Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

United States Army

Communications-Electronics
Research Development and Engineering Command
Intelligence and Information Warfare Directorate

Broad Agency Announcement I2WD 2014

Title: **BAA I2WD 2014**
New Solicitation Number: W56KGU-16-R-A330
Formally Solicitation Number: W56KGU-14-R-0003
Solicitation issued by: Aberdeen Proving Ground- Army Contracting Center

Initial Date of Issue: 26 August 2014 (Amended 2 February 2016)

Distribution A: Approved for public release; distribution is unlimited

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Table of Contents

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

PART I – INTRODUCTION

This Broad Agency Announcement (BAA), formally Solicitation Number W56KGU-14-R-0003, New Solicitation Number: W56KGU-16-R-A330 sponsored by the U.S. Army Research-Development Electronics Command (RDECOM), Communications-Electronics, Research Development and Engineering Center (CERDEC), Intelligence and Information Warfare Directorate (I2WD) shall be open **five years from Initial Date of Issue**. The BAA is issued under the provisions of paragraph 6.102(d)(2) of the Federal Acquisition Regulation (FAR) which provides for the competitive selection of research proposals submitted in response to this announcement. Accordingly, proposals selected for award are considered to be the result of full and open competition and fully compliant with Public Law (PL) 98-369, "The Competition in Contracting Act of 1984".

This BAA is an expression of interest only and does not commit the Government to make an award or pay proposal preparation costs generated in response to this announcement.

The CERDEC encourages industry interested in conducting scientific research, including educational institutions, small businesses, small disadvantaged business concerns, historically black colleges, university and minority business enterprises, and institutions to submit proposals. Eligible prospective offerors also include Canadian firms participating in the Defense Development Sharing Program (DDSP).

Questions concerning contractual, cost, pricing, or proposal format may be directed to Group email: usarmy.APG.cerdec.list.i2wd-iwo-ac-gov@mail.mil

Questions concerning the receipt of your submission should be directed to Group email: usarmy.APG.cerdec.list.i2wd-iwo-ac-gov@mail.mil
Technical questions will be sent to the appropriate Technical Points of Contact (TPOC), topic authors, and/or Subject Matter Experts (SMEs) to request clarification of their areas of interest. White papers and outlines are encouraged before a final proposal is prepared and submitted to I2WD. No discussions are to be held with offerors by the technical staff **after** proposal submission without permission of the ACC-APG Contracting Officer.

Funds are not presently available for the research interests represented in this Broad Agency Announcement. No contract award will be made unless appropriated funds are available for research and development. Prospective offerors are reminded that only a duly warranted Contracting Officer may obligate the Government to an agreement involving expenditure of Government funds.

Electronic copies of each Proposal or White Paper shall be submitted via the following group mailbox: usarmy.APG.cerdec.list.i2wd-iwo-ac-gov@mail.mil

PART II – GENERAL

Offerors shall make their proposals valid for at least 180 days. Offerors shall complete the representations and certifications set forth in Appendix A.

If an Offeror's proposal is determined to require access to, or require the generation of, classified information, appropriate security clearances will be required of the Offeror and a DD Form 254 will be generated. Any classified materials submitted must be identified, marked, and packaged in accordance with the most up to date Industrial Security Manual. Proposals containing proprietary data should be marked "UNCLASSIFIED - For Official Use Only."

The Government intends to award **cost-plus-fixed-fee** type contracts concerning this BAA. However, offerors may propose alternate contract types or other transaction type agreements providing that the alternative is supported in the proposal. Also, the Government reserves the right to select the contract type as a matter of negotiation.

Each offeror's cost proposal shall contain sufficient quantitative and narrative documentation necessary to adequately support and explain the costs proposed, to include subcontractor costs. The cost narrative shall also include information demonstrating that the offeror and any subcontractors with other than firm fixed price subcontracts have accounting systems adequate for determining costs applicable to the order.

Research and development contracts awarded from this BAA will be primarily Cost Plus Fixed Fee as it is not expected that the scope of the contract will be sufficiently defined to allow for a firm fixed price contract. Potential offerors should be aware that in accordance with FAR 16.301-3(a), a cost-reimbursement contract may only be used when the contractor's accounting system is adequate for determining costs applicable to the contract. Determination of adequacy is normally performed by DCAA.

Special consideration shall be given to R&D proposals that exhibit revolutionary and innovative problem solutions. Revolutionary, in this context, means a far-reaching change that improves capabilities well beyond what was initially envisioned. Moving from having no operational capability to satisfy a listed Army requirement to having an initial, demonstrable prototype capability also fits the context of "revolutionary."

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

PART III – RESEARCH INTERESTS

Preamble

The U.S. Army I2WD BAA program is organized by Army application discipline. The reader may note some overlap between sections.

Ultralite satellite communications link joint forces to the world-wide intelligence systems.

The research areas described may have short or long-range impact on Army Signals Intelligence (SIGINT), Electronic Intelligence (ELINT), Measurement & Signature Intelligence (MASINT), Electronic Warfare (EW), Information Operations (IO), Information Warfare (IW), Language Translation, Command, Control, Communication, Computers Intelligence, Surveillance, and Reconnaissance (C4-ISR) Integrity, Automatic Target Recognition (ATR), Combat Identification (CID), Radio Detecting and Ranging (RADAR), Aircraft and Ground Vehicle Survivability Equipment (ASE & GSE), Electro-Optics (EO), or Infrared (IR) requirements advancement.

If development in certain topic areas requires the interaction of several investigators from differing interdisciplinary areas, proposals for comprehensive research programs shall be considered. Only a limited number of such large programs can be initiated under this BAA. Inquiries related to comprehensive and interdisciplinary programs should be sent to the Director, USA I2WD, ATTN: RDER-IW, Building 6003, Combat Drive, Aberdeen Proving Ground, MD 21005. Or to Group email: usarmy.APG.cerdec.list.i2wd-iwo-ac-gov@mail.mil

See included references and glossary of terms pertinent to this solicitation.

Objective: Information Dominance on the Battlefield

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330
Topic title: Intelligence and Information Warfare - General

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 this BAA:

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-09-01: Survivability and Force Protection. Future combat system-based combat battalions will have organic capabilities for Identification of Friend or Foe (IFF), air/missile defense, early warning, surprise-avoidance, active and passive protection systems, and operational shielding from unconventional approaches. Future Combat Systems (FCS) must provide CID of friend, foe, and noncombatant in a joint, allied/coalition environment, through platform-to-platform (manned and unmanned,

ground and air), platform-to-soldier, soldier-to-platform, and soldier-to-soldier, under all battlefield and weather conditions, across the spectrum of operations.

An additional key capability in the Objective Force's survivability approach is hit avoidance, which includes both avoiding acquisition or tracking by enemy fire control and avoiding being struck by enemy weapons once they have been fired. Active protection measures and signature management are critical capabilities for Objective Force systems.

Detection avoidance capabilities include technologies and strategies used to mitigate or disguise signature emissions of all types (visual, audio, seismic, radar, electronic, and thermal) associated with maneuver combat. In conjunction with advanced Reconnaissance, Surveillance and Target Acquisition (RSTA) assets, suppression of these signatures to the extent that soldiers and future weapon system-of-systems are indistinguishable from their surroundings, provides the warfighter with the ultimate advantage of battlefield surprise.

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/

Topic title: Collect - Advanced Radio Frequency Technology and Techniques for Signal Intelligence

The purpose of Signal Intelligence (SIGINT) is to intercept intentionally transmitted signals. These signals can be categorized and defined as Electronic Intelligence (ELINT) and / or Communication Intelligence (COMINT). COMINT, one of the primary SIGINT disciplines, includes information derived from intercepted communications transmissions. COMINT targets voice and teleprinter traffic, video, Morse code traffic, or even facsimile messages. COMINT can be collected from the airwaves, or any other transmission medium. ELINT includes the interception and analysis of non-communications transmission, such as radar. Signals intelligence collection can be performed from a variety of platforms. Examples include overt as well as covert ground collection sites; ships and aircraft. SIGINT facilities can monitor transmissions from communications satellites, as well as terrestrial facilities. This topic is concerned with identifying and developing revolutionary and evolutionary technologies, e.g., RF front-end components and signal transmission techniques, which will provide a new and enhanced operational capability and/or improve existing SIGINT capabilities.

SIGINT systems must operate over a wide frequency range to address COMINT and ELINT requirements. The need exists for components, e.g., antennas and receivers, that can operate over wide instantaneous bandwidths, detect and identify conventional and modern digital signals, are reconfigurable, and can operate in multiple physical and signal environments. State-of-the-art software should control the receivers, classifiers, down converters, or other hardware used in RF collection and processing. It is desirable that the system can be interchangeable in function; e.g., COMINT and/or ELINT.

It is also desired that commercial-off–the-shelf radios, components, and sub-assemblies be investigated to the maximum extent to reduce development time and cost and to expedite system integration, test, and fielding. This includes researching, developing, testing, analyzing, and applying the rapid advancement of commercial communications techniques such as Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA), Personal Communication Systems (PCS), and burst-digital and multimode communications hardware.

Additionally, SIGINT systems must consider the following:

- SIGINT information should be presented in a manner that allows the commander to quickly interpret the data to make informed decisions.
- The system should be flexible and adaptable to a dense and changing signals environment.
- The system should be capable of being reprogrammed quickly in order to perform missions with changing requirements, using software reloads or other innovative approaches.
- Systems should strive for interoperability with other tactical, operational, and strategic SIGINT systems, either airborne or ground based platforms, to enable a more complete Situational Awareness (SA) of the battlefield.
- Systems providing automated electronic mapping of the battlespace including signal characterization, precision location, parametric measurement, basic traffic analysis, and critical node analysis are of interest.
- SIGINT sensors and collectors should be frequency scaleable and provide “plug and play” capability, i.e., change internal hardware to perform various tasks without interrupting the soldier’s mission.
- SIGINT systems should take into account co-existence / compatibility with current force protection Electronic Warfare (EW) Systems.

SIGINT Sub-topic # 1 – Antenna Design for Airborne and Ground Platforms

Antennas remain a critical component in SIGINT systems. There are several areas with potential for technological improvement in antenna design. Efficient small and lightweight antennas are very difficult to construct, especially at the lower frequency bands. The lower frequencies translate to large wavelengths and therefore result in large antennas to achieve higher gain. The attempt to make these antennas smaller in

order to meet platform constraints often results in non-optimum performance. Additionally, antennas with fixed or variable beamwidth would be of interest. Currently, various antenna structures, e.g. single and multi-element antenna arrays, are required to provide the degree of coverage required (from narrow beam to full 360 degrees). Another area of interest is improvement in the antenna mounting structure to ensure that the structure does not interfere with antenna performance. Proposed antenna configurations should take into consideration that operating environments may cover temperature extremes or harsh conditions. Novel antenna concepts that can solve these limitations and satisfy SIGINT requirements are desired. To address these needs Research and Development (R&D) emphasis could include:

- Electromagnetic Modeling (EM) of single and multiple mounted antennas to predict beam patterns and gain.
- The development of compact High Frequency/Very High Frequency (HF/VHF) antennas for SIGINT systems on smaller payload platforms such as manpacks and Unmanned Aerial Vehicles (UAVs). Research should also emphasize low-drag, conformal, efficient designs for both collection and Direction Finding (DF) purposes.
- Development of next generation antennas using basic research and novel technologies, e.g., Fractals, High Temperature Superconductors (HTSC), revolutionary designs, exotic materials with variable properties (permeability / permittivity), metamaterials, frequency selective surfaces (FSS), and frequency agile apertures, etc.
- Development of broadband capability while maintaining good electrical performance, e.g. Gain and Voltage Standing Wave Ratio (VSWR).
- Antennas that are operational from HF through Millimeter wave to address current and future COMINT and ELINT needs.
- Development of antennas that address all or some of the following characteristics: miniature, disposable, small aperture, and reconfigurable.

SIGINT Sub-topic # 2 – RF techniques to enhance SIGINT receivers

Research and development (R&D) of advanced receivers that can enhance the performance and capabilities of future SIGINT systems is required. Emphasis shall be on wide bandwidth, small size, low power, low noise, wide dynamic range, and advanced signal processors and processing algorithms. The goal is to improve SIGINT system techniques for signal detection, recognition and sorting in a cluttered Radio Frequency (RF) environment. Also, of interest are signal processing or alternate techniques for interference signal rejection and suppression. These developments should address the following:

- Methods and techniques for improving the intercept range (distance) of ground based and low-flying systems
- Improvements in man-machine interfaces
- Adaptability to address future modulations through the use of software reloads.

- Ability to operate within various environmental operating conditions – temperature, vibration
- Wideband instantaneous operational frequency range from High Frequency (HF) through millimeter Wave (mmW).
- Capability to handle conventional and modern signal types; ability to be easily configured to address future signals.
- The ability to automatically adapt for optimal sensitivity to achieve high signal-to-noise ratios for select signal types that are present for a very brief period of time.
- Reduction in size and power consumption requirements
- The combination of ELINT and COMINT receivers into single or dual use packages.
- Active and Passive SIGINT technologies to improve signal identification should be considered.
- Other technological advances improving on existing receiver capabilities

SIGINT Sub-topic # 3 – Tactical SIGINT Capabilities

Research and development (R&D) of advanced tactical receiver components and capabilities is required. Emphasis shall be on low size, weight, power, and cost (SWaP-C) receivers, transceivers, antennas, amplifiers, and other hardware required to perform SIGINT missions. Low SWaP-C is critical for man-pack SIGINT systems where every additional component means another left behind. These developments should address the following:

- Wideband man pack receivers and transceivers
- Low profile wideband man pack direction finding antennas
- Conformal direction finding antennas
- Modular, small, and efficient man pack amplifiers
- Radio and Network Emulator for Operator Training and Testing
- Utilizing low-cost commercial off the shelf (COTS) hardware to perform SIGINT missions
- Android Signal Processing capabilities
- Signal processing techniques for platforms with limited processing capabilities

Topic title: Collect – Signals Intelligence for Conventional Analog/Digital Signals & Low Probability of Intercept Signals

SIGINT systems must operate in a signal environment that uses conventional signal types, e.g., Amplitude Modulation (AM), Frequency Modulation (FM), and phase modulation, as well as more modern signal types, e.g. Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), Quadrature Phase-key shifting (QPSK). Also, the future signals environment will be rich in the number of electromagnetic signals of different types, e.g. encrypted, multi-media, Low Probability

of Intercept (LPI), and digital. SIGINT systems must quickly detect and process multiple signals to identify and locate the threats thus providing the warfighter with real time data to improve situational awareness.

SIGINT Sub-topic # 1 – COMINT Enhancements for Conventional Signals

This topic is concerned with improving the ability to quickly and uniquely identify and locate communication targets on the tactical battlefield. Areas of research and development include, but are not limited to, super resolution Direction Finding (DF) algorithms, DF antenna array design, system calibration and EM/ RF interference rejection, critical component development, real-time signal processing, wide-band / LPI signal exploitation, High Frequency-Direction Finding (HF-DF) and non-DF signal geolocation techniques. Many of these areas are addressed in further detail in the following paragraphs:

Super-Resolution DF Algorithms
Super-resolution DF algorithms enable the user to identify and distinguish between closely spaced transmitters. Also, these algorithms have evolved as a means to reduce the degrading effects of co-channel and multi-path interference signals. New DF algorithm techniques or enhancements to existing approaches that can exploit the space and time diversity of co-channel signals are of current research interest.

System Calibration and Electromagnetic Modeling
Currently, SIGINT systems are subjected to extensive calibration procedures before being operational. Additionally, any changes to the system hardware could require a complete recalibration. This is highly inefficient and extremely costly. Therefore, advanced and novel system calibration techniques that could minimize or even eliminate the system calibration are required. This can be accomplished using advanced algorithms or developing a calibration technique that is insensitive to hardware changes. Additionally, Electromagnetic Modeling (EM) to provide accurate system performance predictions could be applied as a technique to possibly reduce calibration requirements. Generic solutions that can be applied to different platform types and / or extrapolated to similar systems, are preferred and of particular research interest.

RF Interference
RF interference caused by high power transmitters, co-channel signals, or other sources is recognized as a major problem in receiving systems. RF interference can overload SIGINT systems resulting in the loss of potentially critical intelligence. Methods and techniques are required that can discriminate, manage, or eliminate interference signals to ensure continuous operation. Broadband rejection techniques are of particular interest but reduced alternatives will also be considered. Possible solutions can be implemented in hardware, software, or both. Several examples of interference rejection/management are: broadband excision, narrow band cancellation,

adaptive nulling, covariance matrix extrapolation, Digital Beamforming (DBF), and closed loop self-adapting circuits. These systems should work in real time for maximum operational efficiency. RF interference management should include the ability to select specific signals of interest from among all other emitters in a tactical battlefield environment and additionally offer protection from high power signals that can damage the receiver front end. Automatic system operation is preferred, but manual operation either alone or with some degree of automation will be considered. Application of these techniques to both ground-based and airborne platforms (helicopters, fixed wing and Remotely Piloted Vehicle (RPV)/Unmanned Aerial Vehicle (UAV) is of current interest.

