TABLE OF CONTENTS

I. OVERVIEW OF THE FUNDING OPPORTUNITY

A. REQUIRED OVERVIEW CONTENT
1. **FEDERAL AGENCY NAME**
2. **RESEARCH OPPORTUNITY TITLE**
3. **ANNOUNCEMENT TYPE**
4. **RESEARCH OPPORTUNITY NUMBER**
5. **CATALOG OF FEDERAL DOMESTIC ASSISTANCE (CFDA) NUMBER AND TITLE**
6. **RESPONSE DATES**

B. ADDITIONAL OVERVIEW INFORMATION

II. DETAILED INFORMATION ABOUT THE FUNDING OPPORTUNITY

A. PROGRAM DESCRIPTION
1. **ARL INTERNET OF BATTLEFIELD THINGS VISION**
2. **ARL INTERNAL MISSION AND RELATED PROGRAMS**
3. **CRA PROGRAMMATIC STRATEGY**
4. **CRA RESEARCH STRATEGY**
5. **COLLABORATION**
6. **MANAGEMENT**
7. **FUNDING**

B. AWARD INFORMATION

C. ELIGIBILITY INFORMATION
1. **ELIGIBLE APPLICANTS**
2. **COST SHARING OR MATCHING**

D. APPLICATION AND SUBMISSION INFORMATION
1. **ADDRESS TO REQUEST APPLICATION PACKAGE**
2. **CONTENT AND FORMAT OF APPLICATION SUBMISSION**
3. **SUBMISSION DATES AND TIMES**
4. **INTERGOVERNMENTAL REVIEW – NOT APPLICABLE**
5. **FUNDING RESTRICTIONS**
6. **OTHER SUBMISSION REQUIREMENTS**

E. APPLICATION REVIEW INFORMATION
1. **EVALUATION CRITERIA**
2. **REVIEW AND SELECTION PROCESS**
3. **RECIPIENT QUALIFICATION**

F. AWARD ADMINISTRATION INFORMATION

1. **AWARD NOTICES**
2. **ADMINISTRATIVE AND NATIONAL POLICY REQUIREMENTS**
3. **REPORTING**

G. AGENCY CONTACTS

I. OVERVIEW OF THE FUNDING OPPORTUNITY

A. REQUIRED OVERVIEW CONTENT

1. **Federal Agency Name:** U.S. Army Research Laboratory, 2800 Powder Mill Road, Adelphi, MD 20783-1197

   Issuing Acquisition Office: U.S. Army Contracting Command – Aberdeen Proving Ground, Research Triangle Park (RTP) Division, 800 Park Office Drive, Suite #4229, Research Triangle Park, NC 27709

2. **Research Opportunity Title:** Internet of Battlefield Things (IoBT) Collaborative Research Alliance (CRA)

3. **Announcement Type:** Initial

4. **Research Opportunity Number:** W911NF-17-S-0005

5. **Catalog of Federal Domestic Assistance (CFDA) Number(s):** 12.630 - "Basic, Applied, and Advanced Research in Science and Engineering"

6. **Response Dates:** The following is a summary of the events and dates associated with the IoBT CRA Program Announcement (PA):

EVENT	ESTIMATED DATE/TIMEFRAME
PA released	3 March 2017
Opportunities Conference	27 March 2017
Deadline for Questions on PA	24 April 2017
Whitepapers due	8 May 2017
Whitepaper Feedback/Invitation to Submit Proposal	Early June 2017
Proposals due	27 July 2017
Award	September 2017

B. ADDITIONAL OVERVIEW INFORMATION

Purpose: The ability of the Army to understand, predict, adapt, and exploit the vast array of internetworked things that will be present of the future battlefield is critical to maintaining and increasing its competitive advantage. The explosive growth of technologies in the commercial sector that exploits the convergence of cloud computing, ubiquitous mobile communications, networks of data-gathering sensors, and artificial intelligence presents an imposing challenge for the Army. These Internet of Things (IoT) technologies will give our enemies ever increasing capabilities that must be countered, but commercial developments do not address the unique challenges that the Army will face in using them.

The U.S. Army Research Laboratory (ARL) has established an Enterprise approach to address the challenges resulting from the Internet of Battlefield Things (IoBT) that couples multi-disciplinary internal research with extramural research and collaborative ventures. ARL intends to establish a new collaborative venture (the IoBT CRA) that seeks to develop the foundations of IoBT in the context of future Army operations. The Collaborative Research Alliance (CRA) will consist of private sector and government researchers working jointly to solve complex problems. The overall objective is to develop the fundamental understanding of dynamically-composable, adaptive, goal-driven IoBTs to enable predictive analytics for intelligent command and control and battlefield services.

For the purposes of this CRA, an Internet of Battlefield Things (IoBT) can be summarized as a set of interdependent and interconnected entities (e.g. sensors, small actuators, control components, networks, information sources, etc.) or "things" that are: dynamically composed to meet multiple mission goals; capable of adapting to acquire and analyze data necessary to predict behaviors/activities, and effectuate the physical environment; self-aware, continuously learning, autonomous, and autonomic, where the things interact with networks, humans, and the environment in order to enable predictive decision augmentation that delivers intelligent command and control and battlefield services.

The IoBT is the realization of pervasive computing, communication, and sensing where everything will be a sensor and potentially a processor (i.e. increased number of heterogeneous devices, connectivity, and communication) where subsequent information is of a scale unseen before. The battlespace itself will consist of active red (enemy), blue (friendly), and gray (non-participant) resources, where deception will be the norm, the environment (e.g. megacities and rural) will be dynamic, and ownership and other boundaries will be diverse and transient. These IoBT characteristics all translate into increased complexity for the warfighter, requiring situation-adaptive responses, selective collection/processing and real time sensemaking over massive heterogeneous data.

To achieve the CRA's vision a different research approach is imperative. Current research structures for the commercial the Internet of Things allow research to proceed independently along commercial/industrial stovepipes. This partitioning of scientific contributions will not address the complexity of Army problems. The IoBT CRA is expected to foster a new way of conducting collaborative research that breaks down

research barriers, builds new collaborative relationships, and develops mutual understanding across organizations, technical and scientific disciplines, and Research Areas. ARL strongly believes that a joint collaborative approach by a multidisciplinary researcher team is required to make fundamental advances towards meeting the CRA research objectives and overall vision.

ARL has identified three interrelated aspects or Research Areas specific to the IoBT CRA vision that when jointly studied will advance the theoretical foundations of IoBT phenomena. In addition, advancing the theoretical foundations that impact the challenges of these three Research Areas (RAs) requires trans-disciplinary research that takes into account the adversarial and security concerns of the Cyber-Physical IoBT. This Cross-Cutting Research Issue (CCRI) addressing Cyber-Physical Security must be studied jointly in the context and constraints of the three identified Research Areas. The three Research Areas and Cross Cutting Research Issue are defined as follows:

- **Discovery, Composition and Adaptation of Goal-Driven Heterogeneous IoBTs**: Novel mathematical theories and scientific insights leading to scalable composition and management of heterogeneous IoBTs enabling secure information sharing to meet multiple dynamic mission goals.
- **Autonomic IoBTs to Enable Intelligent Services**: Theoretical foundations, models, and methods of autonomic complex systems that deliver adaptive cyber-physical capabilities and services necessary to enable effective command and control across military (blue), adversary (red), and civilian (gray) domains.
- **Distributed Asynchronous Processing and Analytics of Things**: Scientific principles, theories, and methods and enable predictive processing, analytics, and anomaly detection of broadly heterogeneous and varied data, that may be unknown combinations of sparse and voluminous; centralized and distributed; and trusted and suspect for the purposes of augmenting goal-driven decision-making.
- **Cyber-Physical Security**: Theoretical and pragmatic cross-cutting methods that address the challenges of the above research areas, while enriching the resiliency of the IoBT, such that it can be hardened against tampering and adversarial compromise, continue operating under attacks, and provide bounded guarantees of performance.

A foundational problem to be addressed by the RAs and CCRI is the fundamental understanding of how to learn and devise complex models of IoBT goals, networks, information, and analytics that enable intelligent command and control, and battlefield services. A critical issue embedded throughout all aspects of IoBTs is cyber physical security, as the Army will need to use things it does not control (e.g. adversarial and open/allies' resources), accommodate deceptive data, and counter advanced persistent threats. Joint research in the RAs and CCRI should lead to deep, persistent, and meaningful collaboration among the Alliance and should synchronize definitions, ontologies, metrics, representations, and processes to build understanding of how to learn and devise complex

models of IoBT mission-goals, networks, information, and analytics to enable intelligent command and control and battlefield services.

The proposed research should develop appropriate mathematical representations, models, methods, and analysis techniques. Expected outcomes are principled theories and fundamental methods that lead to greater utility, efficiency, and control of the IoBT. Validation of theories and models through principled experimentation should be a critical aspect of the proposed research. While theoretical and fundamental research prosed effort should retain focus on accomplishing IoBT mission-goals as well as simplifying the complexity of IoBT command and control, while minimizing negative impacts on Army operations.

The CRA is intended to foster collaborative basic research (Budget Activity 1 - see definition below) involving the Consortium and the Government. ARL's strategy is to continue exploiting research and expertise where it exists through the issuance of a single award through this Program Announcement. Collaboration between the Consortium and the Government is integral to the execution and success of the CRA. It is ARL's strong belief that work conducted under the IoBT CRA cannot be successful, either in whole or in part, without collaboration. That is, collaboration among the members of the Consortium and the Government Members of the Alliance is integral to the execution of the research program and achieve the IoBT CRA vision.

Award Instrument: This PA is expected to result in the award of a cooperative agreement (CA) as defined at 31 U.S.C. 6305 for the execution of the program. The CA will be awarded to a Consortium of organizations that may include institutions of higher education, and industrial and non-profit organizations.

