requirement of fusion is to provide meaning to the information that has been acquired. This, the most important function of fusion, ensures that information gets converted as quickly as possible into actionable information.

TRADOC FOC-10-01: Understand the Battle Space Environment. The five basic functions required to fully understand the Battle Space environment are: Data Acquisition, Data Exploitation, Data Management, Data Representation, and Data Dissemination.
Required capabilities include:

1. Collection and fusion of high-resolution geospatial data, and comprehensive battle space environment information that includes real time collection of new data, as well as supplementing existing data sets with more detail.
2. Sensor cueing and placement.
3. Stand-off wide area ISR.
4. Tailored, digitized, and usable battle space environment data that is timely, and compatible with the network-centric environment.
5. Actionable and scalable visualization products to mitigate the threat's 'home-court' advantage, displayed either visually or in some other form that is compatible with the user needs.
6. Computer-aided analysis and reasoning tools that enable prediction and understanding and provide actionable advice.
7. Reach to national and other sources, when needed.
8. Data storage, retrieval, and update capabilities.

In order to achieve unprecedented momentum and freedom of maneuver, the Objective Force must *see* the complete picture of the operating environment, in all of its aspects. Further, the Objective Force must have an *understanding* of this picture that allows it to take away the enemy's 'home court advantage', and give our leaders a better understanding of the environment than our adversaries. Objective Force units will *see first* by detecting, identifying, and tracking the individual components of enemy units. Advanced technologies that lead to unprecedented ISR capabilities, coupled with other ground, air, and space sensors, are networked to provide a common integrated operational picture that will enable seeing the enemy, both in whole and in part, as a complex, adaptive organization.

TRADOC FOC-10-05: Enable Force Protection and Security.

Provide full range of security operations, including proactive measures and response forces, to foster protected movement of forces between operating areas in ‘gray spaces’ (includes cueing and early warning to the lowest levels).

Required capabilities include:

1. Means to obscure the full range of RSTA and electromagnetic threats, both to protect friendly forces, and to attack enemy forces.
2. Combat Identification (CID), Friend-Foe, and Neutral information in support of current and future operations.
3. Antiterrorism and Facility Planning (FP) equipment and vulnerability assessment planning tools.
4. Integrated ISR and dynamic sensors for standoff detection/assessment, to aggressively perform FP and security operations.

More information on each FOC can be found in TRADOC Pam 525-66, 7 March 2008, Force Operating Capabilities. This document is available on the TRADOC homepage at http://www.tradoc.army.mil/