Critical Component Development

The capability of SIGINT systems is directly dependent on the performance of the individual components that comprise the system. Some of these standard components include: high gain low noise amplifiers, rapidly tuned agile filters (bandpass, notch), low sidelobe low phase noise direct signal synthesizers, high speed Digital-to-Analog (D/A) converters, and wideband high dynamic range receivers. Advances in basic research such as high electron mobility transistors (HEMTs), High Temperature Superconductors (HTSCs), wideband gap devices, ferroelectric material, etc have resulted in higher performance components thus enabling better system detection, improved resolution, and increased range. New component applications of these existing research technologies and next generation research that could further enhance these components is desirable. The ultimate goal is to integrate these technologies/components into SIGINT systems to obtain the following capability improvements:

- Good selectivity, improved sensitivity, and phase stability
- Broad instantaneous bandwidth
- High two-tone spur-free dynamic range
- Multi-mode, e.g., broadband dual channel or narrow-band multi-channel

Wide-band / LPI Signal Exploitation Techniques

The current trend in RF communication systems is the use of advanced digital modulation schemes and ultra wideband technologies. These formats present a unique challenge to SIGINT systems because the signals are difficult to identify and track, e.g., LPI. The signals could be frequency hopping, buried below the noise floor, require precise timing, or spread the transmitted energy over a wide band. Basically, these signals are designed to cause ambiguity and/or unpredictability in time, frequency and power and to bring new problems to tactical Directional Finding (DF). Possible solutions to these problems will require innovative techniques or technologies and are of particular interest.

Electro-Magnetic Environment (EME) Activities

To perform efficient utilization of the Radio Frequency (RF) spectrum and to coordinate SIGINT activities it is desirable to collect, store, and analyze the Electro-Magnetic

Environment (EME). This data and analysis is used to determine the typical signaling activity present in a particular area of operation. There is interest in hardware and software capabilities to collect and store RF information and to perform analysis of the RF environment. Topic areas that will be considered are:

- Hardware to effectively collect a broad range of frequency, large instantaneous bandwidth, sufficient high dynamic range, and sufficient frequency resolution.
- Hardware to efficiently and effectively transfer large amounts of collected data to storage devices at a high rate over a sufficient time period.
- Software techniques and capabilities to automatically detect signal energy, effectively filter signals of varying bandwidth, and effectively identify signaling modes and modulation types present for varying periods of collection in varying Signal to Noise Ratio (SNR) environments.

SIGINT Sub-topic # 2 – Advanced Receiving Techniques

A comprehensive understanding of how a SIGINT system can operate to its full potential is critical. The soldier must understand the system, know its limits, know the best method of operating, and how to interpret the results. This is generally referred to collectively as Tactics, Techniques, and Procedures (TTPs). Therefore, developing superior SIGINT TTPs will enhance the efficiency, capability, and understanding of SIGINT system operation and enable optimum usage. An emphasis on reliable and robust techniques for signal detection, recognition and sorting in a cluttered RF environment is of interest. Several examples of additional areas of interest include but are not limited to the following:

- TTPs for automated intercept, processing and exploitation of Low Probability of Intercept (LPI), Low Probability of Exploitation (LPE) signals.
- Techniques for robust processing of signals in noise and interference. Developed TTPs must be usable on a tactical battlefield where there are many signals of non-interest interspersed with the desired target signals.
- Methods and techniques for enhancing the intercept range of systems.
- Improvements to the user interface for rapid and improved operation.
- Automated system control for optimum performance with limited user interaction / interpretation.

SIGINT Sub-topic # 3 – Advanced Geolocation Techniques

This topic addresses the goal of identifying the precise location of threat emissions. Upon detection of threat signals it is desired to locate the source within a certain degree of accuracy, and then decide what action is required (jam, eliminate, etc). Many techniques such as Time Difference of Arrival (TDOA), Frequency Difference of Arrival (FDOA), and interferometry have been developed to solve this problem. Each approach

has unique benefits and can achieve various degrees of accuracy, especially when placed on moving platforms. Enhancements to existing approaches and new, novel techniques that can result in more accurate results and can operate either in a stationary or mobile environment are of interest. Additional considerations are:

- Geolocation of LPI
- Novel methods and techniques for extending the detection range of ground based and low flying DF systems
- Geolocation from a single site, preferred, or from multiple cooperative sensors.
- Advanced geolocation techniques and algorithms for threats in a high-density, high multipath environment.

SIGINT Sub-topic # 4 – Individual Specific Emitter Identification (SEI)

SEI is a method of recognizing individual electronic emitters through the precise measurement of selected signal "externals", i.e., parameters and/or characteristics of the transmission. To be identified by SEI techniques, a specific emitter must have one or more of these signal externals that are stable and that are unique within the measurement capabilities of most collectors. SEI can provide reliable and timely intelligence data for keeping track of individual target emitters and the particular units operating them. An SEI system is driven by four key concepts:

- Accurately measuring signal features that are consistent from one transmission to another for a given emitter but differ from emitter to emitter
- Clustering the features by emitter, so that different emitters can be identified or verified.
- Entering the cluster information into a database and maintaining the clusters as the features age in time
- Providing ground truth (the correct Identification (ID) of the emitters being evaluated) for the naming of the clusters and evaluation of the clustering process.

A typical SEI system consists of several subsystems: RF system, data collection, signal processing, feature estimation, identification classifier, cluster management, and database. The RF subsystem usually contains a set of downconverters to translate the frequency so that it is compatible with the data collection subsystem. The data collection subsystem collects samples of the emitters without modifying the signal characteristics. The signal processor processes the data to identify features for classification. The feature estimation defines the signal features from the demodulated signal. The cluster management subsystem is responsible for maintaining and modifying the clusters in the database. Finally, the database catalogs, stores, and retrieves data for processing. Developing systems that can accurately perform these functions to correctly identify signals with a high degree of accuracy is of current interest.

SIGINT Sub-topic # 5 – Issues Peculiar to High Frequency Electronic Support Measures

Electronic Support Measure (ESM) is considered the eyes and ears of the Electronic Warfare (EW) effort, in that ESM is responsible for the detection, processing, recording, location, and identification of electromagnetic energy transmitted by hostile and neutral emitters. The main purpose of ESM is to gain sufficient information about sensors to allow an understanding of the signals characteristics, e.g., transmitted power, operating frequency, polarization, and signal bandwidth, and includes identifying the systems role, method of operation, and its strengths and weaknesses. With this information, the Electronic Support (ES) system can identify the asset, assess its relative threat and provide information to the operator on how best to manage the threat. The HF frequency band presents unique design and environmental challenges that are not associated with systems at the higher frequency bands. The following topics demonstrate some of these key issues and desired attributes associated with HF operation but, are not all inclusive.

- Near vertical incident skywave
- Ionosphere measuring and modeling techniques
- Antenna arrays for high-angle skywave
- High dynamic range HF receivers
- Small aperture antenna
- Active elements
- Dielectric loading
- Polarization diversity
- Minimum operator action to provide situational awareness
- Priority Threat Alarming
- Manual & Automatic Receiver Queuing
- Automatic Threat Identification

New and innovative methods to address these concerns and that can ultimately enhance HF system performance are of high research interest.

SIGINT Sub-topic # 6: Multi-Intelligence Electronic Support (ES) for Integrated Electronic Warfare

This topic addresses the goal of providing the Warfighter with improved Multi-Intelligence Electronic Support (ES) Situation Awareness (SA) of wireless communications in the presence of, and cooperation with, electronic communications and force protection systems. New and innovative technologies and techniques will be applied to improve the Multi-Intelligence ES sensing capability and SA of threats within the Electro-Magnetic Environment (EME). Technology and techniques will be researched and developed to provide improvements in efficiency, effectiveness,

detection, identification, and emitter location for Multi-Intelligence sensor systems. Considerations will be made for use of these capabilities in dismount, ground vehicle, airborne, and unmanned platforms. Technologies and techniques may be provided for stand-alone sensor system operation or network coordinated and distributed sensors system operation.

Topic title: Collect – Signals Intelligence for Modern Signals

The topic of SIGINT for modern signals is concerned with improving the ability to detect, identify, locate, demodulate, survey, search, and correlate modern communication targets on the tactical battlefield. Improving man machine interfaces (MMI) is also important in the complicated SIGINT environment. In general, modern communication emitters are characterized by a very wide range of platform size, mobility, signal duration, power, bandwidth, frequency reuse, coding complexity, global connectivity, data rate, and spectral overlay/underlay; and operating in various co-channel signal densities, dynamic multi-paths, and terrains or altitudes. New technologies are continually evolving. The complexity of the signals environment and the multiple variations of signal generators require constant innovation to remain effective in the SIGINT arena.

SIGINT Sub-topic # 1 – Communications Intelligence Enhancements for Modern Signals

COMINT concerns itself with areas of research and development including, but not limited to, super resolution Direction Finding (DF) algorithms, DF antenna array design, system calibration, and Electromagnetic Modeling (EM), radio frequency interference (RFI) rejection, critical component development, real-time signal processing, wide-band/ Low Probability of Intercept (LPI) signal exploitation, high-frequency DF issues, non-DF signal geolocation techniques, emitter identification, and signal-associated internal/external information extraction. Urban terrain scenarios require the ability to locate signals through walls and similar materials as well as the improvement of the DF and non-DF location accuracy that approaches Cramer Rao (CR) bound in urban multi-path channels.

COMINT in modern signal environment often requires cooperation with remote active devices that set target emitters in such a mode that a passive COMINT system can intercept them in a timely efficiency. Areas of Research and Development (R/D) are to investigate those cooperative techniques that are maximally effective yet maximal covert. Research and Development (R&D) of critical components to improve DF and TDOA/FDOA systems is required. Current topics of interest include, but are not limited to: high gain low-noise amplifiers, rapidly tuning notch filters, low side-lobe direct digital synthesizers, and receivers exhibiting the following characteristics:

- Super-high selectivity, sensitivity, and phase stability
- Broad instantaneous bandwidth with low distortion
- High two-tone spur-free dynamic range
- Dual mode (broadband dual channel or narrow-band multi-channel), 14+ bit analog-to-digital converters that operate at 200+MHz, analog devices for spectrum channelization, and adaptive broadband Radio Frequency/Intermediate Frequency (RF/IF) delay devices.

Real-time signal processing in embedded computers has become an ad hoc standard for tactical system design. Closely related to this type of design are the following research topic areas: high speed Digital Signal Processors (DSP), optical computing, analog Very Large Scale Integration (VLSI), parametric and non-parametric density estimation, multivariate sorting and decision support, high speed algorithm development, parallel processing, and Versa Module Eurocard (VME) Bus and future bus architecture improvements.

Improvements are needed in the rapid acquisition and processing of SIGINT data as well as in the presentation of this data in a format usable to military operations in support of Intelligence, Surveillance and Reconnaissance (ISR) activities with multiple user access.

SIGINT Sub-topic # 2 – Advanced Receivers and Receiving Techniques

R&D is required for advanced receivers and receiving techniques. Topics of interest include:

- Wide bandwidth, small size, low power, and reliable advanced signal processors
- Processing focused on reliable and robust techniques for signal detection, recognition and sorting/tracking in a cluttered Radio Frequency (RF) environment
- Signal processing or other techniques for interference rejection and suppression
- Small, efficient, and broadband receiving antennae

RF interference is recognized as a major weakness in receiving systems when caused by non-cooperative emitters. Rejection techniques that might be applied to broadband receiving systems are of current interest. Such techniques include, but should not be limited to, broadband excision, narrow band cancellation, adaptive nulling, and covariance matrix extrapolation. The application of these techniques to both ground-based and airborne (helicopter, fixed wing and Remotely Piloted Vehicles (RPV)/Unmanned Aerial Vehicles (UAV)) platforms is of current interest to the government.

Tactics, Techniques and Procedures (TTPs) for automated intercept, processing, and exploitation of LPI and Low Probability of Exploitation (LPE) signals are required. The developed TTPs must be usable on a tactical battlefield where there are many signals

of non-interest intermixed with the desired target signals. Techniques for robust processing of signals in noise and interference should be considered.

SIGINT Sub-topic # 3 – Platform and Antenna Array Modeling

Super-resolution DF algorithms have evolved as a means of reducing the degrading effects of co-channel (non-coherent) and multi-path (coherent) interference. Techniques that exploit the spatial and/or temporal diversity of co-channel signals are of current research interest. Successful application of these techniques to tactical systems is considered a challenge to technical system designers.

Advanced techniques for improving location accuracy are required. Areas of interest include:

- Reducing the entire set of contributing errors originating from time/space references
- Measurement/processing devices/techniques
- Array calibrations
- Propagation channel disturbances.

Location can be estimated not only by signal externals but also by a set of the internals that are directly or indirectly associated with emitter locations. The combined approach of externals/internals is considered an R&D area for improving location accuracy.

System calibration and electromagnetic modeling, especially as globally applied and/or extrapolated to like systems, is of particular research interest. Required R&D includes platform modeling and antenna array modeling.

Wide-band/LPI signal exploitation techniques and research issues closely related to them are of particular interest. Signals designed to cause ambiguity and/or unpredictability in time, frequency and power bring new problems to tactical DF, that requires innovative solutions.

SIGINT Sub-topic # 4 – Advanced Communication, Specific Emitter Identification (SEI)

Specific Emitter Identification (SEI) by both signal externals and internals is desired for sorting/tracking and for more tightly correlating and improving SIGINT battlefield mapping of target emitters. The following are the R&D areas of interest:

- Advanced communication SEI techniques by externals
- Advanced communication SEI techniques by internals
- Estimations of tight SEI performance bound for arbitrarily selected SIGINT scenarios

- General purpose communication SEI system architecture
- Minimal but consistent data set representation of SEI information of an emitter operating in different channels and with intended signal parameters
- SEI techniques in time-varying multipath

Topic Title: Multiple-Intelligence

The Army is interested in a combined approach to intelligence collection, processing, and dissemination. This combined approach is termed Multi-Intelligence (Multi-INT). Multi-INT crosses traditional Intelligence lines that traditionally have operated in a stovepipe manner. This parochial approach to intelligence, in very specific areas, has benefits when detailed analysis in each area is required. Detailed analysis can yield large benefits to the War fighter. However, as the actionable Intelligence level moves to lower Commanders levels, integration of these individual intelligence areas into a multi-intelligence "picture" has tremendous benefits in areas such as:

1. Increased Commander's confidence in the provided intelligence from individual sensor types
2. Harder to spoof overall intelligence collection
3. Enhanced understanding of the Battle Space and the threat's intent
4. Understandable intelligence without the need for area specific analysts or linguists
5. Area coverage that maximizes utilization of existing sensor assets

The multi-INT approach also presents technology challenges that are unique to multi-INT and require research and development solutions over and above those of each individual intelligence area. Multi-INT crosses or encapsulates the following traditional intelligence areas; Signals Intelligence (SIGINT); which includes Communications Intelligence (COMINT) and Electronic Intelligence (ELINT), Measurement and Signals Intelligence (MASINT), Human Intelligence (HUMINT), Radio Frequency Intelligence (RFINT), Imagery Intelligence (IMINT), and other areas.

The logical approach to the multi-INT technology challenge is to look at it from a functional viewpoint: collection (the sensors), processing (collection management), and dissemination (how the data is sent, to whom, how much, and how it is integrated and presented to the client users). This requires an over arching all encompassing multi-INT architecture: What is the architecture to support this multi-INT approach?

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

MultiINT Sub-topic # 1 – Multi-INT Sensors for Urban Operations

Urban Operations presents a unique challenge for multi-INT sensors and also is a major operation mode for the Army. Deployment methods, manned or unmanned operation, weight trade offs, and antennas must be designed so that sensors can perform their missions in the optimum way without adding unrealistic requirements on the users. Under this subtopic, the bidders should address this and specifically with concern to the following:

1. Mobility requirements and possible mobility solutions for the multi-INT sensor suites.

2. Limitations of operations in the urban environment of the sensors in a multi-INT role.

3. Multi-INT payoff for the urban environment. This includes Unmanned Aerial Vehicle (UAV) multi-INT payload packages (flight considerations are addressed under the airborne platform section of the topic).

4. Ability to enhance detection and location of targets with the multi-INT payloads for user survivability and targeting must be addressed. Comparisons of multi-INT sensor suites versus individual sensors must be studied.

5. The level of integration of sensor capabilities into a new ‘integrated’ multi-INT sensor package shall be addressed. Here in the urban environment where man carry and robotics limit SWaP significantly, the SWaP aspects of the multi-INT sensor suite must be addressed for both man portable and robotic platforms. This includes the cost of integrating sensor capabilities into one new sensor, and at what level that integration makes sense.

6. Ability to operate and operational payoff of multi-INT versus stand-alone sensors will be studied. Especially with respect to the ability to detect and locate within the given urban environment. Also included shall be the ability to enhance survivability and targeting for the urban assault team. This includes survivability when serving in the ‘policing’ mode as well as the initial assault mode.

7. Special miniaturized antenna approaches shall be suggested.

All the considerations above result in the need for interested bidders, under this portion of the Broad Agency Announcement to be invited to submit proposals dealing with the solution of the above technology and operational areas of challenge. Specifically, but not limited to, this agency is interested in:

- Research and development (R&D) of advanced techniques for application of Multi-INT sensors and associated technology to support and or enhance the performance

of *dismounted soldiers* during Urban Operations. This includes development and testing of prototype devices and subsystems, potential interface to existing and or future architectures (hardware and communications), and demonstration of accomplishments in a simulated operational environment. Emphasis should be placed on optimum sensor combination(s), size, weight, power, and communications (sensor to sensor, sensor to soldier(s), sensor to central control point) considerations.

- R&D of advanced techniques for application of Multi-INT sensors and associated technology to *Small Unattended Ground Vehicles (SUGV)* for utilization during Urban Operations. This includes development and testing of prototype dynamic payloads with potential interface to existing and or future architectures (hardware and communications) and demonstration of accomplishments in a simulated operational environment.