The Consortium must be led by an institution of higher education charged with spearheading the focused basic research program. This organization will be designated as the Lead Research Organization (LRO). Each Research Area will be led by a different Lead Research Area Organization (LRAO), one of which could also be the LRO. The same entity cannot be the LRAO for more than one Research Area. Together the LRO and LRAOs make up the Consortium, who are responsible for shaping and steering the CRA through collaboration, with ARL. Performance under the CA may also include other organizations as subawardees to the LRO. To assure the creation of a well-focused research program, the number of partners should balance the need for expertise in all three Research Areas and the Cross Cutting Research Issue with the need to maintain a focused, cohesive, well-integrated research program.

Proposal Submission: The application process (see **PART II.D)** consists of a Whitepaper stage and a Proposal stage. The purpose of requesting Whitepapers is to minimize the effort associated with the production of detailed proposals for those Applicants that have little chance of being selected for funding. The Government's decision to invite a Proposal will be based upon the evaluation results of the Whitepaper submission. Only the most highly rated Whitepapers will receive an invitation from the Government to submit a Proposal. **Applicants that do NOT receive invitations from the Government to submit a Proposal are NOT eligible to submit Proposals and will NOT receive feedback or a**

"debriefing" on their Whitepaper. Applicants invited to submit Proposals will receive feedback on their Whitepapers in order to improve their Proposal submissions. **If an Applicant has NOT submitted a Whitepaper, they may NOT submit a Proposal for consideration for funding.** Applicants should note that there are page limitations and other requirements associated with the submission process for both the Whitepaper and the Proposal. Submissions in connection with this PA are due by the date and time specified in **PART II.D.3.**

Period of Performance: The Award made as a result of this PA will provide for a period of performance of five years, with an optional five-year extension period.

Place of Performance: There is no limitation on the place of performance for any organization participating under the CA.

Funding: This PA is issued subject to the availability of funds. ARL has submitted the requisite documents to request funding for the period covered by the CA. However, Applicants are reminded that this request is subject to Presidential, Congressional and Departmental approval. The PA provides the estimated funding levels for the Basic Research (6.1) for the IoBT CRA. **The funding levels provided in the PA are for Whitepaper and Proposal preparation purposes only. The actual funding level of the CA will be updated annually as part of the appropriation process.** Further, this PA identifies additional levels of funding to potentially enhance the research program with additional basic and applied research funds. It is expected that during performance there will be opportunities to secure this additional funding from ARL or other Government agencies to enhance the core basic research program.

Profit/Fee: In accordance with 32 Code Federal Regulations (CFR) §22.205, profit/fee is not permitted under the CA.

Cost Sharing: Cost sharing is not required under this PA. During the evaluation of proposals, any cost sharing will be evaluated as it relates to the evaluation factors listed in the PA, based on the degree to which the proposed cost sharing enhances the proposal to result in added benefits to the IoBT CRA. To allow for evaluation of a proposed cost sharing, a proposal should express a firm commitment to provide such cost share and evidence a process for integrating the cost share into the collaborative research program.

Evaluation and Award: Evaluation and Award in connection with this PA will be performed in accordance with **PART II.E.** Whitepapers and Proposals that are in compliance with the requirements of the PA will be evaluated in accordance with merit based, competitive procedures. These procedures will include evaluation factors and an adjectival and color rating system. A Review Team, consisting of a qualified group of scientists, managers and business specialists, will evaluate both the Whitepapers and Proposals and provide the results of that evaluation to the decision maker for the Government. The decision maker will make both the decisions concerning the Whitepaper down selection and award selection.

Opportunity Day: An Opportunity Day meeting will be held to discuss this PA and to encourage dialogue, interchange and teaming related to responding to the PA. The meeting will be held at the US Army Research Laboratory, Adelphi, MD on Monday, 27 March, 2017. While attendance is strongly encouraged, attendance at this meeting is not a requirement for submission of a Whitepaper or Proposal in connection with the IoBT CRA Program. Registration details can be found on the IoBT CRA Program website at www.arl.army.mil/cra/IoBT/. The presentations from this meeting, the list of attendees, and the non-proprietary questions posed and answers provided will be made available on the above mentioned website for the benefit of all interested parties. Information presented, written or oral, during the Opportunity Day meeting will not change this PA. Any changes to this PA will be issued via an amended PA being posted in grants.gov.

Contact Information. Outside of questions posed at the Opportunity Day, all questions or comments concerning this PA shall be submitted to the Government through the IoBT CRA Program website at www.arl.army.mil/cra/IoBT/. Comments or questions submitted should be concise and to the point, eliminating any unnecessary verbiage. In addition, the relevant part and paragraph of the PA to which a comment or question pertains should be referenced. Responses to non-proprietary questions received will be posted to the IoBT CRA Program website under the “General Information/Questions & Answers" section for the benefit of all interested parties. All clearly identified and marked proprietary questions posed will be responded to via an individual email response. Applicants are encouraged to submit any questions as early as possible. The deadline for submission of questions which will be answered under this PA is 24 April 2017. Any answers provided to questions do not change the requirements of this PA. Any changes to this PA will be issued via an amended PA posted in grants.gov.

II. DETAILED INFORMATION ABOUT THE FUNDING OPPORTUNITY

A. PROGRAM DESCRIPTION

1. ARL Internet of Battlefield Things Vision

The ability of the Army to understand, predict, adapt, and exploit the vast array of internetworked things that will be present of the future battlefield is critical to maintaining and increasing its competitive advantage. The explosive growth of technologies in the commercial sector that exploits the convergence of cloud computing, ubiquitous mobile communications, networks of data-gathering sensors, and artificial intelligence presents an imposing challenge for the Army. These Internet of Things (IoT) technologies will give our enemies ever increasing capabilities that must be countered, but commercial developments do not address the unique challenges that the Army will face in using them. The U.S. Army Research Laboratory (ARL) has established an Enterprise approach to address the challenges resulting from the Internet of Battlefield Things (IoBT) that couples multi-disciplinary internal research with extramural research and collaborative ventures. ARL intends to establish a new collaborative venture (the IoBT CRA) that seeks to develop the foundations of IoBT in the context of future Army operations. The Collaborative Research Alliance (CRA) will consist of private sector and government researchers working jointly to solve complex problems. The overall objective is to develop the fundamental understanding of dynamically-composable, adaptive, goal-driven IoBTs to enable predictive analytics for intelligent command and control and battlefield services.

The Future Army will operate in a highly complex and rapidly changing environment, thus the U.S. Army's Operating Concept is to "*Win in a Complex World*". The Army must tackle wicked problems wherein objectives and constraints evolve in unpredictable ways. Complexity arises from the increasing heterogeneity, connectivity, scale, dynamics, functionality and interdependence of networked elements, and from the increasing velocity and momentum of human interactions and information. Events now unfold in internet time, as noted by the Defense Science Board (DSB) 2014 Study on *Decisive Army Strategic and Expeditionary Maneuver*. In this context, future IoBTs will be significantly more complex that today's networked systems, and novel mathematical approaches and techniques will be needed to represent them, reason about them, understand their behaviors, and to provide predictive analytics in diverse and dynamic environments.

The Army will use IoTs for diverse and dynamic missions and will require rapid deployment and adaptation in environments with high mobility, resource constraints, and extreme heterogeneity in both very dense and sparse environments. In addition to Things and IoTs that the Army owns and controls, it may also need to make use of IoTs that it does not own or fully control. A foundational problem to be addressed by the CRA is the fundamental understanding of how to learn and devise complex models of IoBT goals, networks, information, and analytics to enable intelligent command and control, and battlefield services. A critical issue embedded throughout all aspects of IoBTs is cyber physical security as the Army will need to use things it does not control (military (blue), adversary (red), civilian (gray)), accommodate deceptive data, and counter advanced persistent threats.

ARL strongly believes that a joint collaborative approach by multidisciplinary researchers is required to make fundamental advances towards meeting the CRA goal to develop a fundamental understanding of IoBTs. ARL has identified three interrelated Research Areas (RAs) that when jointly studied will advance the theoretical foundations of IoBTs in the context of future Army operations.

- Discovery, Composition and Adaptation of Goal-Driven Heterogeneous IoBTs
- Autonomic IoBTs to Enable Intelligent Services
- Distributed Asynchronous Processing and Analytics of Things

In addition to these three RAs, Cyber-Physical Security has been identified as a Cross-Cutting Research Issue (CCRI) that is inherent in each of the RAs and that must be jointly studied with the RAs to make fundamental advances in IoBTs.

The CRA is intended to create a collaborative environment that enables the Alliance to advance the state-of-the-art and to take advantage of the diverse scientific capabilities and viewpoints of both the private sector and government researchers. The CRA will work collaboratively with ARLs Enterprise research programs to identify areas where joint, multi-disciplinary, collaborative research is advantageous. Continuous collaboration, technical exchanges, site visits, and staff rotations will strengthen and improve the CRA research and its Army relevance.

2. ARL Internal Mission and Related Programs

The IoBT CRA will become an integral part of ARL's Science & Technology (S&T) Campaign Strategy. Collaboration with the internal IoBT research program and the Information Science campaign is critical to its success, and interactions with other related ARL research programs may bring different insights to bear on the CRA's research problems. Moreover, interactions with ARL's analysis and operations elements may increase relevance of CRA research and eventually lead to transition of research results.

ARL's Internal Mission

The U.S. Army Research Laboratory (ARL) is the Army's corporate research laboratory whose mission is to discover, innovate, and transition science and technology to ensure dominant strategic land power. Three Directorates of ARL -- the Computational and Information Sciences Directorate (CISD), the Human Research and Engineering Directorate (HRED), and Sensors and Electron Devices Directorate (SEDD) – conduct research related to IoBT and it is expected that CRA researchers will collaborate with researchers in these Directorates. ARL will specifically fund in-house staff to foster direct highly collaborative partnerships between Consortium and Government researchers.

ARL's Army Research Office (ARO) serves as the Army's premier extramural basic research agency and it is expected that there may be opportunities to interact with their extramural programs.