- R&D of advanced techniques for application of Multi-INT sensors and associated technology to a *stand off platform* (e.g., UAV Class I-III, Unmanned Ground Vehicle (UGV), Manned Ground Vehicle (MGV)) for utilization during Urban Operations. This includes development and testing of prototype dynamic payloads with potential interface to existing and or future architectures (hardware and communications) and demonstration of accomplishments in a simulated operational environment.

- Trade studies and other technical analysis to determine optimum combination of operational and performance requirements versus technical requirements for application of Multi-INT sensors technology to Urban Operations. This may include employment mechanisms.

Topic title: Collect Signal Intelligence for Electronic Intelligence

The topic of ELINT is concerned with improving the ability to detect, identify, locate, demodulate, survey, search, and correlate Radio Detecting and Ranging (RADAR) targets on the tactical battlefield. Improving man machine interfaces is also important in the ELINT environment. Areas of Research and Development (R&D) include, but are not limited to, super resolution Direction Finding (DF) algorithms, DF antenna array design, system calibration and Electromagnetic Modeling (EM), Radio Frequency Interference (RFI) rejection, critical component development, real-time signal processing, wide-band / Low Probability of Intercept (LPI) signal exploitation, High Frequency-Direction Finding (HF-DF) issues, non-Direction-Finding (DF) signal geolocation techniques, emitter identification, and signal-associated internal/external information extraction. Urban terrain scenarios require signal location through walls and similar materials.

SIGINT Sub-topic # 1 – COMINT Enhancements for ELINT

R&D is required so that ELINT and Communications Intelligence (COMINT) receivers can be combined into a single, dual-use package.

R&D of critical components to improve DF systems is required. Current topics of interest include, but are not limited to: high gain low-noise amplifiers, rapidly tuning notch filters, low side-lobe direct digital synthesizers, and receivers exhibiting the following characteristics:

- Super-high selectivity, sensitivity, and phase stability
- Broad instantaneous bandwidth with low distortion
- High two-tone spur-free dynamic range
- Dual mode (broadband dual channel or narrow-band multi-channel), 14+ bit analog-to-digital converters that operate at 200+Megahertz (MHz), analog devices for spectrum channelization, and adaptive broadband Radio Frequency/Intermediate Frequency (RF/IF) delay devices.

Real-time signal processing in embedded computers has become an ad hoc standard for tactical system design. Closely related to this type of design are the following research topic areas:

- High speed Digital Signal Processors (DSP)
- Optical computing
- Analog Very Large Scale Integration (VLSI)
- Parametric and non-parametric density estimation
- Multivariate sorting and decision support
- High speed algorithm development
- Parallel processing
- Versa Module Eurocard (VME) Bus and future bus architecture improvements

Improvements are needed in the rapid acquisition and processing of SIGINT data as well as in the presentation of this data in a format usable to military operations in support of intelligence, surveillance, and reconnaissance activities requiring multiple user access.

SIGINT Sub-topic # 2 – Improvement of Electronic Intelligence (ELINT) Techniques

This topic addresses advanced ELINT digital IF receivers, algorithms, and processors and their design architectures. Particular emphasis is placed on wide bandwidth ELINT signal processing algorithms requiring small size and low power.

Techniques for computer mediated ELINT intercept, high-resolution and high-throughput analog-to-digital conversion for ELINT signals, parallel processing and exploitation of ELINT for LPI signals, and fast/real-time de-interleaving and clustering of very large Pulse Description Words (PDWs) are of particular interest. An improvement of ELINT sub-system techniques, such as the Radio Frequency (RF) down or up conversion, pulse compression, high probability of detection and interception, pulsed signal de-interleaving and clustering, advanced PDW processing for wide bandwidth emitters, and Tactical-ELINT report generation, is vital.

R&D is required for demonstrating a superheterodyne, fully programmable, digital ELINT IF receiver with a bandwidth greater than 160 MHz. This receiver should include required algorithms and processors.

R&D is required for demonstrating through-the-wall, and/or ground penetrating bi-static/multi-static multi-function RADAR capability.
Advanced ELINT receivers and ELINT receiving techniques should be developed to meet the following performance objectives:

- Agile techniques for automated ELINT intercept, high resolution, and throughput of analog to digital conversion of ELINT signal, processing and exploitation of low-probability-of-intercept signals, de-interleaving and clustering for high throughput production of very large PDWs are of particular interest.
- Advanced geolocation techniques and algorithms for threats in a high-density environment.

ELINT receiver technology should be developed for use against LPI Threat RADAR emissions, with the following characteristics:

- Wide bandwidth
- Small size (mug, slug, and bug-sized receiver sub-system)
- Low power
- Ability to autonomously adapt for optimal sensitivity to a selected signal where a high signal-to-noise ratio sample of the selected signal is present for a very brief period
- Integration of other desired characteristics with miniature robotic systems

SIGINT Sub-topic # 3 – Precision Geolocation

Develop high performance location techniques that deal with the entire process of channel estimation, collection, and location estimation along with time standard, antenna phase center, antennae locations/dynamics, and system calibration data.

Advanced techniques for improving location accuracy in a high-density ELINT environment are of interest. Possible approaches include reducing the entire set of

contributing errors originating from time/space references, measurement/processing devices/techniques, array calibrations, and propagation channel disturbances.

System calibration and electromagnetic modeling, especially as can be globally applied and/or extrapolated to like systems, are of particular research interest. Required R&D includes platform modeling and antenna array modeling.

SIGINT Sub-topic # 4 – Emitter Identification Capability

Develop emitter identification capability targeting both conventional and advanced RADAR operating on various platforms. Different techniques may be applied for different ELINT platforms, although a commonly sharable database is desired. The following areas are of interest:

- Unintentional Modulation on Pulse (UMOP)-based or Pulse Repetition Interval (PRI)-based SEI techniques
- Building a common database or sharable database among different SEI techniques
- Fast data matching techniques
- Performance improvement techniques using sorting and combining multiple pulses
- Estimation of tight performance bound

SIGINT Sub-topic # 5 – Data Thinning & Autonomous Target Search

Develop effective techniques for organizing the collection process and the processed emitter information in order for the system or operators to utilize resources effectively.

Develop an autonomous target search engine that quickly converges on a set of emitters meeting the target profile provided by a target database. The areas of interest include:

- Multi-level emitter externals and internals relational database
- Representing target emitters with accurate PDW
- Hypotheses-driven data mining
- Mission database compatible to the search process
- Search process controller
- Man-machine interfaces for tactical intercept systems

Tactics, Techniques and Procedures (TTPs) shall focus upon utilization of Artificial Intelligence techniques to automate much or all of system control requirements.

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Topic title: Collect – Measurement and Signature Intelligence

Objective: This topic is concerned with providing an initial operational capability for:

- Improving existing capabilities for MASINT sensors
- The integration of those sensors
- Improving MASINT sensors and MASINT system data dissemination

Definitions:

Note: MASINT falls under the functional management of the Defense Intelligence Agency (DIA). Sensors developed under this category may or may not clearly fit into the Army's MASINT definition, shown below.

U.S. Army U.S. Army Intelligence and Security Command (INSCOM) MASINT Operational Concept, 30 May 1997 offers the following definition:

MASINT is the measurement or characterization of any unintentional energy or substance, emitted or reflected from an object that permits unique identification of that object.

A key word in this definition that helps us to understand the scope of MASINT is the word "**unintentional**."

This definition helps us to contemplate the facilitating known component disciplines of MASINT.

Six Component Disciplines of MASINT

MASINT is currently comprised of six primary disciplines: Electro-Optical Discipline, Radio Detecting and Ranging (RADAR) Discipline, Radio-Frequency (RF) Discipline, Geophysical Discipline, Materials Discipline, and Nuclear Radiation Discipline. Conventional thinking and approaches to MASINT disciplines are as follows:

- **RADAR Discipline:** Systems in this discipline illuminate a target with RADAR and collect the reflected energy for analysis. A target reflects radar energy, some of which travels very long distances, in a unique pattern or a radar cross section (signature) that is a function of the shape and material properties of the target. These signatures can be used to identify and classify targets of interest and analyzed further to deduce essential elements of information. Radar systems provide surveillance, detection, tracking, identification, size, and shape characterization of moving targets.

- **Radio-Frequency Discipline:** Organizations working in the Radio Frequency (RF) discipline use systems to collect, process, and exploit RF electromagnetic pulse emissions associated with nuclear explosions or other high energy events. RF systems also collect, process and exploit unintentional electromagnetic radiation features from targets of interest. Applications are classified SECRET.

- Expanded definitions for **Materials** Discipline**, Nuclear Radiation** Discipline**, Geophysical** Discipline**, Electro-Optical** Discipline are classified SECRET.

MASINT Sub-topic #1 – Active and Passive RF MASINT Technology

Requirements. (Abbreviated. See TRADOC Pub 525-66, Mar 08)

TRADOC FOC-03-03: Advanced Collection, Processing, Analysis, Management and Sharing of Information. A network of advanced sensors that sense in multiple domains (e.g., radio frequency, thermal, acoustical, Electro-Optical (EO), Infrared (IR), seismic) and operate independently, or as components of other systems/platforms, including dismounted soldiers, manned/Unmanned Ground Vehicles (UGVs), manned/Unmanned Aerial Vehicles (UAVs), satellites, and even cyber-based platforms. Networked ISR is linked to all shooters. Soldiers and leaders will be empowered with timely, accurate information about terrain and weather, and will receive accurate, timely, up-to-date digital map information of the battlefield. Units will be able to receive and disseminate terrain and weather information immediately throughout the Area of Operation (AO), even while en route, to gain the advantage at all times. The network automatically collaborates raw data to provide actionable/targetable information, directly to soldiers, for immediate action/engagement. The network also provides information for assessment by highly trained intelligence analysts to generate or refine Situational Understanding (SU).

Objectives:

- Research and development (R&D) in identification and geo-location of **non-cooperative target identification** through RF MASINT technique in RF frequency range for all mission areas in the Air to Ground and Ground-to-Ground architecture. Key entities to be identified in the architecture include (but are not limited to) ground, airborne, and dismounted targets by active and passive techniques. The emphasis is to provide the identification and geo-location of the target signature information at the stand off distance required by the missions. Operational covertness, operational robustness in the presence of countermeasures, interoperability with existing systems in the architecture and minimization of cost, size, and weight are required.
- R&D of advanced RF MASINT systems, active and passive sensors for ultra-lightweight, airborne applications at tactical ranges. Ultimate use is in Unmanned Aerial Vehicles (UAV) and pods for a variety of air vehicles. This includes testing of prototype devices and subsystems.

- Tradeoff and other technical analyses to determine optimum combination of operational and performance requirements vs. technical requirements for tactical operations. These should take into account factors such as payload size and weight vs. target velocity, geo-location accuracy and range, and on-board (image formation) processing vs. data link requirements.

MASINT Sub-topic #2 – System of Systems Integration of Delivery, Processing and Dissemination Systems

Requirements. (Abbreviated. See TRADOC Pub 525-66, Mar 08)

TRADOC FOC-03-03: Advanced Collection, Processing, Analysis, Management and Sharing of Information. 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, and present targets and other streaming video and text information to commanders and staffs. It is supported by adaptive reasoning tools that automatically collate and transform sensor data into knowledge 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. Required capabilities include highly advanced information processing, employing automated filters, decision support aids, comparative analysis, 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-03-04: Network Operations. Objective Forces must be interoperable with Joint forces and systems consistent with the mission and responsibilities of each echelon of the Unit of Action (UA). The Future Combat Systems (FCS) must be capable of supporting operations with legacy and interim units, coalition forces, and law enforcement agencies.

Objectives:

- Research and Development (R&D) of MASINT **sensors integration** into current and future delivery systems for battlefield requirements. Develop electronic and mechanical systems to deliver and or retrieve MASINT collection devices at precise locations. Develop packaging technology to allow MASINT devices to withstand the delivery process. Develop expendable delivery systems for MASINT sensors for battlefield environments to meet tactical and operational level of war requirements.

- R&D of MASINT sensor/system **processing capability** for U.S. Army requirements. Tradeoff and other technical analyses to determine optimum

division of processing capability at the remote sensor and the local processing systems. Develop and fabricate prototype system of systems to test within the context of the Future Combat System (FCS).

- R&D of MASINT sensor/system information **dissemination** processes to enhance the integration of current and future Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems. Tradeoff and other technical analyses to determine affordable solutions to integrate the dissemination process into Army and Joint C4ISR systems.

MASINT Sub-topic #3 – Sense Through the Wall

Requirements: (abbreviated; see TRADOC Pub 525-66, Mar 08**)**
TRADOC FOC -02-02: The Ability to Observe and Collect Information Worldwide. Capstone capabilities for observing and collecting information worldwide include: Find, fix, track, target, and assess IEDs (and networks), weapons, munitions, and full spectrum chemical, biological, radiological, nuclear, and explosives (CBRNE) and WME. • Detect, image, and characterize activity within urban structures and complex terrain. • Detect, identify, and track in near real time, with precision friendly and enemy forces, neutrals, and other groups in close proximity at standoff distances. This capability includes individual leadership figures and high value targets, in a complex and chaotic urban environment. • Detect, image, and characterize activity in sub-surface locations. • Find, fix, classify, and track friendly, enemy, and neutral fixed and moving equipment and people.

TRADOC FOC-03-02: Operations in Urban and Complex Terrain. Capstone capabilities for operations in urban and complex terrain include: Systems must have the ability to move rapidly across open areas, and be highly maneuverable within the confines of the urban operational environment. • A wide array of sensors to 'fill gaps' during large urban area operations • A variety of robotic platforms, Unmanned Aerial Sensors, and Unmanned Ground Vehicle, which will assist with clearing operations allow for greater Soldier standoff, provide early threat and hazard detection, conduct breaching operations, assist in reconnaissance, perform high-risk clearing operations and employ a wide variety of nonlethal effects • Employ a significant number of sensors and unmanned systems within the urban core, and on the periphery, to monitor noncombatant activities, and provide early warning against enemy activities. Sensors that can monitor more than one dimension/media simultaneously will assist the Joint Force Commander (JFC) in monitoring significantly more of the OE, while allowing the majority of the maneuver force to continue mission preparation, and other essential tasks.

Objective:

- This topic is concerned with providing an initial operational capability and/or improving existing capabilities to exceed threshold requirements and provide

mounted/dismounted users with the capability to detect, locate, and "see" personnel with concealed weapons and explosives who are hidden behind walls, doors, visible obstructions and inside structures in complex urban environments. Walls consist of exterior and interior walls, which include drywall, brick wall, cinderblock, concrete, and adobe/stucco.

Description:
Sense Through the Wall (STTW) capability has direct application to both US Army and Special Forces requirements for Military Operations In Urban Terrain (MOUT) and hostage recovery operations. One version will be soldier borne and modularly designed to facilitate integration into a Future Combat System (FCS) Small Unattended Ground Vehicles (SUGV). Another configuration will be mounted on a larger FCS Unmanned Ground Vehicle (UGV), manned vehicle or Unmanned Aircraft System (UAS) and will have increased standoff distance from the target area. The Suite of STTW systems will provide: near real time situational awareness information, persistent sensing capabilities, increased standoff distance without sacrificing probability of detection, geo-location data on multiple targets, detection of moving and stationary targets, detection of multiple targets in the presence of clutter, detection of concealed weapons and concealed explosives from a standoff distance, detection of targets through various wall materials (including dense materials with higher attenuation properties), and be capable of operation while on the move. Users of STTW information should not require new skills to perform analysis of data. Ideally, the STTW sensors should not have any electromagnetic interference impact on any sensors or communications devices presently fielded to DOD components.

STTW Capabilities Description

- Near real time situational awareness and persistent surveillance information
- Achieve Probability of Detection without exceeding Probability of False Alarm limits
- Improve Standoff capability
- Detect multiple targets through multiple wall types in presence of clutter
- Detect targets in motion and stationary targets
- Develop user-friendly interface
- Improve Graphical User Interfaces (GUIs) (i.e. icon displays for detected targets with geo-location information)
- Improve location accuracy of targets
- Operation on the Move capability
- Detect concealed weapons and explosives behind walls in urban environment
- Develop integrated STTW system (detect personnel, concealed weapons, and explosives through walls)
- Develop common Graphic User Interfaces (GUIs)
- Soldier borne versions shall weigh no more than 6 pounds and be capable of 4 hours continuous operations minimum without replacing power source

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Capabilities Required: Multi-band and multi-mode systems, exploitation of features and signatures, novel signal processing techniques and approaches for user interface, power management, and a system of systems approach is anticipated. In order to achieve extended standoff missions, the STTW capability may need to be based on other manned/unmanned vehicles/platforms.

Topic title: Electronic Warfare for Air and Ground Survivability

Objective:

- The objective is to protect personnel and platforms from threats that have electromagnetic components or electromagnetic susceptibilities. Threat warning, threat identification, jamming, high-power destructive techniques, and electronic deception are implicit in this objective. Relevant platforms for protective devices and protective suites include individual soldiers, rotary aircraft, fixed wing aircraft, and ground-based vehicles. Air and Ground active and passive protection systems should be considered for RF, Laser, IR/UV, and hostile fire detection systems.

The objective will be met in the following ways:

- Design, development, and testing of new protective equipment, protective suites, and techniques
- Enhancement of existing protective equipment and suites
- Maintenance, improvement, and expansion of in-house simulations, simulators, test equipment and databases
- Technical support to fielded equipment

Requirements: Relevant FORCE OPERATING CAPABILITIES (FOC's) are posted below in an abbreviated format; see TRADOC Pub 525-66, 7 March 2008.

Mounted/Dismounted Maneuver
FOC-03-01: Mobility a. Capstone Capabilities.
Units must possess superior capability to detect presence, identify disposition, and counter antitank and antipersonnel mines, above and below surface, and booby traps/IEDs, such as side-charge and remote detonated mines. Units must possess superior capability to detect and identify CBRN hazards. Mounted units require the ability to conduct route reconnaissance with forward looking and off-road sensors, to clear at greatly improved speeds (at least 50 kilometers (km) per hour). Specific capabilities include: • Enable protective countermobility and survivability position support available at transition to defensive operation. • Incorporating full spectrum CBRN sensors, detectors, analyzers, and classification devices into ground and air vehicles. • Provide near real time CBRN agent detection capability.

Maneuver Support
FOC-06-01: Enable Freedom of Maneuver
Enabling freedom of maneuver includes all those actions that guarantee the JFC the ability to deploy, move, and maneuver, by ground or vertical means, where and when desired, without interruption or delay, to achieve the intent. The counter IED missions are critical aspects of enable freedom of maneuver. The fundamentals of assured mobility are: predict, detect, prevent, avoid, neutralize, and protect. These six fundamentals represent overlapping and concurrent tasks that must be accomplished, allowing the JFC to mitigate impediments to mobility from standoff, and greatly reduce the likelihood of traditional breaching or neutralization requirements. Applications of route security and clearance route include reconnaissance and surveillance techniques to enhance situational awareness for platform survivability.

Ability to differentiate between IED explosives at standoff distances. Ability to deploy and detect full spectrum chemical, biological, radiological, and nuclear (CBRN) sensors along with RF and IR sensors in support of platform survivability. The sensors must be operational during daylight, darkness, and adverse weather conditions are also a critical requirement.

Air Maneuver Operations
FOC-04-02: Effective Aviation Operations in the Contemporary Operating Environment
Key air maneuver missions envisioned for future Modular Force are: close combat attack, interdiction attack, reconnaissance, security, vertical maneuvering, and air movement. • Conduct survivable missions against threats that include unconventional and hard to detect opponents who may use cover, concealment, camouflage, denial and deception tactics, including operations in close proximity to noncombatants and civilian structures. • Survivable aircraft that counter threat offensive systems, survive weapons' lethal effects (to include CBRNE), and prevent/limit crew and passenger injuries, and system damage in crashes. • Conduct safe, worldwide, aviation operations (manned and unmanned systems in a degraded visual environment and complex terrain), including flight path and landing zone obstacles (wire, trees, poles, towers, vehicles, etc.), by crewmembers in high task loaded environments• Enhanced crew mission performance through management of cockpit workload to allow the crew to maintain better external SA and SU. Aviation survivability and reaction time are insufficient against unpredictable and hard to detect threats. Manned and unmanned aviation systems often operate against unpredictable threats and within the range of small arms fire, rocket propelled grenades, man portable air defense systems, antihelicopter mines, and natural or emplaced flight path obstacles. Ground and air platforms that employ the best combinations of low observability, ballistic protection, long-range acquisition and targeting, early attack, and high probability of first round hit and kill technologies will be required to ensure the desired degrees of survivability.

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Line of Sight (LOS)/Beyond Line of Sight (BLOS)/Nonline of Sight (NLOS) Lethality for Mounted/Dismounted Operations

FOC-05-01: LOS/BLOS Lethality
Electronic warfare (EW) includes any military action involving the use of electronic measures (EM) and directed energy (DE) to control the EM spectrum or attack an enemy. There are three major categories of EW: electronic attack, electronic support, and electronic protection. Military operations are executed in an increasingly complex EM environment. EW provides scalable lethality as a key component to fires that has been largely missing and is now required for all potentially hostile operations. EW provides the means to achieve decisive operations, freedom of maneuver, and FP in highly volatile, distributed environments without the politically unacceptable repercussions often tied to more lethal options. EA is the use of EM energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Thus, EA adds both lethal and nonlethal capabilities to LOS/BLOS fires. Aerial EW platforms provide the best EA capability with the best delivery options.

Teaming capability by Battle space Awareness and EA fire systems, dispersed throughout the Operational Environment is critical. A system of systems framework will achieve the requirements for such a capability. It is critical that an enabling, integrated networked fires functional component within the BCS of systems leveraging a wider set of capabilities, including sensors, C2, and attack means from Army, joint and multinational forces will provide the operational capability. Protective EA fires can also support maneuver by suppressing enemy air defenses, degrading, disrupting, or destroying enemy sensors and C2, countering the fires from enemy indirect fire systems and disrupting enemy access to critical space based capabilities with space control capabilities.

Ability to provide protection of strike systems and platforms from enemy EW effects. (Soldier platform to ARFOR and CJFLCC levels). • Ability to employ EW in support of IO and Electronic deception.

EW Sub-topic #1 – Radio Frequency Sensors/ Receivers/ Countermeasures

Research and develop: 1) RF active/passive sensors and RF receivers for threat warning, and 2) countermeasure system development for aircraft and ground vehicles.

- Research, develop, and implement ultra high-speed, ultra-wide (multi-octave), high dynamic range analog input bandwidth Analog to Digital Converters (ADCs) that can be used in digital receivers to replace RF tuners and also to offer functionality not possible with current receivers. The conventional receiver architecture requires an RF tuner for channel selectivity in the analog domain prior to digitization and

digital signal processing. The limiting factors of such architecture are the analog input bandwidth, dynamic range, and sampling frequency of the ADC. Until now, it was impossible to obtain cost-effective ADCs with greater than 1Gigahertz (GHz) analog input bandwidth and greater than 1 Giga-Samples Per Second (GSPS) sampling frequency. Replacing RF tuners with a high-performance ADC allows simultaneous digitization of the entire RF input signal. This also results in a reduction in power consumption, cost, and size associated with receivers containing multiple bulky RF tuners.

- Increasingly, the need to geo-locate or, at a minimum, have very accurate direction of arrival of a threat emitter signal(s) in the battlefield and multipath environments has been recognized as necessary to target and cue weapons. Design and evaluate a prototype plug and play modules that will evaluate either multipath signals and/or the free energy from battlefield emitters in a Bistatic mode of operation to locate threat targets with sufficient accuracy to target or, at a minimum, cue other weapon systems to target the threat.

- Extending the capability of EW systems to cover the lower frequency ranges will allow the interception and classification of signals (including communications) by common equipment. Develop and evaluate a prototype module that can be integrated into an Electronic Countermeasure (ECM) system that will allow the reception of lower frequency ranges and then prove the usefulness of increased capability.

- Research and develop innovative techniques to reliably detect Rocket Propelled Grenades (RPGs) at meaningful distances so that countermeasures or evasive action can be taken as required. RPGs are an increasing threat to airborne platforms. Focus on improved efficiency to the query pulse and improved signal processing of the returned response to identify RPGs and other small arms with an objective of enabling the use of current EW assets in the process.

EW Sub-topic #2 – Infrared Countermeasures

- Research, develop and implement Infrared Countermeasure (IRCM) technology with emphasis on key system components, such as high power laser sources, electro-optics, fiber-optics, pointing/tracking devices, advanced jamming techniques against passive homing, command to line of sight, and beam-rider missiles. Research and Development (R&D) shall include systems concept research and design, analyzing threat capabilities, developing system prototypes, and conducting proof-of-concept laboratory and field demonstrations.

- Develop improved infrared sources particularly in, though not limited to, the 3-5 and 8-12 micron spectral regions. Emphasis is on efficient conversion of electrical to optical energy.

- Research and develop advanced IRCM techniques and devices to spatially and/or temporally modulate Infrared (IR) radiation. Their ultimate use would be in countermeasures systems used to jam threat weapons/sensors. Employment would be on Army aircraft and ground vehicles. Threats include IR guided/unguided missiles, smart munitions and unguided projectiles.

- Conduct digital and semi-physical simulations of IR guided missiles to assess effectiveness of advanced IRCM techniques/technologies. Techniques/ technologies would include omni-directional and directional jammers, multi-spectral decoys, and combinations of the above.

EW Sub-topic #3 – Multi-Spectral Electro-Optics/Infrared/Ultraviolet Sensors for Warning/Countermeasure

- Research, develop and implement multi-spectral active/passive sensors/devices for threat warning and to cue countermeasure systems. Threats include laser-guided missiles and other laser aided weapon systems (laser rangefinders/ designators/ beamriders), Anti-Tank Guided Missiles (ATGMs), IR surface-to-air missiles, top-attack smart munitions, and small firearms such as RPGs.

- Develop, fabricate, and demonstrate multi-spectral threat warning/ countermeasure system to provide sufficient early warning to vehicle commander and provide accurate and precise threat direction of arrival for countermeasures with emphasis on low-cost, efficient and conformal systems.

- Additional emphasis shall be on Horizontal Technology Integration (HTI) of EW sensors and open-architecture infused with low cost and adapted Non-Developmental Item (NDI) technologies for air and ground vehicle threat detection. The purpose shall be primarily to control and direct countermeasures, but also for target cueing, situational awareness, combat identification assistance and off-board sensor network communication.

EW Sub-topic #4 – RADAR Countermeasures, Warning and Deception

I2WD requires R&D of:

- Advanced Phased Array/Monopulse, Bi-Static, Synthetic Aperture Radar (SAR) Deception and Countermeasure Techniques - New weapon systems employing phased array/monopulse, bi-static, and SAR hardware and processing must be countered to negate their threat to Army Fixed and Rotary Wing Aircraft. Research shall focus on low-cost effective monopulse and phased array countermeasures such as on-board countermeasures, off-board countermeasures, and cooperative Electronic Attack (EA) (countermeasures). In addition, methods to implement such

techniques as cross polarization while lowering system production and maintenance costs are desirable. Deception against all types of advanced radars is also needed. The goal is to analyze future Threat capabilities, develop the technical performance requirements for a countermeasure system, design countermeasure/deception techniques for testing, and conduct test programs with final reports.

- Low Cost, High Accuracy, Ultra-Wide Bandwidth Direction Finding for Radar Warning Receivers - Improved Angle of Arrival (AOA) accuracy (over 7-8 octaves) is needed to support situational awareness displays on future air and ground vehicles. The goal is to increase the accuracy of radar warning by developing innovative antenna receiver, Command, Control, Communications, Computers, and Intelligence (C4I) data fusion, Air Defense Artillery (ADA) based expert system software and processor technology that can be field tested on both ground and airborne vehicles.

- Countermeasures Against Top Attack/Smart Munitions - Innovative countermeasures to counter top attack/smart munitions are needed to protect ground vehicles, high value targets, and personnel from smart sensor based weapons. The goal is to analyze the Threat capabilities, develop countermeasure prototypes against RF based radar sensors in smart munitions, and conduct proof-of-principal laboratory and field demonstrations.

- Ultra-High Speed and Ultra-Wide Bandwidth Digital Receivers and Modulators Development - Future Threat radar capabilities and signal characteristics will require a new generation of RF countermeasure receivers and modulators. They shall be applied to deceive and/or jam advanced coherent radars such as imaging, Low Probability of Intercept (LPI), and frequency hopping radars. Research ultra high-speed, ultra-wide bandwidth digital receiver and modulator technologies (e.g. Digital RF Memory (DRFM), Field Programmable Gate Array (FPGA), Direct Digital Synthesis (DDS), Fiber Optics, etc.), and develop prototypes. The purpose of digital receivers and modulators are to: 1) allow simultaneous digitization of the entire RF input signal, thus eliminating or reducing the need of RF tuners, and 2) allow simultaneous countermeasure waveforms to be modulated onto the digitized RF signal. The digital modulators shall be programmable to generate coherent Electronic Counter-Measures (ECM) techniques that can be modulated onto the digitized RF threat signal prior to retransmitting the RF back to the threat receivers. Perform tests to demonstrate the feasibility of advanced ultra-high speed, ultra-high bandwidth digital receivers and modulators using advanced coherent digitized ECM waveforms to counter advanced coherent radar systems (such as air defense radars, homing missile seekers, proximity fuzed artilleries/top attack munitions, and imaging radars) which uses the latest Electronic Counter-Countermeasures (ECCM) features.

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

EW Sub-topic #5 – Advanced RADAR Countermeasures

I2WD requires R&D of advanced RADAR Countermeasures (RCM) for Information Operations applications. Specific areas of interest are:

- new countermeasure concepts and techniques
- technique evaluation methods
- value-added analysis
- critical sub-system improvements

Military system trends indicate movement toward more capable, but less complex electronic systems. Added capability comes at the expense of system vulnerability. RF based architectures are particularly susceptible.

Exploiting these vulnerabilities can provide a wide range of effects applicable to Information Operations. When understood in the context of military operations, these effects can be used as a force multiplier.

R&D under this EW sub-topic shall address the following areas:

- Revolutionary RCM concepts and techniques
- Revolutionary concepts, techniques, and non-traditional electronic attack (countermeasures) and technologies are sought that can expand the scope and impact of EA in military operations.
- Corresponding new RCM technique evaluation methods
- The cost, risk, and time currently associated with evaluating and optimizing hardware implemented RCM technique are becoming increasingly prohibitive. A better approach is needed to evaluate technique potential and optimize performance earlier in the process. A virtual or a mixed virtual/real approach may be the solution.
- Operational Value
- Countermeasure techniques must be viewed in the context of operations. Methods and tools are needed to identify and quantify value-added within specific phases of military operations.
- Novel or improved RCM sub-systems and components
- New and novel methods of performing RCM using coherent devices are a driving factor. Submissions are requested pertaining to development of coherent devices, solid-state power amplifier, and advanced state-of-the-art receiver technology sub-systems that extend the current performance envelope.

EW Sub-topic #6 – Electronic Deception & Advanced Signature Management

Approach:

- Develop and/or demonstrate technologies for revolutionary assets and personnel signature manipulation/suppression techniques that deliberately alter an adversary's perception of friendly force existence, location, identification, capabilities, intentions, or operations. Such manipulations of signature shall cause the Threat to take specific actions (or inaction) that contribute to the success of friendly force missions by enhancing survivability or concealing friendly force assets.

- Concealment emphasis shall be based on Low Cost, Low Observable (LCLO) systems to provide mobile and semi-mobile Command, Control, Communication, Computer, Intelligence, Surveillance, and Reconnaissance (C4-ISR) assets, including Tactical Operations Centers (TOCs), with low cost, low burden survivability upgrades addressing detection avoidance in global battlefield conditions. The approach is to utilize an integrated system of both physical devices and electronic devices to deceive Threat systems such as sensors, smart munitions, or C4-ISR assets, under battlefield conditions.

Key technologies for demonstration:

- Electronic deception devices to include three-dimensional electro-optical image projection
- Synergistic coupling of physical and virtual decoys multi-spectral signature management to improve survivability of TOCs and C4-ISR assets
- Model and simulation tools to enable planning, coordination, and implementation of military deception activities
- Fully active Integrated Modular Electronic Deception System (IMEDS) operating in the RF, electro-optic, Infrared (IR), acoustic, seismic, and communication bands for tactical, operational, and strategic missions
- Materials and coatings to reduce equipment and solar loading signatures
- Camouflage screen to reduce the signature of general purpose platforms

EW Sub-topic #7 – Projectile Warning / Tracking using LADAR

LADAR stands for *LAser Detection And Ranging*. It is also commonly referred to as LIDAR, for *LIght Detection And Ranging*. Its operation is similar to radar but involves the use of light, typically a laser, rather than radio waves.

- Research, develop, and demonstrate an effective LADAR system to acquire and track ballistic missiles/payloads, improve intercept prospects, and assess results of intercepts. Current approaches may have insufficient range or discrimination capability, require more platforms/interceptors and more expensive defense than

desired, or have unacceptable target leakage/false alarm rates. Passive systems, even with projected technology, lose too much discrimination performance and battlespace to evolving threats. Currently conceived LADAR systems either have insufficient range and discrimination performance, or may include immature technologies which threaten reasonable deployment time frames.

- Investigate novel coherent LADAR/processing/tracking systems to detect incoming projectiles, make acquisition of projectiles in the boost phase, and discriminate the projectiles from the background in the post-boost phase prior to the deployment of decoys and other countermeasures.

- R&D shall include systems concept research and design, analyzing threat capabilities, developing system prototypes, and conducting proof-of-concept laboratory and field demonstrations.

EW Sub-topic #8 – Integrated ASE (IASE) Hardware/Host Evaluation

- Review/evaluate host processor candidates for processor, memory and interface capabilities to host IASE Government-owned software with respect to current legacy ASE suite augmented by an emerging HFDS solution.
- Evaluate integration complexity of Government-developed Integrated Aircraft Survivability Equipment (IASE) software into the supplied candidate host processor, as well as A-kit and B-kit implications.
- Interest in host candidates is limited to boxes at technology readiness level 7 or higher. Candidates can be fielded ASE processors, modified ASE processors, or non-ASE processors which have potential to host the IASE software.

EW Sub-topic #9 – Advanced Radar Warning Receiver Demonstration

The current APR-39A(V)1/4 RWR is a Crystal Video Receiver (CVR) based system that was developed in the early 1980's and utilizes PRI, Pulse Width and Scan as the primary discriminates for threat emitter ID. Insertion of Digital Receiver technology will greatly increase the pilot's situational awareness by increasing the Probability of Detection/Probability of correct Identification, increase sensitivity, and reduce the number of threat ambiguities and the False Alarm Rate (FAR).