Full details about ARL’s organization and strategic planning can be found on the ARL website: https://www.arl.army.mil

ARL has developed eight S&T campaigns: Extramural Basic Research, Computational Sciences, Materials Research, Sciences for Maneuver, Information Sciences, Sciences for Lethality and Protection, Human Sciences, and Assessment and Analysis. The research program envisioned for the IoBT CRA crosses a number of Campaigns:

- **Information Sciences** is focused on gaining a greater understanding of emerging technology opportunities that support intelligent information systems that perform acquisition, analysis, reasoning, decision-making, collaborative communication, and assurance of information and knowledge through Sensing and Effecting, System Intelligence and Intelligent Systems, Human and Information Interaction, Networks and Communications, and Cyber Security.

- **Human Sciences** is focused on gaining a greater understanding of individual physical, perceptual, and cognitive performance through Human-Physical Interface, Human-Human Interface, and Human-Technology Interface.

- **Extramural Basic Research** is focused on steering and oversight of systematic studies to increase fundamental knowledge and understanding in the Physical Sciences, Information Sciences, Life Sciences, and Engineering Sciences related to long-term national security needs.

- **Computational Sciences** is focused on advancing the fundamentals of Predictive Simulation Sciences, Data Intensive Sciences, Computing Sciences, and emerging Computing Architectures to transform the future of complex Army applications.

Full details and a full listing of related ARL campaigns can be found on the ARL website.

ARL's **Open Campus** is a collaborative endeavor, with the goal of building a science and technology ecosystem that will encourage groundbreaking advances in basic and applied research areas of relevance to the Army. Through the Open Campus framework, ARL scientists and engineers will work collaboratively and side-by-side with visiting scientists in ARL's facilities, and as visiting researchers at collaborators' institutions. Central to the research collaborations is mutual scientific interest and investment by all partners. The global academic community, industry, small businesses, and other government laboratories benefit from this engagement through collaboration with ARL's specialized research staff and unique technical facilities. These collaborations will build research networks, explore complex and singular problems, enable self-forming expertise-driven team building that will be well-positioned for competitive research opportunities, and expose scientists, engineers, faculty and students to realistic research applications and perspectives, helping to ensure our nation's future strength and competitiveness in these critical fields.

Full details about ARL Open Campus can be found on the ARL website: https://www.arl.army.mil /opencampus/

Related Programs at ARL:

- **Network Science (NS) Collaborative Technology Alliance (CTA).** The objective of the NS CTA is to perform foundational research leading to a fundamental understanding of the interplay among the Social/Cognitive, Information, and Communication Networks (multi-genre) that are key components of a tactical network. This research will lead to insights on how processes and parameters in one network affect and are affected by those in other networks; these in turn should enable us to predict and control the composite behavior of these complex interacting networks. Research in the NS CTA is organized along four basic themes: (1) How -multi-genre networks behave over time (optimal design, group phenomena, large dynamic networks, prediction of network properties and structure, controllability of complex networks); (2) How information representation, discovery, and analytics contribute to distributed understanding and social influence; (3) Control of semantically-adaptive network behaviors so that the capacity of the composite network to deliver relevant information can be maximized using intrinsic, contextual, and semantic properties; and (4) The impact of trust on distributed decision-making in the presence of human cognitive limitations and conflicting, incomplete, or malicious information. Collaborations between researchers in the IoBT CRA and the NS CTA may be beneficial.

- **Cyber Security Collaborative Research Alliance (Cyber CRA).** This CRA focuses on developing a fundamental understanding of cyber phenomena, including aspects of human attackers, cyber defenders, and end users, so that fundamental laws, theories, and theoretically grounded and empirically validated models can be applied to a broad range of Army domains, applications, and environments. Specifically, this basic research program is developing and advancing the state of the art of Cyber Security in three research areas: risk, detection, and agility. Intersecting with each of the three research areas is a cross cutting research issue in psychosocial effects. Collaborations between researchers in the IoBT CRA and the Cyber CRA may be beneficial.

- **Distributed Analytics & Information Science (DAIS) International Technology Alliance (ITA).** The objective of the DAIS ITA is to establish the fundamental underpinnings for enabling distributed, dynamic, secure coalition communication-information infrastructures that will enable the formation of ad-hoc coalition teams supported by distributed analytics to derive situational understanding. Key areas of research include: (1) Dynamic adaptation of secure, resilient context-aware information systems; (2) Distributed integration and exploitation of coalition data and information across heterogeneous information infrastructures; and (3) Derivation of situational understanding of complex situations by human users synergistically supported by machines. Collaborations between researchers in the IoBT CRA and the DAIS ITA may be beneficial.

- **Network Science Research Laboratory (NSRL).** The NSRL is the first major Information Sciences Campaign laboratory space to be designed specifically to support the ARL Open Campus initiative. The NSRL is located at the Adelphi Laboratory Center, Adelphi, MD, and contains extensive space and equipment for collaborative activities in person or via remote access. It is built on an extensible infrastructure for real-time modeling of mobile network systems providing a controlled, repeatable emulation and simulation environment for the research, development and evaluation of network algorithms and protocols. Collaborations in the NSRL between researchers in the IoBT CRA may be beneficial.

A full listing of related ARL programs can be found on the ARL website.

3. CRA Programmatic Strategy

The CRA is intended to foster collaborative basic research (Budget Activity 1 - see definition below) involving the Consortium and the Government. ARL's strategy is to continue exploiting research and expertise where it exists through the issuance of a single award through this Program Announcement (PA) to a Consortium of organizations that may include institutions of higher education and industrial and non-profit entities. The Consortium will work in collaboration with ARL scientists and engineers to advance the state-of-the-art in IoBT to meet the challenges of future Army operations. ARL and the Consortium selected for award will establish an Alliance that will conduct joint collaborative basic research addressing key scientific gaps and barriers critical to realizing dynamically composable, adaptive, goal-driven IoBTs. Additionally, other government agencies may participate in the CRA and contribute their technical expertise, personnel and facilities. A significant goal of this effort will be to create a critical mass of collaborating scientists and engineers focused on solving IoBT research challenges outlined within the scope of the CRA. This intellectual synergy is also expected to include sharing equipment, personnel and facilities to promote efficiency and enhance collaboration.

Based upon the gaps discussed in Section II.A.4 and the resources identified in Section II.A.7, the research and collaboration strategy developed by the Applicant should adopt a systematic approach to fundamental research focused on understanding IoBT-related phenomena so that techniques can be used to learn IoBTs models in complex environments and to uncover hidden insights and meaningful events and anomalies. This research should lead to an elucidation of fundamental laws, theories and theoretically grounded and empirically validated models that enable design of dynamic, adaptive, goal-driven IoBTs. Applicants must carefully choose research topics to ensure a critical mass of researchers addressing the challenges proposed. Applicants are expected to apply relatively equal resources to each of the three Research Areas: 1) Discovery, Composition and Adaptation of Goal-Driven Heterogeneous IoBTs; 2) Autonomic IoBTs to Enable Intelligent Services; and 3) Distributed Asynchronous Processing and Analytics of Things. Further, a portion (approximately 15%) of the research dedicated to each area must address the Cyber Physical Security Cross-Cutting Research Issue (CCRI). The CCRI resources are an integral part of the Research Area efforts.

It is the intent of this PA to solicit the most creative, innovative, and flexible approaches to the ultimate goal of generating and exploiting research to solve pressing research gaps and issues impacting both the military and commercial sectors. This PA seeks Whitepapers and Proposals from those who receive a subsequent invitation which will result in the award of a single cooperative agreement. In response to the PA, Applicants will be required to:

- Define the strategy for implementing an approach which synergistically integrates the three Research Areas and the CCRI, and outlines the metrics by which success of the program is expected to be measured.

- Scope and define the research, appropriate to the overall funding of the CRA, ensuring all elements of the proposed research are tightly integrated in a way that results of research in one area support and enhance the results in other areas. Applicants should identify the most critical research issues and describe how the set of research efforts meet the goals of this program. Sufficient resources should be allocated to ensure enough critical mass to make fundamental progress.

- Formulate a basic research program which clearly demonstrates innovative, detailed and substantive scientific plans to address each of the three Research Areas and the CCRI as discussed in Section II.A.4. The proposal should clearly articulate the Applicant's vision for the area and the Applicant's research goals for the program (two, five and ten year goals).

- Present the experience, qualifications and availability of the scientific staff and the quality and relevance of research facilities.

- Identify approaches to building collaborations within the Consortium and with ARL, which are essential to the success of the CRA.

- Identify the overall management (business plan) and programmatic and administrative team with the expertise to achieve the stated research goals and to oversee and manage finances, reporting, data, meetings, reviews and intellectual property.

Providing the requirements above will furnish the structure for the desired comprehensive and cohesive outcome of the basic research performed under the CRA. The core basic research program will be initially funded under Budget Activity 1 (basic research) funding. However, the CRA will also allow participation from other Government agencies and may result in additional Budget Activity 1 (basic research) funding as well as Budget Activity 2 (applied research) funding (**see discussion of Enhanced Program below**). Therefore, the research proposed and performed must comply with the definition for Budget Activity 1 or Budget Activity 2 funding (as appropriate) as outlined in the DoD Financial Management Regulation (FMR), Volume 2B, Chapter 5 (December 2016) as follows:

- **Budget Activity 1: Basic Research.** Basic research is systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of

observable facts without specific applications towards processes or products in mind. It includes all scientific study and experimentation directed toward increasing fundamental knowledge and understanding in those fields of the physical, engineering, environmental, and life sciences related to long-term national security needs. It is farsighted high payoff research that provides the basis for technological progress. Basic research may lead to: (a) subsequent applied research and advanced technology developments in Defense-related technologies, and (b) new and improved military functional capabilities in areas such as communications, detection, tracking, surveillance, propulsion, mobility, guidance and control, navigation, energy conversion, materials and structures, and personnel support. Program elements in this category involve pre-Milestone A efforts.