I2WD is requesting proposals from industry to support an Advanced Digital receiver RWR hardware-in-the-loop demonstration at the I2WD Aberdeen Proving Ground facility. Testing will determine the Technology Readiness Level (TRL) of industry to develop a low cost, light weight Advanced Radar Warning Receiver for aviation platforms that can be integrated into the existing APR-39A(V)1/4 footprint.

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

The information provided may be used by the Army in developing its acquisition strategy and performance specifications.

Specific entrance criteria are as follows:

- System hardware/software shall be TRL 6 or better.
- System shall fit in the footprint of the APR-39 A(V)1/4 or submittal of a growth path to achieve the footprint (size, weight and power (SWaP)).
- System shall be able to be programmed with Government provided threat list.
- System shall be able to support direct and/or free space testing.
- Contractor shall provide any special test equipment required to verify system performance.
- Testing will include direct injection and free space radiation of threat RF signals.
- System shall be ready for testing 4 months after contract award.
- Interested parties are responsible for adequately marking proprietary or sensitive information contained in their response.

Topic Title: Offensive Information Operations

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

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 BAA 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.

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

OIO Sub-topic # 1 – Communications Electronic Warfare

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

- EW TTPs
  - Development of EW architectures, specification and supporting protocols facilitating interoperability and cooperative and distributed system operation
  - Application of Artificial Intelligence (AI) or Expert system or dynamic scheduling for the purpose of automating the functions of target signal detection/selection and jam/no-jam decisions based on appropriate target information and defined user parameters.
  - Research and development of efficient, low power, low duty cycle EW techniques against current and emerging threat technologies.

  - Propagation and environmental modeling and simulation technologies leading towards an improved understanding of phenomena in both urban and rural deployment environments involving new or unique communications capabilities

- EW Interoperability
  - Ability to coexist and/or interoperate with electronic force protection systems
  - Ability to minimize interference with warfighter communication systems
  - Research and modeling of the effects a common timing protocol will have on EW system interoperability and effectiveness
  - Ability to disseminate information within Common Operating Environment (COE) picture.

OIO Sub-topic # 2 – Cyber Electronic Warfare

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

OIO Sub-topic # 3 – Distributed Electronic Warfare

Historically, Electronic Attack (EA) systems have been designed to mitigate a single electromagnetic threat. This has caused the development and proliferation of a multitude of EA platforms to counter the large number of RF threat devices being utilized by our adversaries with little or no regard for interoperability or supportability. Consequently, our warfighters are now overburdened with the training, deployment, sustainment, and coordination responsibilities associated with each of these diverse assets. The next generation Electronic Attack system must reduce this burden by facilitating the integration of all of these threat specific capabilities within a well defined and flexible EA framework which can operate in a stand alone or distributed mode.

The next generation EA system must be based on a flexible and robust software architecture. This architecture must be able to minimize and abstract HW dependencies, allow for rapid development and integration of new attack waveforms and techniques, and support concurrent mission execution against a diverse target signal set. Furthermore, to maximize effectiveness and efficiency, advanced EA

systems require specific target information for identification, classification and targeting purposes. As such, next generation EA systems cannot solely be designed to conduct Electronic Attack but must be inherently able to concurrently perform necessary Electronic Support (ES) functions.

The envisioned architecture, as depicted in Figure 1, provides these capabilities. The architecture is modular, layered and is based on a service oriented structure, with each component providing services to the layer above via a well defined software interface; guaranteeing the required capabilities and performance, while at the same time abstracting internal as well as lower layer implementation details. This SW architecture was specifically designed to abstract and minimize hardware dependencies, facilitate the development and integration of advanced Electronic Warfare techniques as well as to inherently support concurrent execution of multiple EW missions against a potentially dense and heterogeneous target environment.

Figure 1.

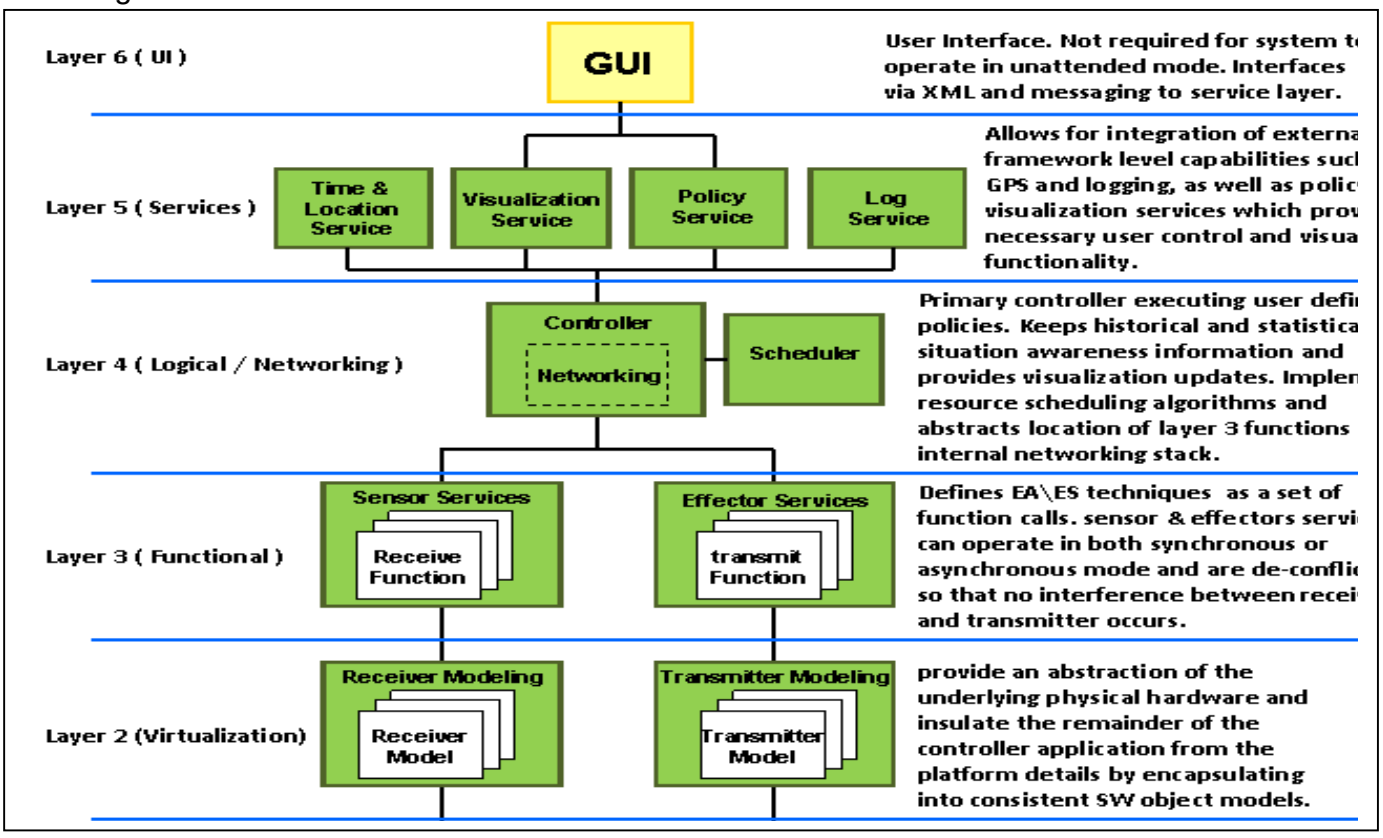


Figure 2.

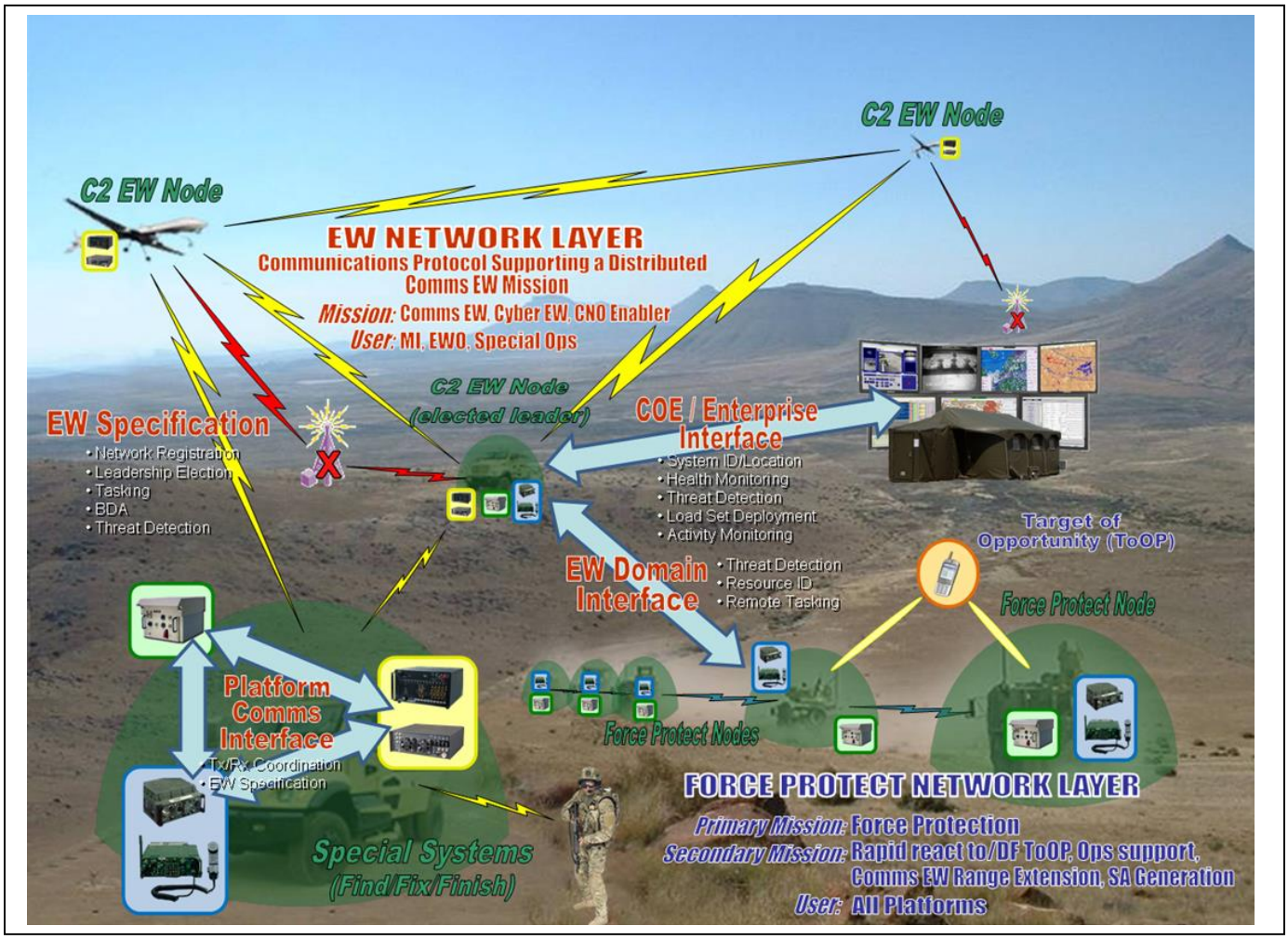


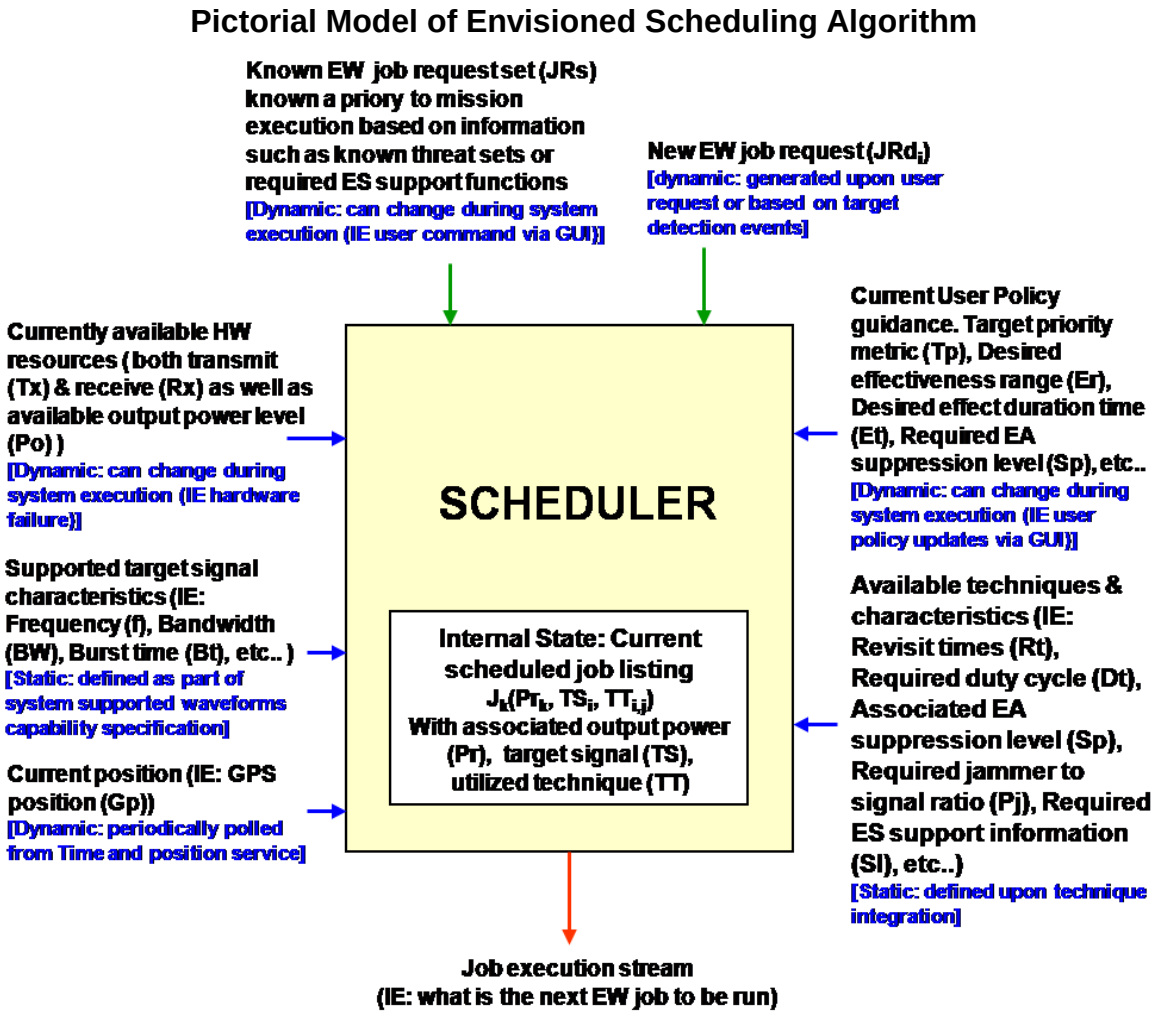
Figure 2 depicts the outcome of this development effort that would give the Army the ability to provide any third party EW system developer a standardized EW system specification with associated network interfaces, including a protocol stack and a Software Development Kit (SDK) for supported hardware. This will enable interoperability between all newly developed EW systems. It is further envisioned that such a specification will allow for various levels of EW network membership from simple ES sensors, to single signal or multi-signal taskable ES and/or EA nodes, as well as fully capable systems able to assume group leadership and scheduling responsibilities.

Challenges remain in the development of the supporting mechanisms required to allow for simultaneous execution of EA and distributed ES missions, such as geo-location, which will be required for the optimal tasking of individual nodes within the EW network. Furthermore, it is important to note that all coordination and update messages traversing the network must be passed without interference from ongoing EW missions, which may likely be reactive and unpredictable in nature.

Efficient scheduling algorithms to support this next generation EW concept will need to be developed. Existing well understood scheduling methods are not suited to account for the complex and highly interdependent nature of all the diverse EA and ES jobs which will be dynamically generated by the system during execution.

Figure 3 provides a conceptual model of an envisioned scheduler with currently considered input and output parameters.

Figure 3.



The goal of the scheduler should be the optimal (or near-optimal) utilization of available HW resources, while at the same time complying with user defined policies (e.g., target priority and/or threat level assignments). Many of the jobs to be scheduled within the

system will be dynamically generated during mission execution as new target signals are identified. However, the scheduler must also be able to support repetitive ES/EA tasks. Furthermore, jobs can be either periodic or aperiodic, depending on the technique being utilized. The scheduler must also mitigate interactions between receive and transmit functions and ensure that scheduled tasks do not interfere with each other. Based on the complex nature of this problem space, an optimal scheduler may not be achievable, however, it is hypothesized that a scheduling algorithm that operates at an acceptable level of performance and fidelity is possible.

As previously discussed, it is proposed that the next generation EW system cannot just be composed of individual independent units, but must be able to expand its operational effectiveness and efficiency by networking amongst all available ES/EA resources. The envisioned EW network is hierarchical in nature with an elected group leader assuming the scheduling responsibilities for all registered EW nodes.

This will require scheduling algorithm augmentations to account for the challenges (and advantages) which are present when scheduling across a distributed environment. This higher layer distributed scheduler will need to keep state information for all identified and assigned threat targets, as well as currently executing ES missions. Then, based on all the aggregated information, the lead node must properly assign and distribute EW jobs based on additional factors such as capability (C), current load (CL), and RF vantage point to the target (Vp), while at the same time continuing to manage its own resources.