- **Budget Activity 2: Applied Research**. Applied research is systematic study to understand the means to meet a recognized and specific need. It is a systematic expansion and application of knowledge to develop useful materials, devices, and systems or methods. It may be oriented, ultimately, toward the design, development, and improvement of prototypes and new processes to meet general mission area requirements. Applied research may translate promising basic research into solutions for broadly defined military needs, short of system development. This type of effort may vary from systematic mission-directed research beyond that in Budget Activity 1 to sophisticated breadboard hardware, study, programming and planning efforts that establish the initial feasibility and practicality of proposed solutions to technological challenges. It includes studies, investigations, and non-system specific technology efforts. The dominant characteristic is that applied research is directed toward general military needs with a view toward developing and evaluating the feasibility and practicality of proposed solutions and determining their parameters. Applied Research precedes system specific technology investigations or development. Program control of the Applied Research program element is normally exercised by general level of effort. Program elements in this category involve pre-Milestone B efforts, also known as Concept and Technology Development phase tasks, such as concept exploration efforts and paper studies of alternative concepts for meeting a mission need.

A successful research program will lay the scientific foundations for a theory of goal-driven IoBTs by combining new developments in theory, innovative extensions of existing theory, computationally efficient modeling techniques, empirically driven model development, and principled experimental validation. Research in each Research Area must not be stove-piped and it must inform and be informed by the developments in the other two Research Areas given the strong inter-dependencies between the three Research Areas.

4. CRA Research Strategy

a. Definitions, Scope, Rationale

For the purposes of this CRA, an Internet of Battlefield Things (IoBT) is a set of interdependent and interconnected entities or "things" that can include: **Sensors**, **Actuators**, **Devices** (computers, weapons, vehicles, robots, human-wearables...), **Infrastructure** (networks, storage, processing), **Analytics** (on-node, in-network, centralized), **Information sources & Open Source Intelligence**, and **Humans**:

- *That are…* Dynamically composed to meet multiple missions, tasks, or goals
- *And…* Adapt in order to capture/process data, predict behaviors/activities, and effectuate the physical environment
- *And are likely to…* operate autonomously and autonomically, i.e. properties include Self-Star characteristics (Self* = SELF organizing, configuring, adapting, maintaining, protecting)
- *Necessarily…* Interacting with humans, environment, networks
- *In order…* To enable predictive analytics that deliver intelligent command and control, and battlefield services

The Army IoBT domain will have the following characteristics:

- **Diverse IoBT missions, tasks, and goals**. An Army IoBT will be specifically created and adapted to meet a mission, complete a task, or accomplish a goal. There will likely be many IoBTs operating simultaneously, possibly competing for IoBT resources. The possible tasks are diverse including such things as wide area persistent surveillance, tracking a dispersed group of humans and vehicles moving thought cluttered environment, monitoring cities for protests, disaster relief operations, or monitoring physiological and psychological state of soldiers. Tasks are not expected to start or end simultaneously, and new tasks may emerge as others are executed.

- **Need for rapid IoBT composition, deployment, and adaptability to changing missions/tasks**. To be effective, goal-driven IoBTs must be composed and deployed rapidly, for example at a quickly-formed forward operating base. This includes identifying available things (blue, gray, red), composing to meet goals, and configuring and deploying as rapidly as possible. Once deployed, missions and tasks will be constantly changing, and new tasks may emerge, as conditions on the ground change, analysts/commanders change tactics, and as the fluid battlefield changes so the IoBT must adapt as well.

- **Highly dynamic, mobile, and resource-constrained environment**. Many IoBTs will be forward-deployed and will consist of disadvantaged assets with limitations on energy, power, storage, bandwidth, infrastructure (fixed infrastructure may not be available), computing, and communications. IoBTs must be able to operate with

these severe constraints and often need to support tasks with limited time availability.

- **Extreme heterogeneity**. The variety of things available to an IoBT is immense. In addition to the various classes of things described above, IoBTs will contain a mixture of entities that include military devices controlled by the military, adversarial devices that we do not control or partially control, or commercial and open source entities. Coexistence and co-deployment of commercial Internet of Things (IoT) devices and networks with purposefully built, certified, and carefully controlled military devices and networks will be required. These things will have a wide variety of security, provenance, and capabilities that must be accommodated and will need to exploit very capable devices and simple disposable devices.
- **Varying scale**. IoBTs will be deployed in a wide variety of places and domains, usually in contested environments. On one extreme is the highly dense and cluttered mega-city environment and on the other extreme sparse terrain with limited entities and gaps in sensor coverage and networks.
- **Contested and adversarial environments**. Many IoBTs will be forward deployed with limited physical security and will include entities in the IoBT that are owned and controlled by the adversary. It must be assumed that adversaries are already on the IoBT network and that the IoBT must be protected from sophisticated and persistent threats. Cyber/information security measures must be taken to protect IoBTs and analytics must be able to deal with conflicting and deceptive data, and identify adversarial activity.

Some of the technical challenges for IoBTs include:

- Abstractions, formalisms, and models for constructing and reasoning about dynamic composition of heterogeneous systems with complex and dynamic dependencies
- Composing and connecting sets of entities (an IoBT) from the vast array of possibilities to meet multiple (conflicting) goals
- Adapting an IoBT to sparse entities (which may require augmentation) and dense entities (like in megacities)
- Establish theoretical foundations for robust self-learning and optimization in distributed IoBTs
- Accommodating safety critical functions
- Real time synchronization and coordination for real-time analysis
- Adapting to highly dynamic resource availability (sensing, computing, bandwidth and connectivity)

The possible research challenges for IoBT are extensive and the resources available are not adequate to address them all. It is important that the Applicant identify the most critical research issues that the CRA should focus on to advance the state-of-the-art in IoBTs.

Internet of Things (IoT) technologies are rapidly being developed by the commercial sector and it is imperative that the Army exploit these future advances whenever possible, however this CRA should address the gaps that will not be addressed by the commercial sector. It is unlikely that the following lines of research would be productive for the purposes of this CRA:

- Development of standards for IoT devices and protocols
- Low power communications or novel communications modalities or protocols
- Design, development and analysis of sensors or RFIDs
- Standalone security mechanisms that are not studied jointly with other CRA research efforts
- Approaches limited to current or static IoT environments

b. Overview of Research Areas (RAs) and Cross Cutting Research Issue (CCRI)

To achieve the CRA's vision, a different approach to current research models for the commercial Internet of Things, where areas proceed independently along commercial/industrial stovepipes, is imperative. The three Research Areas (RA) and Cross Cutting Research Issue (CCRI) are:

- **RA1: Discovery, Composition and Adaptation of Goal-Driven Heterogeneous IoBTs:** Novel mathematical theories and scientific insights leading to scalable composition and management of heterogeneous IoBTs enabling secure information sharing to meet multiple dynamic mission goals.
- **RA2: Autonomic IoBTs to Enable Intelligent Services:** Theoretical foundations, models, and methods of autonomic complex systems that deliver adaptive cyber-physical capabilities and services necessary to enable effective command and control across military (blue), adversary (red), and civilian (gray) domains.
- **RA3: Distributed Asynchronous Processing and Analytics of Things:** Scientific principles, theories, and methods and predictive processing, analytics, and anomaly detection of broadly heterogeneous and varied data that may be unknown combinations of sparse and voluminous; centralized and distributed; and trusted and suspect for the purposes of augmenting goal-driven decision-making.
- **CCRI: Cyber-Physical Security**: Theoretical and pragmatic cross-cutting methods that address the challenges of the above research areas, while enriching the resiliency of the IoBT, such that it can be hardened against tampering and adversarial compromise, continue operating under attacks, and provide bounded guarantees of performance.

Research proposed in each area should be substantially different than commercial Internet of Things approaches and they must fit coherently together. Research should not be stove-piped as there are significant inter-dependencies between the RAs and the CCRI. As examples, analytics (RA3) needs/results impact goals (RA1) which require IoBT adaptation (RA2); IoBTs must adapt to changing needs/goals and to meet new service

requirements; analytics results impact the goals and autonomic behaviors; and conflicting information may trigger IoBT adaptation to detect anomalous behaviors versus faults.

The research goals to be addressed by the Applicant in each of the Research Areas and the CCRI are discussed in the following sections. Research in each RA must be performed in the context and constraints of the complementary research in the other RAs. Cross cutting research that spans the three RAs should lead to insights into the cyber-physical security aspects of IoBTs. Joint research in the RAs and CCRI should lead to deep, persistent, and meaningful collaboration among the Alliance and should harmonize vocabularies, ontologies, metrics, structures, and processes to build understanding of how to learn and devise complex models of IoBT goals, networks, information, and analytics to enable intelligent command and control and battlefield services.

RA1: Discovery, Composition, and Adaptation of Goal-Driven, Heterogeneous IoBTs

The battlefield of the future will be densely populated by a variety of 'things', comprising a heterogeneous mixture of sensors, actuators, devices, information sources, analytics, humans, and infrastructure, with varying 'intelligence' and capabilities, and constraints on energy, power, computing and communications bandwidth. The number of nodes in a future Army brigade IoBT might be several orders of magnitude greater than today. In such a scenario, the brigade may not own or fully control all the things it uses. For example, a brigade may find it advantageous to make use of "things" that it does not own, e.g., local civilian IoT, or even an adversary's IoT in a megacity operation. This heterogeneous mixture of blue, gray and red nodes is a unique differentiator from commercial IoTs. Multiple missions with differing goals will need to make use of resources in the IoBT. These missions will be asynchronous and goals may change dynamically. The massive scale might be advantageous in terms of redundancy and availability; but the massive scale, coupled with the extreme heterogeneity and dynamics, also brings several challenges that will require new theoretical results, models, concepts and technical approaches.

New concepts and approaches will be needed to facilitate discovery, characterization and tracking of relevant, available but potentially hidden, and useful things (which includes their capabilities), dynamically in time and space. The Army may use IoTs that it does not own or directly control (e.g., a local IoT or an adversary's IoT in a megacity operation), and in such a scenario behaviors and characteristics of the IoT will have to be learned and updated automatically and dynamically on the fly. Behaviors and intents of humans (friendly warfighters, adversaries, and neutral civilians) will also have to be dynamically detected, identified, characterized and accounted for as part of IoBT's operation.

Automated approaches for continuous allocation and reconfiguration of sensing, processing, communications, and sense-making assets must be designed. Information sensing, processing, and sharing strategies and policies (who senses what, what is processed where, who talks to whom, when, about what, and how long) will have to be automatically designed and modified dynamically. The high complexity, scale and dynamics of the IoBT leads to challenges in communications between things. Novel approaches are required to overcome the key challenge of finding, sharing and managing

communication channels and modalities, between large numbers of competing, heterogeneous and often unpredictable things. Additional complexity will arise from the wide range of timing constraints on communications, as, for example, tolerable delays in information sharing may vary from several hours to real-time. Highly scalable architectures and protocols will be needed, along with rigorous methods to determine and validate properties of protocols and architectures.

Dynamic management of the IoBT will require "situational awareness" of the IoBT. Appropriate definitions of "network state" are required, along with scalable approaches to distributed measurement and inference of state, possibly with impaired communications. It is expected that such state information will be distributed and decentralized, and appropriate learning techniques in this context must cope with the various constraints discussed above, as well as potential sparsity of data; in addition, data may be dirty, small/sparse, dynamic and deceptive. Parsimonious quantitative metrics of the complex system are expected to provide insights and help the decision maker.

The scale and connectedness of the IoBT increases the attack surface for our adversaries, leading to increased vulnerability of the cyber-physical systems, embedded in or connected to or controlled through the IoBT. Device constraints and demands for real-time control and decision making, random and targeted thing failures, all potentially enhance vulnerability; aspects that an Applicant would need to address in developing solutions for RA1 and consider in the context of the CCRI.

The following paragraphs describe important research issues in this research area. These should be understood as suggested topics and issues for consideration in formulating a research program to address the above-described gaps and challenges, and not as definitive or exhaustive. Indeed, it is expected that competitive proposals will contain other innovative topics and approaches, and may identify other gaps and challenges. The inherent nature of the problem calls for a multi-disciplinary approach and tackling these research challenges requires a mix of expertise in information science, network science, communications & networking, computer science, theory of complex systems, mathematics, etc.

Important research issues, in the context of the preceding discussion of challenges in this area, include:

- Dynamic discovery and tracking of potentially hidden IoBT assets leading to secure dynamic distributed composition and control of assets (information sources, sensing, computing, storage, communications, and subnetworks) to support multiple diverse missions
- Novel network and information theory, in the context of dense IoBT networks and IoBT data/info traffic patterns, leading to strategies for scalable information sharing (secure communications & networking) protocols and architectures for a dynamic IoBT

- Appropriate definitions of network state and scalable approaches to measure and infer network state; learning must be robust in the presence of sparse measurements, and data that may be dirty, small/sparse, dynamic and deceptive.
- Theoretical understanding of multiple complex tradeoffs; e.g., in expected redundancy of devices and services vs. availability (and lifetime) and robustness and resilience (to adversarial actions)
- Detection, identification and characterization of the behaviors and intents of humans (friendly warfighters, adversaries, and neutral civilians) as part of and in order to operate the IoBT

Research in this area must not be stove-piped, but must inform and be informed by the developments in the other two Research Areas, given the strong inter-dependencies between the three Research Areas. For example, results of Analytics (RA3) may impact goals leading to reconfiguration and re-composition of IoBTs. Adversarial behaviors and required deceptive practices (RA3) will drive resource allocation. To facilitate rapid adaption to node failures and adversarial actions (RA2), sufficient redundancy may need to be built into resource allocation via jointly developed metrics. As noted earlier, cyber-physical security is an inherent aspect of each research area, and is embedded in the research issues listed above.

RA2: Autonomic IoBTs to Enable Intelligent Services

The IoBT will manifest as a broad, ubiquitous, sensor-network field that supports actuation where the boundaries of ownership, access, and control are non-deterministic, rapidly changing, and contested. The dynamics and pervasiveness of IoBT assets will present unique challenges to command and control, situational awareness, and the accomplishment of mission-goals. Moreover, adversaries will exist in the IoBT network and represent a persistent threat to the services that the IoBT may deliver. Complexity and uncertainty will be high and unforeseen opportunities will lead to competitive advantage assuming the sensor field can be manipulated. For example, while entering a building in order to accomplish a mission objective, a squad may need to temporarily disable visual or acoustic sensors deployed and operate on the squad's military network, while concomitantly actuating a series of doors using existing enterprise network infrastructure. Even in this simple example of a mission objective, uncertainty can be seen in the assurance that the IoBT services and related actuation actually executed, let alone in consideration of adversarial activities on the enterprise network. In achieving more involved mission goals, the IoBT will operate as a complex autonomous system that can be defined as a set of a huge number of interacting (heterogeneous) entities and services; the global behavior of which cannot be easily predicted analytically or confirmed by an external observer.

New theories and methods will be needed to enable intelligent and adaptive re-composition, orchestration, and execution of IoBT services. Approaches that provide this functionality intelligently and autonomously while incorporating uncertainty quantification must be designed and developed. Moreover, developed approaches must address run-time IoBT dynamics that exceed human op-tempos. While autonomy supports

accomplishment of delegated mission goals, autonomicity supports survivability of mission assets, especially when human tending is not available/feasible. Autonomic system properties (which ensure self-configuring, self-optimizing, self-healing and self-protecting behaviors) enable battlefield dynamics not previously possible and are critical to maintaining information dominance in an IoBT-enabled battlespace. Intelligent services in the IoBT have a critical need for autonomous repurposing and re-tasking of devices and information objects where autonomic properties are equally important to autonomous functions.

The heterogeneity of IoBT devices will require adaptive controls to effect linkages and changes that are useful to end users and accomplish mission goals; and thus, will rely on a high degree of autonomy and self-awareness in order to perform and respond dynamically to changing internal or external circumstances, both foreseen and unforeseen, in order to support the dependability of the system. To achieve this self-awareness and versatility novel machine learning and artificial intelligence approaches will need be developed to deal with the voluminous and dynamic IoBT data and environmental uncertainty, as well as to deal with terrain where assets / data are sparse. However, such continuous learning processes, as will be required, may computationally inhibit timely IoBT actuation and effecting. Interactions with the IoBT will be further challenged by the possibility that an adversary will adapt and could evolve faster than the learning process can.

This research area should have linkages to solutions proposed under the other two research areas (RA1 and RA3). Addressing issues of adaptive IoBT execution, autonomicity, and resiliency necessarily requires that a mission-goal relevant IoBT has been defined, discovered, composed (RA1), as well as concepts and methods for processing, analyzing, and understanding IoBT data, such that anomalies are detected, uncertainty is reduced, and mission-goal related decisions are augmented (RA3). Further, challenges in this research area cannot ignore security considerations. For example, Autonomic security is a more complicated problem, compared to "reconfigurable" security. Reconfigurable security typically only requires adding more automation in the entire reconfiguration process so as to make the security system self-responsive, whereas autonomic security implies combined characteristics of self-awareness, continuous learning, and intelligent automation.

The following list provides sample gaps in the state-of-the-art that would be applicable to this research area. It should be understood this list is given as exemplar gaps for consideration in formulating the research to address the above-identified challenges in this research area, rather than being a definitive or exhaustive list of challenges or topics. Moreover, it is expected that competitive proposals will contain other innovative topics and approaches, and may identify additional gaps.

Major gaps in the state-of-the-art in this research area include:

- Theoretical foundations for self* (e.g. self-organizing, self-managing, self-adapting, self-maintaining/self-protecting, etc.) properties in heterogeneous complex-systems that define approaches, which facilitate interoperability, just-in-

time (JIT) human interactions, and the implementation of local-adaptation functionality in self-organizing, complex systems

- Theoretical principles that span the multiple levels at which autonomic systems can exist-from systems to enterprises; e.g. formalisms to support diverse, nonlinear, likely non-ergodic, and emergent system behaviors or tractable optimization strategies in non-stationary systems
- Novel distributed or hierarchical control theories that consider interactions and actuation among independently or hierarchically controlled elements, versus individually controlled elements
- Methods for computational learning and reasoning that operate on shorter time scales and/or where there may be few or no guarantees of convergence and are amenable to adaptive learning and optimization

RA3: Distributed Asynchronous Processing and Analytics of Things

The expected exponential growth in the number of interconnected devices creates many challenges from a perspective of information management, situation understanding, behavior prediction, and system modeling. The scale, complexity and ubiquity of IoBT devices and computing resources processing sensed events will reach a level never seen before. Reliance on intelligent and automated processing of information will be essential to handle the expected density and scale of IoBT devices. This processing is likely to be distributed across high-capability centralized nodes to edge-devices with specialized processing power. For example, a squad at the tactical edge may require information from unattended ground sensors that have built-in at-sensor-processing to classify sensed phenomena, but may also require it to be correlated with logistics data at the tactical operations center. In the IoBT, data that needs processing will come from widely heterogeneous sources, formats, and volumes. Moreover, the IoBT will demand distributed processing of discrete and potentially continuous data arriving for processing with varied temporal resolutions. Users of distributed computing services (i.e. warfighters) should not need to care about how the services are implemented, what technologies are used, or how they are managed. Further IoBT data is both: sparse and dense. Thus, the focus in this Research Area is on distributed data processing and anomaly detection, as these analytical challenges include issues of data sparseness, volume, resolution, integrity, and relevance.

Foundational theories and approaches are needed for complex event processing, with compact representations, efficient pattern evaluation, and anomaly detection. Mission-Goal driven IoBT data will not only come from environmental sensors (e.g. acoustic, tripwire, snapshot, etc.) but also sensor data such as images and videos, electrocardiograms, electroencephalograms, platform-kinematics, and other platform-centered monitoring. The research on formulating and automatically creating (and dynamically maintaining) composite models of heterogeneous multi-scale sensor information and complex event sequencing is only now emergent. Effective solutions to this challenge will likely involve distributed analysis, calibration, validation, and anomaly detection of IoBT data. Research in this area must go beyond algorithmic sort/filter-and-reduction techniques and focus on

other approaches that allow for faster, possibly real-time, updating of models/solutions when new data or constraints are added to the mission goal.