OIO Sub-topic # 4 – Electronic Warfare (other)

I2WD is also interested in research and development activities that will enable / facilitate the ability for EW system to conduct the following operations

- Psychological operations (PSYOP)
- Electronic deception
- Directed energy

OIO Sub-topic # 5 - Computer Network Operations

Descriptions:
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.

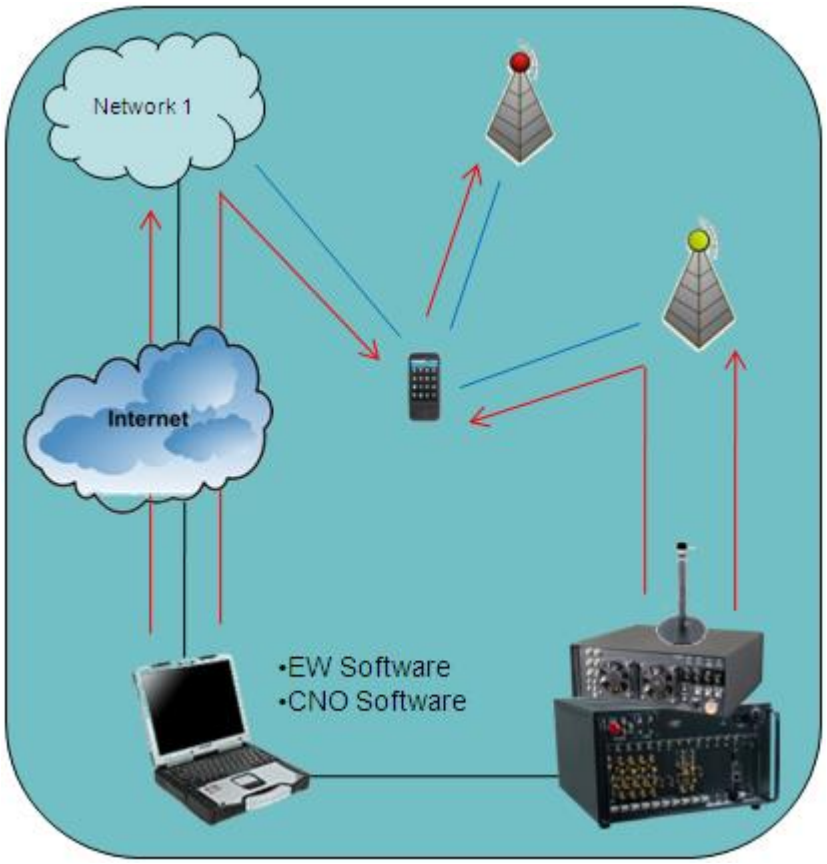
- Stealthy component mapping of logical networks and location data correlation and deconfliction with other all-source intelligence data.

- 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 (R&D) of TTPs to accomplish this collection, fusion and overlay of pertinent data shall be required.

OIO Sub-topic # 6 – Cyber EW Framework

A critical need for an integrated, offensive focused framework has arisen to allow for the rapid integration of new techniques, new technologies, and 3rd party applications. This framework needs to be flexible, modular, and scalable to allow for interoperability with other similarly focused frameworks.

This framework should have common interfaces to allow for other linkages to other system frameworks, whether they are Electronic Warfare (EW) frameworks or Computer Network Operations (CNO) frameworks. The future offensive Cyber Electronic system will be a convergence of EW and CNO capabilities to allow for cross domain and full spectrum coverage as shown below in the following figure.



This framework will allow for the execution of cross domain effects such as performing Electronic Surveillance (ES) using EW methods and performing effects against those targets using CNO techniques and vice versa.

This framework needs to allow for the execution of the following types of mission at a minimum:

- Network Surveillance and Reconnaissance
- Command and Control (C2)
- Traffic Analysis
- Resource Management
- Intelligent Scheduling
- Effect Execution

OIO Sub-topic # 7 – Software Agent Technologies

The U.S. Army has a requirement to research, develop, test, evaluate, and demonstrate **software agents**[1] that can be shown to contribute to military operations such as:

- Computer Network Operations[2]
- 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

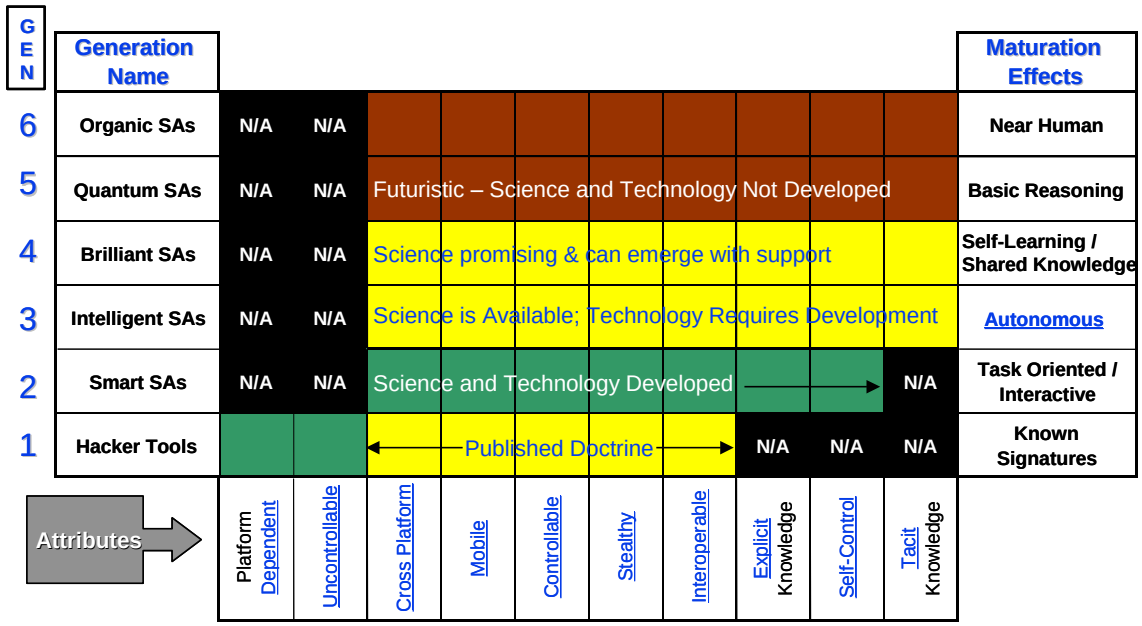
[1] Software agents are discrete bundles of computer code that go out onto and into the network environment to perform functions in accordance with their design.
[2] Computer Network Operations (CNO) is comprised of three sub-components that are Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Defense (CND).

- 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

Special consideration shall be given to R&D proposals that exhibit revolutionary and innovative software agent solutions within the context of military operations.

Figure 1 illustrates desired generational maturation of software agents.

Figure 1



OIO Sub-topic # 8- OIO Technique Development

Descriptions:
Applications of research in this area are aimed at cutting edge capabilities that could be considered enabling technologies for the full spectrum of Information Operations capabilities that would be relevant to the Army in a tactical environment. The key objective of this research and development is to discover new TTP's targeting both voice and data communication technologies maximizing jammer system efficiency and at the same time minimizing required power output and duty cycle times.

Technology is advancing at an ever increasing rate, but instead of the historical model of military forces being the driving factor behind the advancement of technologies, the commercial sector has become the driving force. Because of declining defense spending worldwide, as well as the significant rise in the number of asymmetric threats, the integration of commercially available components into threat devices is now the norm rather than the exception. This has enabled a wider variety of technologies to be employed against US forces than ever before. These systems provide high data rates for data transmission and communications, as well as much broader use of the electromagnetic spectrum. In many cases, adversaries use commercially available technology to take advantage of lower acquisition and sustainment costs, ease of use and the reliability of these devices. The use of commercial devices as threats makes it very difficult to differentiate between threats and devices being used for legitimate purposes.

Simple jamming techniques which require continuous or extensive transmit time will severely hamper system performance by limiting receive functionality within that transmission band and utilizing transmitter resources inefficiently. As such, we must develop more advanced EA techniques that require the least amount of power and transmit time possible while still successfully achieve their intended effect.

The techniques development process begins by identifying and obtaining specific threat devices identified by the Threat Working Group. Techniques Development then follows a process with clearly defined management controls and timelines. All findings are aggregated and a detailed findings report is generated, reviewed, and submitted for release to government and supporting contractor organizations.

1. Signal Characterization

The first phase of the techniques development process is Signal Characterization. This includes capturing, digitizing and recording all signaling waveforms and reverse engineering the signal characteristics. Signal externals such as the operational frequencies, channel spacing, power output and channel usage is documented. Signal modulation(s) is then determined, allowing the investigator to demodulate the captured

signal, and if digital, obtain the data byte stream. Lastly, all attempts are made to derive the protocol used by the device.

Once the protocol and associate message structures are determined and understood, extensive testing and experimentation of protocol behavior is performed to determine if exploitable weaknesses exist. Different devices/technologies have diverse capabilities and features which may be utilized in unexpected ways to cause system errors and communication failures. This is particularly common with low end systems that tend to rely solely on Cyclic Redundancy Check (CRC) as error detection mechanisms.

Vulnerabilities identified at the protocol level facilitate the development of many different types of surgical attacks. These exploitation methods are independent of the corresponding RF channel. Since these messages appear valid to the device, they need not overpower legitimate RF signaling, and thus eliminate the requirement for large Jammer to Signal (J/S) ratios and greatly reducing the required duty cycle time.

2. Hardware Analysis

The hardware analysis phase can be conducted in parallel with signal characterization. A thorough inspection of the internal hardware is performed. All identified integrated circuits are documented and researched for known vulnerabilities. A characterization of the hardware is also performed to determine the device receiver frequency response. Internal signal flows are further characterized by probing at various HW points within the signaling chain. At times, machine code can also be extracted from certain chip sets. If possible, inspection of this code for unchecked boundary or input conditions can lead to very effective exploitation methods. The hardware may also be analyzed for Unintentional Radiated Emissions (URE) that could help in developing techniques for detection purposes.

HW investigation can also aid signal characterization. Recently, difficulties in the capture and recording of a fast frequency hopping waveform from a recovered threat device were overcome by investigating the data flow within the device's HW. This, in turn, revealed an access point to the data communication stream prior to it entering frequency hopping mode thus allowing the capture of the desired waveform without having to capture it via RF.

3. Exploitation

The last Technique Development phase is solely focused on the experimentation, development and testing of attack techniques against the threat device. The first phase of this testing is designed to develop and test techniques that are easily implementable on currently fielded jammers. The second approach to be investigated is to mimic the signaling protocol in such a way that the system accepts simulated messages as if from a legitimate source. This, in turn, allows the protocol itself to be utilized in defeating the target system.

Upon completion of this last technique development phase, all obtained results are fully documented in a technical report that is released to all members of the Techniques Working Group community for validation and potential implementation on a fielded system. To date, several techniques have been transitioned and implemented on fielded systems.

The effective application of enabling technologies in this area is intended to provide the Army with a significant tactical advantage by providing capabilities that mitigate these threats with minimal impact to US systems.

All the considerations above result in the need for interested bidders, under this portion of the Broad Agency Announcement to be invited to submit proposals dealing with the solution of the above technology and operational area of challenge. Examples of pacing technology that this agency is interested in may include (but is not limited to) the following:

- Identify, locate, and counter threat RF networks and nodes in any environment
- Identify, locate, and counter threat wired or cabled networks and nodes in any environment
- Identify, locate, and counter threat optical networks and nodes in any environment
- Capabilities to discriminate threats from non-threats, particularly in a high density environment
- Capabilities to discern *intent* from nodal or traffic analysis, or through other means
- Capabilities to detect, identify, and counter key nodes or routing points
- Protocol recognition capability
- Digital protocol generation capability
- Unique attack algorithms
- Traffic Analysis capabilities
- Information analysis capabilities
- Use of Harmonics
- Unintentional radiation collection and analysis
- Out of band communications
- Communications over non-conventional means
- Penetration of isolated systems

Topic Title: Intelligence, Surveillance, and Reconnaissance Technologies

ISR Sub-Topic #1: Radar Technologies and Techniques

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.

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

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

ISR Sub-topic # 2 – Radar Applications

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.

ISR Sub-topic # 3 – Fusion

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.

ISR Sub-topic # 4 – Modeling and Simulation

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008) reference__

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).

ISR Sub-topic # 5 – Multi-Intelligence Analysts Functions

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.

ISR Sub-topic # 6 – Biometric INTEL Processing

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

ISR Sub-topic # 7 – INTEL & Battle Command Collaboration

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.

ISR Sub-topic # 8 – Collection & Sensor Management

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.

ISR Sub-topic # 9 – Human Terrain (HT) / PMESII Data Exploitation and Analysis

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.

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

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

ISR Sub-topic # 10 – INTEL Exploitation and Analysis

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.

Topic Title: Fusion Methodologies

Fusion Sub-topic # 1 – ISR Exploitation Supporting Fusion

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.

Fusion Sub-topic # 2 – Predictive Analysis and Estimation

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.

Topic title: Command and Control Protect, Network Vulnerability, C4ISR Penetration Testing and Vulnerability Analyses

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 Broad Agency Announcement (BAA).
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.

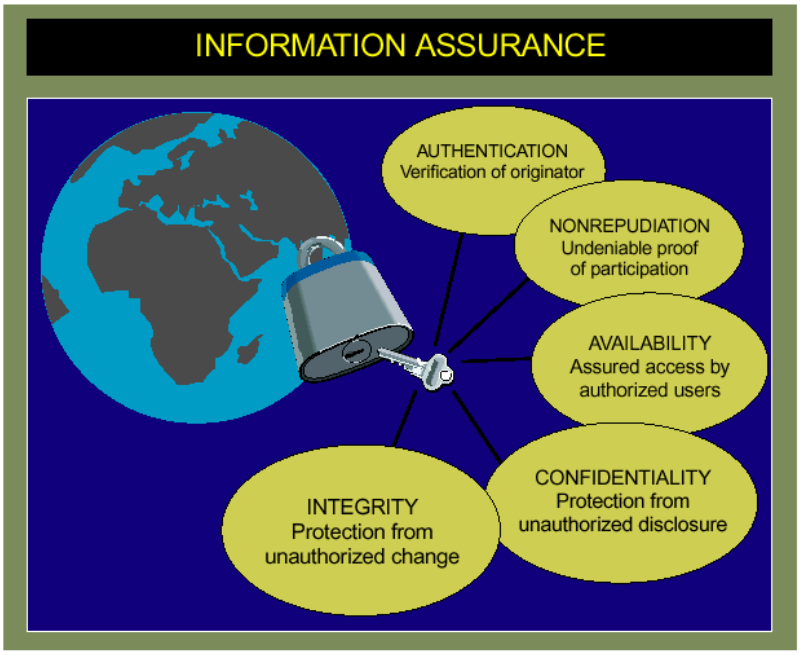
Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

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.

C2 Sub-topic #1 - Blue Attack Blue -- 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.

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Topic Title – Combat Identification

This topic is concerned with providing Combat Identification (CID) capabilities for joint, as well as allied/coalition operations. CID is the capability to detect, discriminate, and identify through active, passive, cooperative or non-cooperative methods. This must be done at ranges in excess of the threat's detection and weapon systems effective ranges and inside the threat's detection and response time. Near real time Identification of Friend or Foe (IFF), and neutral elements, is required. Future combat systems must provide CID of friend, foe, and noncombatant in a joint, allied/coalition environment, through platform-to-platform (manned and unmanned, ground and air), platform-to-soldier, soldier-to-platform, and soldier-to-soldier, under all battlefield and weather conditions, across the spectrum of operations.

CID Sub-topic # 1 – Cooperative Target Identification

Research and development (R&D) in cooperative target identification systems and concepts. The concepts can be in any frequency range for all mission areas or engagement pairs in all mission areas. These areas include ground to ground (both mounted and dismounted), air to ground, and ground to air. Entities to be identified include, but are not limited to, ground vehicles, helicopters, fixed wing, dismounted soldiers, Unmanned Air Vehicles (UAVs), and Unmanned Ground Vehicles (UGVs). Foes, neutrals and noncombatants must also be identified. The emphasis is to provide the CID information at the point of engagement or the point of initiation on an engagement. The CID information is for, but not limited to: ground vehicles, fixed wing aircraft, rotary wing aircraft, dismounted soldiers, Forward Observers, Forward Air Controllers, Fire Support Teams, UAVs, and UGVs. Information is needed for joint operations, as well as operations with coalition partners and Allies. Various Combat ID technologies and concepts to include: millimeter wave (mmW), lasers, Ultra High Frequency (UHF), Very High Frequency (VHF), data fusion and correlation, Tagging Tracking and Locating (TTL) and Radio Frequency (RF) Tags may be explored. Operational covertness, operational robustness in the presence of countermeasures, interoperability with existing systems, and the minimization of cost, size, and weight are key considerations.

CID Sub-topic # 2 – Non-Cooperative Target Identification

R&D in passive or active non-cooperative target identification systems and concepts in any frequency range for all mission area or engagement pairs in all mission areas. Key entities to be identified include, but are not limited to ground vehicles, helicopters, fixed wing aircraft, dismounted soldiers, UAVs, and UGVs. The emphasis is to provide the CID information at the point of engagement and for situational awareness. The CID information is for, but not limited to: ground vehicles, fixed wing aircraft, rotary wing

aircraft, dismounted soldiers, Forward Observers, Forward Air Controllers, Fire Support Teams, UAVs, and UGVs. The various Non Cooperative technologies, such as acoustic, RF, lasers, etc. may be explored. Concepts can include any Non-Cooperative Target Identification (NCTI), Tracking and location (TL) Operational covertness, operational robustness in the presence of countermeasures, interoperability with existing systems, and the minimization of cost, size and weight are key considerations.