Research in this area should inform and be informed by investigations and finding in the other two research areas (RA1 and RA2). For example, the results of processing and analysis solutions in this research area may re-define the mission-goal requirements and resource allocation for the IoBT (RA1). Similarly, the distributed processing and analytics of Things may provide data and information that aids, augments, or enables autonomic self-awareness characteristics (RA2). It is intended that this research area not be partitioned and viewed in isolation, separately from the other two research areas and the cross-cutting research issue (CCRI). As noted in RA1 and RA2, this research area (RA3) should not exclude security concerns from consideration. For example, the detection of anomalies, given dynamic mission goals and a dynamic sensor-actuation-field presents a difficult problem in even defining an anomaly, let alone detecting them.

The following list provides a sample of gaps in the state-of-the-art that would be applicable to this research area. It should be understood this list is given as exemplar issues for consideration in formulating the research to address the above-identified challenges in this, rather than being a definitive or exhaustive list of problems or topics. Moreover, it is expected that competitive proposals will contain other innovative topics and approaches, and may identify additional gaps.

Major gaps in the state-of-the-art in this research area include:

- Theoretical foundations for novel information discovery, processing, inference, and delivery, under adversarial deception / misinformation, leading to an understanding of tradeoffs and identification of anomalies
- Theoretically grounded approaches for uncertainty quantification and propagation in multi-scale, multi-source data and models
- Distributed and asynchronous processing, fusion, analysis and machine learning/reasoning of multi-modal heterogeneous data, including quantification and management of trustworthiness, risk, and uncertainty
- Robust semantically-grounded oriented approaches to represent, organize, reason about, interpret and summarize (the potentially large volume of) information generated by the IoBT to aid human decision making

CCRI: Cyber-Physical Security

The concepts that underlie IoBT will fundamentally change the doctrine and the Techniques, Tactics, and Procedures (TTPs) of the future military battlefield, which will be a highly connected operating environment, containing ad-hoc and large-scale deployments of capillary and high density personal and environmental sensors systems. The prospect of everything in and related to the battlefield being a networked entity, regardless of how small or large, significantly increases the potential for improved situation

awareness at multiple levels. The integration between information and communication technologies and actuated physical systems in the IoBT introduces new security concerns, requiring reconsideration of commonly used theories and methods. As such, deceptive and adversarial operations embedded in red, blue, and gray resources will be the new normal. Cyber physical security will require novel innovations that affect the challenges outlined in RA1, RA2, and RA3.

In the IoBT, existing security approaches will be either inapplicable, not viable, insufficiently scalable, incompatible or simply inadequate in addressing the challenges posed by highly complex networked systems, sensors, and actuators in diverse environments, tasked with accomplishing high level mission goals. Moreover, the self-aware nature of the IoBT will likely include continuous learning capabilities that make the threat of tampering and deception, not only likely, but also difficult to detect. Dependence on widespread computing and networking naturally increases security concerns as the availability, integrity and secrecy of the data carried has an increased likelihood of being compromised. At the same time, the presence of the physical system widens the range of possible attacks and constrains the set of feasible countermeasures. For example, shutting off the physical system to troubleshoot a communications issue will not generally be a viable solution. On the other hand, the linkages to the physical domain and other IoBT characteristics will provide unique opportunities for combatting security challenges. For example, the sheer quantity of things (especially in those cases when friendly forces leverage the local IoT) permits the use of "disposable" security: devices that are believed to be potentially compromised by the enemy are simply discarded or disconnected from the IoBT. This example illustrates how a physical security measure can dramatically impact many of the challenges in RA1: Discovery, Composition, and Adaptation of Goal-Driven, Heterogeneous IoBTs.

As an illustration of how the intrinsic quantity of IoBT devices can impact RA2 (Autonomic IoBTs to Enable Intelligent Services) and RA3 (Distributed Asynchronous Processing and Analytics of Things), consider the following example. To defeat adversaries' eavesdropping, defenders may want to take advantage of plentiful availability of things and inject misleading information into a fraction of them. However, this approach to defense, which actually implements a physical attack, can also compromise key security properties such as data confidentiality, integrity and availability, without compromising the cyber part of the system. Without taking into account physical system dynamics, cyber security alone, (which is ***not*** the sole point of this CCRI), can only predict the effects of an attack on the system in a limited fashion; therefore, it is not well equipped to either provide insights aimed at robust design, goal-level impact risks, or appropriate runtime countermeasures.

The Cyber Physical Security CCRI must be jointly studied in the context and the constraints of the three research areas. It is expected that other CCRIs will emerge as the research progresses. New theories of information, complex-system effects, and deception are intricately linked and must be studied jointly. This research must develop appropriate mathematical representations, metrics, models, and analysis techniques. Expected outcomes are autonomous anticipation of, and adaptation to both opportunities and threats

which can eliminate costly, labor-intensive defensive measures and reduce confidence in decision making, thus significantly simplifying the complexity of IoBT usage and of the information that needs to be comprehended, approved by, and/or applied correctly to users, analysts, and defenders

The following list provides a sample state-of-the-art problems that represent exemplar cross-cutting challenges, relevant to this research issue. It should be understood this list is given as s small set of examples for consideration in formulating cyber physical security considerations, as applied in each of the three Research Areas, rather than being a definitive or exhaustive list of challenges in this CCRI. Moreover, it is expected that competitive proposals will contain other innovative CCRI topics and approaches, and ideally identify additional challenges.

Major gaps in the state-of-the-art in this research area include:

- Secure composition and integrated security, e.g. architectural/software approaches that allow components to interact not only with servers but also with other (potentially embedded) components of a sensor fabric where high bit count (e.g. 1024, 2048, 4096-bit, etc.) encryption will not deliver cost-wise effective solution to all security problems.
- Principles of distributed and hybrid approaches combining model-based and data-driven base approaches, to detect anomalies in the environment and in "Things" in a manner that is both aware of and synergistically helpful to learning operating parameters, security considerations, and mission goals of the distributed fabric of IoBT
- Fundamental theories and novel approaches and methods to accomplish secure updates and prevent/detect tampering while enabling deception detection and adaptive hardening against adversarial machine learning techniques
- Principles for self-awareness of space, time and power characteristics and its relation to requirements of active/pending mission(s), of a Thing, with additional ability to degrade or self-destruct gracefully. Furthermore, Things, in IoBT, need to have to ability to balance the trade-off between accuracy of computation required to answer queries of users, security concerns and mission criticality.

5. Collaboration

a. Background

This program continues the ARL concept of creating Alliances (Collaborative Technology Alliances (CTAs) and Collaborative Research Alliances (CRAs)) to facilitate a close collaborative relationship between ARL and its partners. Experience has shown that persistent collaboration across the Alliance enhances innovation and has a high return on investment. Therefore, collaboration between Consortium and Government researchers is

integral to the execution and success of the CRA. It is ARL's strong belief that work conducted under the IoBT CRA cannot be successful either in whole or in part without collaboration. Creation of an environment that is conducive to collaboration is therefore a critical element in establishing the Alliance. This section describes collaborative opportunities and potential avenues to collaborate under the IoBT CRA. The implementation of the collaboration with ARL will be through the proposed Initial Program Plan (IPP) and the subsequent Biennial Program Plan (BPP). Applicants are invited to suggest additional new and innovative avenues for fostering collaboration among Alliance partners.

b . Collaboration Opportunities

ARL will specifically fund in-house staff to foster direct highly collaborative partnerships between Consortium and Government researchers. This in-house effort is anticipated to cover the Research Areas and the CCRI of the IoBT CRA. ARL will shape its mission program for synergies with the CRA research strategy, the CRA Initial Program Plan (IPP) and subsequent Biennial Program Plans (BPPs), thus insuring a direct and continuing collaboration across the Alliance. The BPP will be the basis for the Alliance to optimize the collaboration, information, research and technology transfer between the CRA and ARL. The Government may also leverage and/or integrate other interested Other Government agencies (and funding where appropriate) into the CRA umbrella.

c. Staff Rotation

An important element of CRA collaboration is the advancement, education and rotation of research staff through short-term and long-term temporary assignments. The scope of this collaboration may range from regular, periodic short term visits to sabbaticals lasting as long as a year. Staff rotations will be undertaken to foster and facilitate collaborative research where face-to-face interaction is advantageous, to enable a researcher to utilize unique facilities, to enable Alliance personnel to obtain specialized training or experience and to facilitate the exchange of research results. In addition, this exchange, or cross fertilization, of personnel will provide Consortium personnel with insight into Army unique requirements and will provide Government personnel with insight into state-of-the-art research and commercial practices and/or the opportunity to pursue fundamental research with noted researchers. The success of these interactive and collaborative exchanges will be assessed by the quality of the collaboration as demonstrated by joint efforts such as basic research transitions to applied research programs, archival journal papers, patents, and refereed presentations. Applicants should outline the range of opportunities foreseen for collaboration and the mechanisms that will be put into place to foster staff rotations and other collaborative activities.

All salary and travel costs associated with the rotation of Government personnel will be borne by the Government. All salary and travel costs associated with staff rotations of Consortium members will be funded under the CA or may be provided by the Consortium member as cost-share. It is anticipated that some portion of the Consortium's scientific labor-years will be in staff rotations.

d. Lectures, Workshops, and Research Reviews

The Alliance (Consortium and ARL) will be encouraged to hold, from time to time throughout the period of performance of the IoBT CRA, scientific lectures, short courses and workshops on mutually agreed upon topics. These lectures and workshops will serve as both educational and research outreach opportunities and should involve participants outside the Alliance when appropriate. Additionally, the Alliance is expected to hold regular, periodic research reviews that will permit the free exchange of ideas and research results, especially those impacting any crosscutting research themes, among the entire ARL enterprise addressing IoBT. The costs associated with the Consortium's efforts for these lectures, short courses, workshops and reviews will be funded under the CA.

The Consortium is also expected to host a web based repository of information from the CRA that is accessible by ARL, Consortium members, and CRA stakeholders for the duration of the CRA. At completion of the CRA, documentation will be delivered to the government for record keeping. This repository will include programmatic and review material. It will also serve as a vehicle for software and dataset sharing.

6. Management

a. Background

It is critical that the Consortium be structured and managed to create and foster an open, collaborative research environment. This section describes a framework for the organization of the CRA. The lightweight framework is flexible to minimize overhead, yet ensure research relevance and proper oversight. Applicants can suggest additional management tools and mechanisms as part of the proposal, but in doing so they must also justify and demonstrate the benefit and cost effectiveness of these additional management activities.

b. Overall Management Concept

ARL and the Consortium will establish a Collaborative Research Alliance. Additionally, other Government agencies may be invited to join this Alliance and to contribute, as appropriate, their technical expertise, personnel, access to research facilities and funding. The Alliance will strive for a focused, yet flexible research environment. To accomplish this, the consortium should consist of a small number of institutions of higher education, and industrial organizations, including the Lead Research Organization (LRO), possessing significant expertise in one or more of the Research Areas covered by the CRA, led by a single organization, the LRO, with the ability to integrate the broad palette of research required to realize the goals of the CRA. Each RA will be led by a different Lead Research Area Organization (LRAO), one of which could also be the LRO. Together the LRO and LRAOs make up the Consortium, who together are responsible for shaping and steering the CRA through participation, with their respective ARL Research Area Leads. Performance under the CA may also include other organizations as subawardees to round

out the technical expertise and research tasks in a given RA. Any such organizations are expected to be subawardees to the LRO.

In addition to research conducted by members of the consortium, the research program may be enhanced by research undertaken by other organizations selected jointly by the Alliance as part of its planning process. Applicants are asked to suggest a process for incorporating new topics and organizations into the research program.

c. Technical Guidance and Oversight

The following framework is required for the management and oversight of the Alliance. It consists of parallel managers from the Government and the Consortium who will provide day-to-day coordination, as well as a small managing board representing the interests of each of the Consortium members and a consultative group of interested parties from the Government. Applicants may propose additional plans or mechanisms for management; however, Applicants are cautioned to ensure that any such plans or mechanisms are: (1) not duplicative of the requirements, and (2) not overly burdensome to the Alliance. A description of each component of the Alliance Management follows:

- **Collaborative Alliance Manager (CAM)**. The research executed under the CRA will be considered an extension and integral part of the U.S. Army Research Laboratory (ARL) research program. As such, the program established under this PA will be planned, defended, executed, and reviewed as part of ARL's mission program. Overall scientific management and fiscal responsibility for the CRA will reside with a senior ARL scientific manager, who will be designated the CAM for the CRA under the cooperative agreement. The Grants Officer will receive recommendations from the CAM and will be the ultimate legal authority empowered to make formal adjustments to the CA.

- **Program Manager (PM).** The CRA Program Manager (PM) is the LRO's scientific representative charged with the Consortium's overall responsibility for management and guidance of the cooperative agreement. The PM is required to be an eminent scholar in the field of IoBT-related technologies and have the stature, experience and leadership skills to successfully execute the CRA program. It is also recognized that the PM may require staff support to manage and execute the cooperative agreement, and this staff support should be included in the Proposal submission.

- A **Research Management Board (RMB)** will be established by ARL to identify and develop collaborative opportunities, advise and assist the CAM in setting research goals, and facilitate transition of CRA research to ARL and other Government basic and applied research programs. The RMB will be chaired by the CAM and will include representatives from Army, other service organizations and other Government agencies with interest, expertise in the technologies related to the CRA. The RMB will be invited to CRA meetings, and be informed about the Biennial Program Plan approval process.

- **Consortium Management Committee (CMC)**. The CRA will have a Consortium Management Committee (CMC) that consists of one representative from each member of the Consortium. The CAM participates as ex officio member in all discussions except those that deal with purely internal Consortium matters. The CMC will be chaired by the PM. Each Member will have one vote on the CMC to support programmatic and management-related activities and decisions. In the event of a tie, the LRO will cast the deciding vote. The CMC will be responsible for the management and integration of the Consortium's efforts under the CRA including programmatic, technical, reporting, financial, and administrative matters. The CMC makes recommendations that concern the membership of the Consortium, the definition of the tasks and goals of the participants, and the distribution of funding to the members and subawardees. Quarterly meetings will be conducted by the CMC.

d. Articles of Collaboration (AoC)

The Articles of Collaboration define the operational structure and governance within the Consortium including:

- Membership and management
- Changes to Consortium membership
- Financial, personnel, facilities, and reporting requirements
- Intellectual property
- Information exchange guidelines
- Modifications to the AoC

Applicants invited to submit a Proposal will be provided a model Articles of Collaboration (AoC) with their invitation to submit a Proposal. The model AoC represents appropriate and necessary terms and conditions that the Government finds acceptable for operation of the Consortium. Applicants must submit the AoC with the Proposal signed by a duly authorized representative for each proposed Member of the Consortium. The model AoC can be executed by the proposed Members of the Consortium “as is” or changes can be proposed. If changes are proposed, Applicants are hereby informed that justification of any changes should be included with the Proposal and such changes must be acceptable to the Government for the Applicant to be eligible for award.

e. Initial Program Plan (IPP) and Biennial Program Plan (BPP).

Within 90 days after award, the Consortium and the Government will jointly prepare an Initial Program Plan (IPP) to cover the first 12 months of performance. The IPP will be based substantially on the Proposal received from the Consortium. The IPP will be accompanied by a five-year roadmap that describes the overall plan to be accomplished by the Consortium within the Alliance structure. This roadmap should provide the vision for goals to be addressed during the first five years of the Alliance. The roadmap should provide a detailed description of a well-coordinated preliminary IPP for execution of the

basic research. It should provide approximate timelines for research activities to facilitate potential future basic research transitions.

Eight months after award, the Consortium and the Government will jointly prepare a proposed Biennial Program Plan (BPP) for the next two fiscal years. The BPP will enable integration and execution of multidisciplinary, collaborative research that strives to achieve CRA objectives. The CAM will approve the BPP and formally submit the approved BPP to the Grants Officer for incorporation into the cooperative agreement. This process will continue through the life of the cooperative agreement. Each BPP will cover a two-year timeframe, but may be altered, with the approval of the CAM and the Grants Officer, if research work requirements change. The BPP will provide a detailed plan of research activities (including research goals, key personnel, staff rotation, facilities, experiments and budget) that commits the Consortium to use their best efforts to meet specific research objectives. The BPP will also describe the collaborative efforts with the Government. The BPP will include a detailed description of the projects proposed to be undertaken by any subawardees, including new subawardees that may be included at the discretion of the Government.

During the course of performance, if it appears that research goals will not be met, the CMC will provide a proposed adjustment to the BPP for approval by the CAM. In addition, the CAM may from time to time request that additional research be added to the BPP within the scope of the cooperative agreement. The Consortium, as an entity, will not solicit or accept funding from outside sources without the approval of the CAM and the Grants Officer.

During the course of performance, the Grants Officer, in coordination with the CAM, will have approval authority for certain specific changes to the IPP/BPP including but not limited to:

- Changes in the scope or the objective of the program, IPP/BPP, or research milestones;
- Change in the key personnel specified in the IPP/BPP;
- The absence for more than three months, or a 25% reduction in time devoted to the project, by the PM;
- The need for additional Federal funding; and
- Any subaward, transfer, or contracting out of substantive program performance under an award, unless described in the IPP/BPP.

The CAM, in coordination with the CMC and ARL management, will be responsible for integrating the IPP/BPP into the overall Government research and technology programs. During the course of performance, the Grants Officer, in coordination with the CAM, will have approval authority for certain specific changes to the CA including, but not limited to:

- Changes to the Articles of Collaboration if such changes substantially alter the relationship of the parties as originally agreed upon;
- Solicitation or acceptance of funding under the agreement from sources other than ARL; and

- Changes in Consortium membership. It is expected membership will change as technical efforts progress and resource levels change.

f. Collaboration and Technical Review Meeting

Each year, the Alliance must organize a CRA Collaboration and Technical Review meeting where Alliance researchers engage in face-to-face technical discussions. The overall goal of this meeting is to foster interactions and collaborations among researchers and allow Alliance research leadership to assess research progress. The emphasis is on collaborations (especially multi-disciplinary, cross-Research Area collaborations), experimentation/validation plans, and possible transition opportunities. Planning for the Collaboration and Technical Review Meeting will be executed through the PM and the CAM. Additionally, it is anticipated that the Alliance will participate in other ARL/Army program reviews.

g. Evaluation For Five-Year Extension

The CRA will be awarded for a five-year period. There will be an option to extend the CRA for an additional five years. At the end of the fourth year, a comprehensive program review will be conducted as directed by ARL. This review will consider cumulative performance metrics, the Consortium's vision for the additional five-year period of performance (to be submitted by the Consortium at the end of the fourth year), funding availability and the current research needs and goals of the U.S. Army. Performance metrics are expected to include items that provide an indication of the CRA's accomplishments, the number of refereed journal and conference articles, invited presentations, patents, relevance of the work to ARL, collaboration, and staff rotation. The decision as to whether to exercise the option is expected to be based on the results of the review and evaluation described above.

h. Distribution of Funding

The LRO will distribute the funding to all Consortium Members and subawardees.

7. Funding

The estimated funding levels for the CRA over the projected period of performance, including options years, is shown in the top part of Table 1. The funding includes all known costs associated with the cooperative agreement (CA), i.e. the costs for research, program management, experimentation, travel, etc. The key assumption is that the CA will be awarded in the 4th quarter of FY17. Proposed guidance for unfunded Enhanced Program funding is also depicted in the bottom part of Table 1.

Award will be made to the Consortium that offers the best value to the Government. An Applicant must recognize and understand that there are no guarantees associated with the levels of funding during the period of performance. Consortium Members may be expected to compromise and sacrifice anticipated funding to their organization as necessary and

appropriate to meet the goals and objectives of the CRA as established through the collaborative planning process.