TRADOC FOCs

FOC-02-01: Processing, Analysis and Reporting of Intelligence Information

FOC-02-03: The Ability to Collect and Manage Biometric Data

FOC-03-02: Operations in Urban and Complex Terrain

FOC-04-03: Reconnaissance, Surveillance and Target Acquisition (RSTA) and Attack Operations.

FOC-04-05: Mounted Vertical Maneuver

FOC-05-01: LOS/BLOS Lethality

FOC-05-02: NLOS Lethality

FOC-06-06: Understand the Operational Environment

FOC-07-01: Protect Personnel

FOC-09-08: Soldier Support.

FOC-11-01: Human Dimension for the Soldier

Topic Title – Weather Sensor Technologies

Topic is on Research and Development (R&D) in weather sensor technologies for Field Artillery (FA). This topic is concerned with providing the FA weather component in the battlefield with real-time “nowcast” Meteorological (MET) weather data, across the full spectrum of operations. This R&D topic deals with a system(s) integrating various weather data from ground-based and airborne meteorological sensors, with satellite meteorological data to provide weather profiles in space and time. A supporting suite of sensors and data models provide persistent weather updates using various sensors that

may include organic unmanned aerial and ground vehicles along with other intrinsic battlefield system weather data. Sensor studies will support the integration and development of prototype systems. The assimilation of this data will support Command and Control (C2), Situational Awareness (SA) and sensor to shooter applications. Existing systems in this domain may be upgraded. This family of weather systems should be highly mobile, be able to rapidly deploy and have a reduced logistics footprint. Reliability, Availability and Maintainability will be addressed along with accuracy testing. The system may employ and/or utilize a network of weather sensors that can operate independently on manned or unmanned vehicles and with or without soldier intervention. Soldiers will be provided with accurate real-time MET data for computing ballistic equations and may be provided some basic SA (terrain and location) for the gun and/or target areas to better understand the battlespace environment. The system shall fuse the weather sensor information (assimilate various sources into the model) to create accurate information and knowledge about weather for the FA in its Area of Influence. FA MET data is especially critical in Beyond Line of Sight in order for accurate target acquisition (and to minimize friendly force and civilian casualties). The weather intelligence component will support indirect fire systems for non-line of sight lethality dispersed throughout the battlespace and may support a system of systems framework for enabling integrated network fires. These systems will be linked to precision fires (lethal and nonlethal) that will provide rapid response to enemy actions. These systems and technologies will support future system requirements and may include multinational forces.

TRADOC Force Operating Capabilities (FOCs):

FOC-03-01: Command and Control.

FOC-03-03: Advanced Collection, Processing, Analysis, Management and Sharing of Information.

FOC-04-01: Sensor Fusion.

FOC-05-03: Operations in Urban and Complex Terrain.

FOC-06-02: Non-Line of Sight Lethality.

FOC-10-01: Understand the Battlespace Environment.

FOC-11-01: Sustainability.

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Topic title: Unattended Sensors

Introduction:
Surveillance and force protection needs require the use of a layered network of advanced unattended sensors that sense in multiple domains (e.g., radio frequency, thermal, acoustical, electro-optical (EO), infrared (IR), and seismic). These stationary sensors are not to be confused with unmanned vehicles. Once in place unattended sensors should maintain a persistent surveillance from a fixed location. These systems may operate either independently or as components of other systems/platforms.

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008

TRADOC FOC-03-01, Command and Control. Sensors provide persistent surveillance through a series of layers of individual soldier systems, vehicle warning and defensive aids, organic Unmanned Aerial Vehicles (UAVs), Unmanned Ground Sensors and external sensors from the Unit of Employment (UE), Army, theater, national and joint assets.

TRADOC FOC-03-03, Advanced Collection, Processing, Analysis, Management and Sharing of Information. 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, manned/unmanned aerial vehicles, satellites, and even cyber-based platforms.

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

- Research, development, and demonstrations of advanced Unattended Ground Sensor (UGS) Systems. This includes testing of prototype devices and subsystems. These sensors should be able to employ multiple means such as, but not limited to, Acoustics, Seismic, Radio Frequency (RF), Magnetic, and Infrared (IR) simultaneously to detect and classify targets. Sensors should be able to communicate using wireless means to fixed ground stations as well as a variety of platforms that are on the move, including UAVs, fixed and rotary wing assets, and Low Earth Orbit (LEO) Satellites.

- R&D of separate or combined systems for the detection of chemical, biological and ionizing radiation releases into the atmosphere. These sensor systems would be capable of emplacement from fixed wing/rotary wing aircraft. This effort would include the testing and integration of the developed item.

- Tradeoff and other technical analyses to determine optimum combination of operational and performance requirements vs. technical requirements for unattended stationary operation of battlefield sensors. These may include but are not limited to emplacement techniques, extended duration of operation, and integration into Command, Control, Communication, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) network.

Topic title: Unmanned Vehicles

Introduction:
The 21st century army will need to deploy unmanned mobile sensors on the ground, through the air, and in space. Distant objective areas will need to be monitored for a variety of missions. Rapid deployment of unmanned vehicles capable of providing surveillance and reconnaissance will act as a force multiplier. The payloads for these platforms will be modular and readily interchangeable. Vehicles will need to be configurable for deploying a vast array of lethal and nonlethal effects in addition to sensor systems. In deception operations unmanned vehicles will need to confuse enemy forces and draw fire away from friendly forces. Unmanned vehicles will provide greater warfighter standoff during operations in complex and urban terrain.

Requirements: (abbreviated; see TRADOC Pamphlet 525-66, 7 March 2008)

TRADOC FOC-03-01: Command and Control. Sensors that provide persistent surveillance through a series of layers.

TRADOC FOC-03-03: Advanced Collection, Processing, Analysis, Management and Sharing of Information. Sensors that operate independently and in multiple domains or as components of other systems/platforms.

TRADOC FOC-03-04: Network Operations. Capability to draw information from a wide variety of automated and manual sources.

TRADOC FOC-04-01: Sensor Fusion. Provide targeting combat assessment and eyes on target/man-in-the-loop decision capability for all source fires.

TRADOC FOC-05-03: Operations in Urban and Complex Terrain. Assist with reconnaissance over complex terrain and mapping of high-risk areas.

TRADOC FOC-06-01: Non-Line of Sight (NLOS) Lethality. Reconnaissance and surveillance assets must provide acceptable target location accuracy.

TRADOC FOC-08-01: Air/Ground Operations. Conduct detailed reconnaissance to develop and confirm enemy battlefield disposition. Provide communications relays for extended distances or provide NLOS communications connectivity for ground maneuver

forces. Use tailorable, modular mission payloads, providing synergy and extension of capabilities.

TRADOC FOC 13-01: Human Engineering for the Soldier. Provide the ability to avoid/detect hazardous areas that are inherently close quarters in nature, such as operations in urban and complex terrain.

UV Sub-topic # 1 – Unmanned Aerial Vehicles

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

- Remotely piloted or self-piloted aircraft that can carry sensors, communications equipment, or other modular mission payloads
- Surveillance in tactical and endurance category UAVs
- Imagery intelligence
- Wide-area surveillance
- UAVs directly deployable from Continental United States (CONUS) to the theater of operations
- Software and communications links required to control UAVs
- Connectivity to other C4I systems
- Automated flight control and/or autonomous refueling, which could reduce control-related accidents as well as greatly enhancing UAV endurance and range
- Flight enabling technologies for micro and small UAVs
- Flexible and adaptive structures technology to extend the range and reduce maintenance costs for UAVs
- Active flow control technologies to reduce drag on UAVs
- UAV solutions for applicable military roles across the spectrum of warfare to meet validated needs within the specific mission areas based on cost, capability, reliability, and suitability

UV Sub-topic # 2 – Unmanned Ground Vehicles

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

- Perception, intelligent control, and man-machine interface technologies
- Incorporation of mobile-networked Command, Control, Communication, and Computer (C4) functionalities into UGVs
- Line of Sight (LOS) and Beyond Line of Sight (BLOS) fires
- Reconnaissance, Surveillance, and Target Acquisition (RSTA)

- Assured mobility support (obstacle detection and neutralization)
- Communications relay in all terrain settings
- Performance metrics such as endurance, mobility, payload fraction, airdrop-ability, robustness to crash, reliability, signature, and cost of UGVs
- Man-portable, small, lightweight robot system that is highly mobile and capable of being re-configured for various missions (reconnaissance, surveillance, or assault) by adding or removing sensors, modules, mission payloads, and/or subsystems
- Remote investigation of threat obstacles, structures, and the structural integrity of facilities and utilities
- Lightweight day/night sensor suites on a mast/turret system capable of providing remote surveillance images and sensed information
- On-board sensors that will be able to detect and neutralize mines and/or detect Nuclear, Biological, and Chemical (NBC) presence
- Armed reconnaissance, surveillance, and target acquisition missions
- Interoperation with an organization of vehicles, sensors, Command and Control (C2) hardware and software systems, and communications systems
- Navigation systems capable of autonomously controlling any of several UGVs by providing navigational, perception, path-planning, and vehicle-follow algorithms, as well as the requisite on-board sensor package for autonomous mobility

Tradeoff and other technical analyses to determine optimum combination of operational and performance requirements vs. technical requirements for unmanned vehicle operation.

PART IV – PROPOSAL GENERAL INFORMATION

1. In presenting the proposal material, offerors are advised that the quality of the information is significantly more important than the quantity. Therefore, offerors are requested to confine their submission to essential matters providing sufficient information to define their proposal and establish an adequate basis for the Government to conduct its evaluation.

2. Offerors are requested to submit their best proposal the first time since the Government reserves the right to award without discussion. Failure to comply with these instructions may affect the evaluation or delay consideration of the proposal.

3. Offerors are requested to complete and return the Representations and Certifications set forth in the attachments with their proposal.

4. The offeror's cost proposal shall be prepared in a clear and concise manner that accurately reflects the offeror's cost estimate for accomplishing the proposed technical effort. Cost data shall include all costs expected during the performance of the contract. All details, broken down by cost element, shall be prepared for each major task along with supporting rationale. All cost data is subject to Government evaluation and verification.

5. Contracts awarded under this announcement may be incrementally funded as described under Federal Acquisition Regulation (FAR) 52.232-22, "Limitation of Funds". In view of this and to allow the Government adequate time for budgetary planning, offerors shall submit a monthly expenditure profile containing a breakout of projected funding that is commensurate with the proposed level of effort, technical approach, and milestones.

6. Upon completion of negotiations and agreement on contract price, a certificate of current cost and pricing data may be required in accordance with FAR 15.804-2.

7. Representation and Certification shall be completed and returned by the offeror as set forth in the appendices. Also, offerors are required to identify their DUNS number, tax identification number and Commercial and Government Entity (CAGE) Code. If the offeror does not have these codes, the offeror should register at the System for Award Management website: http://www.sam.gov/ but should not delay proposal submission in the interim.

8. A subcontracting plan is required if the amount of the proposal exceeds $500,000 and the offeror is other than a small business concern. The offeror must agree to prepare, submit, and negotiate in order to incorporate into the contract a plan for subcontracting to small and small disadvantaged business for participation in the effort.

9. Offerors are required to include electronic mail address, phone number, and Topic/Sub-Topic Number proposing to in their cover letter to expedite communications for unclassified proposals.

10. Offerors may request Government Furnished Material (GFM) in their proposals. Such requests shall be clearly identified as GFM or contractor acquired property. When possible, the description or title and known or estimated unit and total costs of each item should be shown. When such information is not available, the items should be grouped by class and estimated values indicated. However, the Government is under no obligation to comply with such requests. Therefore, offerors should make provisions for alternate technical approaches and/or cost variances should the Government be unable to furnish requested materiel.

11. As a minimum, all offerors shall submit Contractor's Progress, Status and Management Report and a Final Scientific and Technical Report in accordance with the requirements of DI-MGMT-80227 and DI-MISC-80711A. Offerors may propose commercial format equivalents for the cited data item provided that all the required information is included and the only deliverables under the resulting contract are reports.

12. Depending on the nature and duration of the project or program, the Government may require the contractor to attend project/program reviews at Aberdeen Proving Ground, Maryland. In addition to required formal reviews, informal reviews may be scheduled at the contractor's facility as deemed necessary by Government management and/or technical personnel. For costing purposes, an offeror should plan for a formal project / program review, of one or two day duration approximately every ninety-calendar days following award. The contractor shall host a kick off meeting at the contractor's facility within thirty days following contract award. Depending upon the level of risk involved in a particular project or program, additional informal and formal reviews may be required by the Government. Such notice could take place at any time during the course of the project or program.

13. A demonstration period should be anticipated and estimated costs proposed for those projects/ programs that produce a demonstrable entity. If necessary, the contractor shall submit to the Government a plan for multiple demonstrations at least 120 calendar days prior to the end of the period of performance. The Government shall approve or specify desired modifications to the contractor's demonstration plan no later than sixty days before the first day of the demonstration period. Demonstrations shall capture the essence of the technology advances within the context of a reasonable scenario that accurately represents at least one U.S. Army requirement (see references a through f).

14. The system design approach shall comply with the applicable portions of the Joint Technical Architecture-Army. Any proposed technical designs that deviate from the standards and practices delineated in the joint Technical Architecture-Army, either

during the evaluation and / or subsequent execution of this contract, shall be approved by the Army Digitization Office (ADO), through the Program / Project Manager, prior to implementation.

15. Intellectual Property.

It is the Government's intention at a minimum to obtain Government Purpose Rights for any HW/SW developed/delivered or data generated as a result of a contract awarded under this BAA. Offerors are encouraged to propose software solutions that are open architecture (API's, etc.) based without restrictions such as intellectual property rights.

a. Noncommercial Items (Technical Data and Computer Software)

Offerors shall deliver all software developed under this effort, including but not limited to waveform code, VHDL code, Modeling and Simulation Basis, and Test Software, including both source and executable codes.

Offerors responding to this BAA requesting a procurement contract to be issued under the FAR/DFARS, shall identify all noncommercial technical data, and noncommercial computer software that it plans to generate, develop, and/or deliver under any proposed award instrument in which the Government will acquire less than unlimited rights, and to assert specific restrictions on those deliverables. Offerors shall follow the format under DFARS 252.227-7017 for this stated purpose. In the event that Offerors do not submit the list, the Government will assume that it automatically has "unlimited rights" to all noncommercial technical data and noncommercial computer software generated, developed, and/or delivered under any award instrument, unless it is substantiated that development of the noncommercial technical data and noncommercial computer software occurred with mixed funding. If mixed funding is anticipated in the development of noncommercial technical data, and noncommercial computer software generated, developed, and/or delivered under any award instrument, then Offerors should identify the data and software in question, as subject to Government Purpose Rights (GPR). In accordance with DFARS 252.227-7013 Rights in Technical Data - Noncommercial Items, and DFARS 252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation, the Government will automatically assume that any such GPR restriction is limited to a period of five years in accordance with the applicable DFARS clauses, at which time the Government will acquire "unlimited rights" unless the parties agree otherwise. Offerors are admonished that the Government will use the list during the source selection evaluation process to evaluate the impact of any identified restrictions, and may request additional information from the Offeror, as may be necessary, to evaluate the Offeror's assertions. If no restrictions are intended, then the Offeror should state "NONE."

A sample list for complying with this request is as follows:

NONCOMMERCIAL			
Technical Data Computer Software To be Furnished With Restrictions	Basis for Assertion	Asserted Rights Category	Name of Person Asserting Restrictions
(LIST)	(LIST)	(LIST)	(LIST)

b. Commercial Items (Technical Data and Computer Software)

Offerors responding to this BAA requesting a procurement contract to be issued under the FAR/DFARS shall identify all commercial technical data and commercial computer software that may be embedded in any noncommercial deliverables contemplated under the research effort, along with any applicable restrictions on the Government's use of such commercial technical data and/or commercial computer software. In the event that Offerors do not submit the list, the Government will assume that there are no restrictions on the Government's use of such commercial items. The Government may use the list during the source selection evaluation process to evaluate the impact of any identified restrictions, and may request additional information from the Offeror, as may be necessary, to evaluate the Offeror's assertions. If no restrictions are intended, then the Offeror should state "NONE."

A sample list for complying with this request is as follows:

COMMERCIAL			
Technical Data Computer Software To be Furnished With Restrictions	Basis for Assertion	Asserted Rights Category	Name of Person Asserting Restrictions
(LIST)	(LIST)	(LIST)	(LIST)

c. Intellectual Property Representations

Offerors are required to provide a good faith representation that it either owns or possesses appropriate licensing rights to all other intellectual property that will be utilized under its proposal. Additionally, offerors shall provide a short summary for each item asserted with less than unlimited rights that describes the nature of the restriction and the intended use of the intellectual property in the conduct of the proposed research.

PART V – PROPOSAL PREPARATION AND SUBMISSION

1. Eligibility

The Government shall consider research proposals from:

- offerors interested in conducting scientific research
- colleges and universities
- nonprofit research institutes
- commercial firms
- small businesses
- small disadvantaged business concerns
- historically black colleges
- universities
- minority owned business enterprises and institutions
- Canadian firms participating in DDSP

To be eligible for award of a contract, a prospective offeror must meet certain minimum standards pertaining to financial resources, ability to comply with the performance schedule, prior records of performance, integrity, organization, experience, operational controls, technical skills, facilities, and equipment. For additional information and guidance concerning qualifications and standards of responsibility for prospective contractors please refer to Part 9 of the FAR.

Research and development contracts awarded from this BAA will be primarily Cost Plus Fixed Fee as it is not expected that the scope of the contract will be sufficiently defined to allow for a firm fixed price contract. Potential offerors should be aware that in accordance with FAR 16.301-3(a), a cost-reimbursement contract may only be used when the contractor's accounting system is adequate for determining costs applicable to the contract.

There are certain post-employment restrictions on former federal officers and employees, including special Government employees, (section 207 of title 18, United States Code). If a prospective offeror believes a conflict of interest exists, the contracting officer should be consulted prior to expending time and effort in preparing a proposal. Foreign and foreign owned firms should be aware that restrictions may apply that could preclude participation in some areas of interest.

2. Contents

NOTICE: The only acceptable file format for soft copy proposals is Adobe® Portable Document Format (PDF). Offerors should indicate whether or not the proposed effort is the subject of ongoing Independent Research and Development (IR&D) efforts and submit their Independent Research and Development (IR&D) projects to the following Federal Register website: http://www.defenseinnovationmarketplace.mil/industry.html. Instructions for submitting the IR&D project are located at: http://www.defenseinnovationmarketplace.mil/resources/ProjectDataEntryInstructions.pdf. Proposals submitted should be based on the information contained in this BAA; no additional written information will be available. Offerors are requested to limit their technical proposals to no more than 100 pages total, consisting of two volumes: Volume I as described below shall contain the offeror's technical approach and management plan; Volume II, as described later in this section, shall contain the cost portions of the proposal. All proprietary data must bear the appropriate restrictive legend and are subject to protection by the contractor. Proposals may be submitted for classified work. Any classified materials must be identified as such, and marked and packaged in accordance with the Industrial Security Manual. SECRET, TOP SECRET clearances and / or special access may be required. Brochures are discouraged and other elaborate presentations, beyond that needed to present a complete and effective response to this solicitation, are undesirable.

3. Technical and Management

At a minimum, shall contain the following:

a. On the organization's letterhead stationary --

1) Legal name and address of the submitting organization
2) Type of organization and place of performance
3) Original signatures of principal investigator or project director and an official authorized to legally bind the organization
4) Brief but descriptive title of the proposed research, citing the Research Area of Interest
5) Period of performance and estimated cost

b. A brief abstract of the proposed effort.

c. Submit a detailed description of the research to be undertaken, objectives, approach, methods, and its relationship to the state of knowledge in the field and to comparable work in progress elsewhere, together with a bibliography and a list of pertinent literature citations. The inclusion of active hyperlinks to unclassified World Wide Web or classified TOP SECRET Joint Worldwide Intelligence Communications System (JWICS)/ IntelLink references is highly encouraged. The following general

outline shall be followed to satisfy minimum requirements. Offerors may add to this minimum outline --

1) Type of project (e.g., pilot or feasibility study, definitive study, survey). Include a summary of the proposed statement of work as well as accomplishment milestones;
2) Technical objective for each twelve-month or shorter period (state concisely the problem to be addressed by each intermediate research objective);
3) Hypothesis (state the hypothesis to be tested, and expectations and utilization of resulting data);
4) Background (provide a brief statement of ideas and reasoning behind proposed study and describe briefly the previous experience most pertinent to this proposal; provide relevant references);
5) Methods (give details on the experimental design and methodology. If the methodology is new or unusual, describe it in detail for evaluation).

d. Personnel: A resume, pertinent to the proposed effort, should be included for the principal investigator and other key personnel. If the principal investigator and/or other key personnel sever connection with the organization or become unable to continue active participation, the Government must be notified in advance and a resume for the replacement individual provided. The Government has the option to terminate the contract in such cases. State any planned consultant fee, including the number of hours and travel expenses, the nature of the consulting effort and why consultants are required to complete the effort.

e. Facilities and Equipment: Describe the facilities and equipment available for performance of the proposed effort and any Government furnished and/or loaned equipment expected.

f. Management Plan: Describe the management plan for accomplishing the effort including a schedule citing major milestones, review dates, and deliverable items.

4. Cost

The cost proposal should include the following elements for the proposed effort:

a. **Direct Labor:** Provide and describe labor categories, the number of work-hours required within each category, and verifiable current and projected hourly rates for each labor category and totals for the entire performance period.

b. **Material:** Itemized list of material requirements for the effort based on recent supplier/manufacturer's quote. Unless otherwise specified, all materials purchased for performance of the effort are to be delivered to the Government upon completion/termination of the contract.

c. **Travel:** For each trip anticipated provide an estimated schedule, a destination and purpose for the travel, an estimated round trip fare, per diem costs, and local travel requirements. Include Other Direct Costs which are Costs associated with things such as laboratory usage, computer usage, and reproduction.

d. **Cost for Consultant:** State any planned consultant fee, including the number of hours and travel expenses, the nature of the consulting effort and why consultants are required to complete the effort.

e. **Cost for Publication and Report:** Estimate the cost of publishing and reporting research results. Include clerical preparation, illustration charges and distribution. Vendor quotes are encouraged.

f. **Cost for Subcontractors:** A breakdown of the subcontract amount by cost element and fee must be shown to fully evaluate the proposal.

g. **Indirect Labor Costs:** Overhead and general administrative rates. Indirect cost shall indicate the rates used are fixed or provisional. Also, indicate the time frames to which the rates are applicable.

h. **Fee:** Proposed fee for cost-plus type contracts shall not exceed the statutory limitations imposed by 10 United States Code (U.S.C.) 2306(d).

i. **Funding Profile:** Since contracts awarded under this BAA may be incrementally funded, the offeror shall submit a monthly expenditure profile containing a breakout of projected funding that is commensurate with the proposed level of effort, technical approach, and milestones.

5. Submission

For UNCLASSIFIED proposal submission: One electronic copy of each Proposal volume or White Paper shall be submitted to the following group mailbox: usarmy.APG.cerdec.list.i2wd-iwo-ac-gov@mail.mil

- For proposal submission for other than UNCLASSIFIED, ie, SECRET, TOP SECRET shall be marked with an appropriate SCI caveat, if one applies, appropriately wrapped, and delivered in hard copy (one each) to the following address:

U.S. Army Research, Development and Engineering Command
Communications and Electronics, Research, Development and Engineering Center
Intelligence and Information Warfare Directorate
ATTN: RDER-IWO-OP (Security)
Building 6003

Combat Drive
Aberdeen Proving Ground, MD 21005

6. Government Evaluation

It is the policy of the I2WD to treat all research proposals as privileged information before award and to disclose the contents to Government personnel only for purposes of evaluation. Highly qualified Government subject matter experts, engineers and scientists shall evaluate each proposal, on its own merit, according to the factors cited in the following section of this BAA. All evaluators are made aware that without written permission from the offeror the proposals sent to them shall not be duplicated, used, or disclosed in whole or part for any purpose other than to evaluate the proposal. If a contract is awarded on the basis of the proposal submitted under this BAA, the negotiated terms of the contract control disclosure and use of the proposal.

Proposals, including technical/management and cost volumes, and completed Representation & Certification, submitted in response to this BAA shall be evaluated as they are received throughout the duration of this solicitation. Proposals lacking scientific merit or relevance to Army's needs, or those proposals that may fall in areas wherein funds are not expected to be available, may be rejected without further action.

Multiple or no awards may be made periodically for each sub topic of the BAA at the sole discretion of the Government; each proposal received will be evaluated on its own merit without comparison to other proposals.

7. Assessment Categories

The Government shall evaluate each proposal received in response to this BAA according to the following factors:

a. **Scientific and Technical Quality:** The scientific and technical quality of the research proposal and its relevance to the area of interest addressed, with special emphasis on its innovation and originality.

b. **Offeror's Qualifications:** The offeror's capabilities, related experience, facilities, techniques, or unique combinations of these, are integral factors in achieving the proposed objectives.

c. **Key Personnel Qualifications:** The qualifications, capabilities, and experience of the proposed Principal Investigator, and key personnel who are critical in achieving the proposed objectives shall be described in detail.

d. **Cost:** The reasonableness and realism of proposed costs and fee/profit, if applicable.

Information relating to the first three categories shall be addressed in Volume I, Technical. All Cost information shall be addressed in Volume II, Cost.

References

a) U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-66, *Military Operations Force Operating Capability* (FOC), http://www.tradoc.army.mil/tpubs/pams/p525-66.pdf., dated 7 March 2008.

b) Joint Publication 3-13, *Joint Doctrine for Information Operations*, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, dated 20 November 2014.

c) Joint Publication 3-13.1, *Joint Doctrine for Electronic Warfare*, http://www.dtic.mil/dtic/tr/fulltext/u2/a562410.pdf., dated 07 February 2012

d) European Co-Ordination Action for Agent-Based Computing

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Glossary of Terms

Term	Meaning within this solicitation
ADA	Air Defense Artillery
ADC	Analog to Digital Converter
ADO	Army Digitization Office
Adversary	Threat
AO	Area of Operations
AOA	Angle of Arrival
ASE	Aircraft Survivability Equipment
ASTMP	Army's Science and Technology Master Plan
ATDS	Advanced Technology Development
ATGM	Anti-Tank Guided Missile
ATR	Automatic Target Recognition
AWE	Advanced Warfighting Experiments
BAA	Broad Agency Announcement
BLOS	Beyond Line of Sight
C2	Command and Control
C2W	Command and Control Warfare; part of IO;
C4	Command, Control, Communication, Computer
C4I	Command, Control, Communications, Computers and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAGE	Commercial and Government Entity
CBRN	Chemical, Biological, Radiological and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear and Biological
CDMA	Code Division Multiple Access
CERDEC	Communications, Electronics, Research, Development and Engineering Center
CI	Counterintelligence
CID	Combat Identification
CL	Current Load
CNA	Computer Network Attack; part of CNO
CND	Computer Network Defense; part of CNO
CNE	Computer Network Exploitation; part of CNO
CNO	Computer Network Operations (CND+CNE+CNA)
COMINT	Communications Intelligence, part of SIGINT
CONUS	Continental United States
COP	Common Operating Picture
COTS	Commercial Off-the-Shelf
Counter C4ISR	C4ISR Exploitation and Attack
CROP	Common Relevant Operating Procedure
D/A	Digital-to-Analog
DARPA	Defense Advanced Research Projects Agency

Title: BAA I2WD 2014
Formally Solicitation Number: W56KGU-14-R-0003
New Solicitation Number: W56KGU-16-R-A330

Term	Meaning within this solicitation
DBF	Digital Beamforming
DCGS-A	Distributed Common Ground System-Army
DDS	Direct Digital Synthesis
DDSP	Defense Development Sharing Program
DE	Directed Energy
DF	Direction Finding
DIA	Defense Intelligence Agency
DIS	Distributed Interactive Simulation
DoD	Department of Defense
DoS	Denial of Service
DRFM	Digital RF Memory
DSP	Digital Signal Processor
EA	Electronic Attack; Part of EW
ECCM	Electronic Counter-Countermeasures
ECM	Electronic Countermeasure (old doctrinal term – now EA)
ELINT	Electronic Intelligence; part of SIGINT
EM	Electromagnetic Modeling
EO	Electro-optics
EP	Electronic Protection
EPLRS	Enhanced Position Location Reporting System
ES	Electronic Support; part of EW
ESM	Electronic Support Measure (old doctrinal term – now ES)
EW	Electronic Warfare; part of C2W;
FAR	Federal Acquisition Regulation
FAX	Facsimile
FCS	Future Combat Systems
FDOA	Frequency Difference of Arrival
FF	Future Force
FLT	Foreign Language Translation
FOC	Force Operating Capability
FOS	Family of Systems
FP	Failure Potential
FPGA	Field Programmable Gate Array
GFP	Government Furnished Property
GHz	Gigahertz (thousands of MHz)
GOTS	Government Off-the-Shelf
GRCS	Guardrail Common Sensor
GSE	Ground Vehicle Survivability Equipment
GSPS	Giga-samples per Second
GUI	Graphical User Interface
HEMT	High Election Mobility Translator
HF-DF	High Frequency-Direction Finding

Term	Meaning within this solicitation
HF/VHF	High Frequency/Very High Frequency
HLA	High Level Architecture
HTI	Horizontal Technology Integration
HTSC	High Temperature Superconductors
HUMINT	Human Intelligence
I2WD	Intelligence and Information Warfare Directorate; part of CERDEC and RDECOM
IA	Information Assurance
IF	Information Fusion
IFF	Identification of Friend or Foe
ID	Identification
IDS	Intrusion Detection System
INFOSYS	Information Systems
INTEL	Intelligence
IMEDS	Integrated Modular Electronic Deception System
IMINT	Imagery Intelligence
INSCOM	U.S. Army Intelligence and Security Command
IntelLink	Intelligence Network – TS (part of TS JWICS)
IR&D	Independent Research and Development
IR	Infrared
IRCM	Infrared Countermeasure
ISA	Intelligent Software Agent, a.k.a. dynamic objects, knowbots, or knowledge agents
ISR	Intelligence, Surveillance and Reconnaissance
IW	Information Warfare; part of IO
JFC	Joint Force Commander
JWICS	Joint Worldwide Intelligence Communications System
LADAR	Laser Detection and ranging- commonly referred to as LIDAR
LCLO	Low Cost, Low Observable
LEO	Low Earth Orbit
LIDAR	Light Detection and Ranging- also referred to as LADAR
LOS	Line of Sight
LPE	Low Probability of Exploitation
LPI	Low Probability of Intercept
M&S	Modeling and simulation; models and simulations
MASINT	Measurement and signature intelligence
MHz	Megahertz
mmW	Millimeter Wave
MOUT	Military Operations in Urban Terrain
MS	Maneuver Support
MULTI-INT	Multi Intelligence
NBC	Nuclear, Biological and Chemical
NCTI	Non-cooperative Target Identification

Term	Meaning within this solicitation
NDI	Non-developmental Item
NGO	Non Governmental Organization
NLOS	Non Line of Sight
OCONUS	Outside the Continental United States
PBXs	Private Branch Exchange (private telephone switchboard)
PCS	Personal Communication Systems
.pdf	Adobe® Portable Document Format
PDW	Pulse Description Words
PEO	Program Executive Officer
PL	Public Law
PM	Program Manager
POC	Point of Contact
PRI	Pulse Repetition Interval
PSYOP	Psychological Operations
QPSK	Quadrative Phase-Key Shifting
R&D	Research and development
RADAR	Radio Detecting and Ranging
RCM	RADAR Countermeasure
RDTE	Research, Development, Test and Evaluation
RFINT	Radio Frequency Intelligence
RDECOM	Research Development and Engineering Command; part of CERDEC
RF	Radio Frequency
RF/IF	Radio Frequency/Intermediate Frequency
RFI	Radio Frequency Interference
RPGs	Rocket Propelled Grenades
RPV	Remotely Piloted Vehicle
RSTA	Reconnaissance, Surveillance and Target Acquisition
RWA	Rotary Wing Aircraft
SA	Situational Awareness
SAR	Synthetic Aperture RADAR
SEI	Specific Emitter Identification
SIGINT	Signals Intelligence
SINCGARS	Single-Channel Ground and Airborne Radio System
SIO	Special Information Operations
SITREP	Situation Report
SME	Subject Matter Expert
SSBA	Social Science Research and Analysis
STTW	Sense Through the Wall
SU	Situational Understanding
SUGV	Small Unattended Ground Vehicles
SWaP	Size, Weight and Power

Term	**Meaning within this solicitation**
TDMA	Time Division Multiple Access
TDOA	Time Difference of Arrival
TOC	Tactical Operations Center
TPOC	Technical Point of Contact
TRADOC	U.S. Army Training and Doctrine Command
TTP	Tactics, Techniques and Procedure
UA	Unit of Action
UAV	Unmanned Aerial Vehicle
UE	Unit of Employment
UGS	Unattended Grounds Sensors
UGVs	Unmanned Ground Vehicles
UHF	Ultra-High Frequency
UMOP	Unintentional Modulation on Pulse
U.S.C.	United States Code
UV	Unmanned Vehicles
VHF	Very High Frequency
VLSI	Very Large-Scale Integration
VME	Versa Module Eurocard
Vp	Vantage Point to the Target
VPN	Virtual Private Network
VSWR	Voltage Standing Wave Ratio

Appendix A – Representation, Certification, and Other Statements of the Offeror

1. The checklist stated in FAR 52.219-1 Small Business Program Representations (Oct 2014) shall be completed by offerors, and submitted as part of their proposal:

2. Certification As To Other Agency Funding.

Provide the names of any other federal, state, local agencies or other parties receiving the proposal and/or funding the proposed effort or activity.

( ) The proposal has not been submitted to any agency except the US Army Communications Electronics Command, Research Development and Engineering Center,(CERDEC) nor is the proposal presently being funded by another source.

( ) The proposal has been submitted to the following sources:

Name	Status of Proposal
_____	_____
_____	_____

f. CAGE Code: _____.

TIN: _____.

DUNS Number: _____.

Point of Contact(s) and Phone Number(s):

3. Additional Representations and Certifications which may be required by appreciable procurement regulations will be provided to the offerors selected for contract award, to be executed prior to such award.