Enhanced Program

The understanding is that the IoBT research is required across all of DOD, so an unfunded Enhanced Program is included in this PA. This provides a mechanism for growth and enhancement within the CRA. ARL, the Army and other Government agencies may choose to support the program with basic and/or applied research dollars in areas of specific interest to their basic and applied mission programs. This enhanced program will leverage parallel and/or transition the research, technology and capabilities that are the core of the ARL funded CRA. **In response to this PA, Applicants are not to include the Enhanced Program in the Whitepaper. Applicants invited to submit a Proposal are required to provide a detailed proposal to address the entire funded core research program as part of the Proposal. In addition, Applicants are asked to include a general discussion of possible additional research that could be pursued should funding be received to enhance the CRA effort. This is required for the Proposal only.**

Table 1. Anticipated CRA Funding
(Funded Core CRA Research Program & Unfunded Enhanced Research Program)

Funding Category	**Core Research Program ($M)* Fiscal Year**										
	FY17	FY18	FY19	FY20	FY21	FY22	FY23	FY24	FY25	FY26	**Total (10yr)**
Basic Research (6.1)	0.5	4.1	4.2	6.0	6.1	6.2	6.3	6.3	6.3	6.3	**52.3**
Core Total	0.5	4.1	4.2	6.0	6.1	6.2	6.3	6.3	6.3	6.3	**52.3**
	Enhanced Research Program ($M)										
Basic Research (6.1)	0.3	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	**4.8**
Applied Research (6.2)	.5	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.2	**10.5**
Enhanced Total	.8	1.6	1.6	1.6	1.6	1.6	1.6	1.6	1.6	1.7	**15.3**
Total	**1.3**	**5.7**	**5.8**	**7.6**	**7.7**	**7.8**	**7.9**	**7.9**	**7.9**	**8.0**	**67.6**

Note: Total Funded 10 Year Core Program $52.3M
Total Funded 10 Year Core and Unfunded Enhanced Program $67.6M

B. AWARD INFORMATION:

One CA will be awarded as a result of this PA. The Applicant selected for award will be notified by the Grants Officer or his/her designee telephonically or via email. Upon notification, the selected Applicant will be required to sign the CA. The award is not official until each Consortium Member on the selected Applicant's Proposal has signed the CA and the Grants Officer has signed the CA.

A CA is a legal instrument which, consistent with 31 U.S.C. 6305, is used to enter into the same kind of relationship as a grant (see definition "grant"), except that substantial involvement is expected between the Federal Government and the recipient when carrying out the activity contemplated by the cooperative agreement. The term does not include "cooperative research and development agreements" as defined in 15 U.S.C. 3710a. No profit/fee is not permitted under the CA for the recipient or any subawardees.

CAs for Institutions of Higher Education and nonprofit organizations are primarily governed by the following:

a. Federal statutes
b. Federal regulations
c. 2 CFR Part 200, as modified and supplemented by DoD's interim implementation found at 2 CFR Part 1103

The following websites may be accessed to obtain an electronic copy of the governing regulations and guidance:

FAR, DFARS, and AFARS: http://farsite.hill.af.mil/
Code of Federal Regulations: http://www.ecfr.gov
DoD Research and Development General Terms and Conditions:
https://www.onr.navy.mil/Contracts-Grants/submit-proposal/grants-proposal/grants-terms-conditions.aspx
Agency-specific Research Terms and Conditions:
http://www.arl.army.mil/www/default.cfm?page=8

C. ELIGIBILITY INFORMATION:

1. Eligible Applicants

During performance, it is envisioned that there will be Consortium Members and Subawardees performing under the CA. The Consortium must be led by an institution of higher education. This organization will be designated as the LRO and this organization has specific leadership and management responsibilities and roles as outlined below. Each Research Area will be led by a different LRAO, one of which could also be the LRO. The same entity cannot be the LRAO for more than one Research Area. Together the LRO and

LRAOs make up the Consortium. Consortium Members are expected to have significant involvement and input on a long-term basis as outlined below. Researchers from any Consortium Member may participate in the research undertaken within any of the three Research Area. It is anticipated that an optimally sized consortium, with subawardees, would include no more than eight organizations, but this should not be considered a hard limit. Whitepapers and Proposals that include more than eight organizations must provide a rationale for the additional members. Thus, Applicants are expected to consider carefully the construct of their proposed Consortium and effectively engage the appropriate Membership and Subawardee performance to achieve the goals of the CRA. See also Section E.3 – Recipient Qualification.

Discussion of Consortium Members and other Participants in the CRA:

- **Lead Member called the Lead Research Organization (LRO):**
  The LRO must be an institution of higher education. This institution is also expected to have doctoral level courses of study in scientific and research areas related to this CRA that can result in the granting of a doctoral degree. The LRO is expected to articulate a vision for the CRA, promote collaboration among Consortium Members, and coordinate crosscutting research themes. The LRO is required to administer the Consortium, participate in the research, and promote the transition of research and technologies resulting from the research program within the CRA. This includes distribution of Government funding to Consortium Members and subawardees in accordance with the approved IPP/BPP. The LRO is responsible for timely billing (invoicing) of executed research for itself and the other Consortium Members to ensure proper disbursement of government funds.

- **Other Consortium Members – Lead Research Area Organizations (LRAO):**
  Each LRAO may be an industrial, non-profit, or institution of higher education and must possess substantial experience and expertise in the research areas contained within the scope of the CRA. Each Research Area will be led by a different LRAO, one of which could also be the LRO. The same entity cannot be the LRAO for more than one Research Area. Under special considerations outlined below, Federally Funded Research and Development Centers (FFRDCs) may participate in the Consortium as a Member. Institutions of higher education are also expected to have doctoral level courses of study in scientific and research areas related to this CRA that can result in the granting of a doctoral degree. Industrial members are expected to have the ability to conduct appropriate research activities utilizing in-house engineers, scientists and facilities. All Consortium Members are expected to demonstrate opportunities for substantive collaboration with ARL, including appropriate opportunities for staff rotations and research collaboration. Researchers from a LRAO may participate in the research undertaken within any of the three Research Area.

- **Subawardees:**
  The Consortium may be augmented with Subawardees to meet the research objectives of the CRA, especially for the conduct of new and innovative research for which they are particularly qualified. Subawardees are organizations that (1) are not expected to

provide strategic input concerning the goals and direction of the CRA and (2) may possibly have only a short term relationship with the Consortium.

- **Federally-Funded Research and Development Centers (FFRDCs):** Federally Funded Research and Development Centers (FFRDC) may be included as Consortium Members (LRAOs) or subawardees in a Proposal under this PA, but an FFRDC may not be the LRO. FFRDCs may propose effort as allowed by their sponsoring agency and in accordance with their sponsoring agency policy.

2. Cost Sharing or Matching

Cost sharing is not required under this PA. See also Section I.B above.

D. APPLICATION AND SUBMISSION INFORMATION

The application process consists of a Whitepaper stage and a Proposal stage. The purpose of requesting Whitepapers is to minimize the effort associated with the production of detailed proposals for those Applicants that have little chance of being selected for funding. The Government's decision to invite a Proposal will be based upon the evaluation results of the Whitepaper submission. **Applicants that do NOT receive invitations from the Government to submit a Proposal are NOT eligible to submit Proposals and will NOT receive any feedback or a "debriefing" on their Whitepaper.** Applicants invited to submit Proposals will receive feedback on their Whitepaper in order to improve their Proposal submissions. **If Applicants have NOT submitted a Whitepaper, they are NOT eligible to submit a Proposal for consideration for funding.**

1. Address to Request Application Package

This PA may be accessed from the following: Grants.gov (www.grants.gov)

Amendments, if any, to this PA will be posted to these websites when they occur. Interested parties are encouraged to periodically check these websites for updates and amendments.

2. Content and Format of Application Submission

The application process is in two stages as follows:

Whitepapers. Applicants are responsible for submitting electronic Whitepapers so as to be received at the Government site indicated in the PA no later than the date and time specified in **PART II.D.3.** Whitepapers shall be emailed to nikolaos.georgakopoulos.civ@mail.mil and must include a subject line of

"WHITEPAPER – IoBT CRA" in order for the Whitepaper to be properly received. When sending electronic files, the Applicant shall account for potential delays in file transfer from the originator's computer server to the Government website/computer server. Applicants are encouraged to submit their responses early to avoid potential file transfer delays due to high demand or problems encountered in the course of the submission.

Acceptable evidence to establish the time of receipt at the Government site includes documentary and electronic evidence of receipt maintained by the agency. All submissions shall be emailed before the cutoff time/date in order to be considered – NO exceptions.

If an emergency or unanticipated event interrupts normal Government processes so that Whitepapers cannot be received at the site designated for receipt by the date and time specified, then the date and time specified for receipt will be deemed to be extended to the same time of day specified in the PA on the first work day on which normal Government processes resume.

Whitepapers sent by any other means (e.g. submitted to other email addresses, hand-carried, postal service mail, commercial carrier or fax) will not be considered. Applicants will receive an email confirmation that their Whitepaper has been received.

Proposals. UPON INVITATION ONLY, Proposals shall be submitted electronically through the www.grants.gov portal. Proposals sent by fax or email will not be considered. Proposals sent by organizations that have NOT been provided an invitation to do so will NOT be considered. Applicants are responsible for submitting electronic Proposals so as to be received at the Government site indicated in the PA no later than the date and time specified in **PART II.D.3.**

Registration Requirements for www.grants.gov:
Each organization that desires to submit applications via Grants.Gov must complete a one-time registration. There are several one-time actions your organization must complete in order to submit applications through Grants.gov (e.g., obtain a Unique Entity Identifier, register with the System for Award Management (SAM), register with the credential provider, register with Grants.gov and obtain approval for an AOR to submit applications on behalf of the organization). To register please see http://www.grants.gov/web/grants/applicants/organization-registration.html. Please note the registration process for an Organization or an Individual can take between three to five business days or as long as four weeks if all steps are not completed in a timely manner.

Questions: Questions relating to the registration process, system requirements, how an application form works, or the submittal process must be directed to Grants.gov at 1-800-518-4726 or support@grants.gov.

Whitepapers:

Whitepapers shall be submitted in Adobe Portable Document Form (PDF) with the following Formatting:

- Page size when printed: 8 ½ x 11 inches
- Margins: 1 inch minimum
- Spacing and Page Numbers: At least single-spaced with numbered pages utilizing one side per page.
- Font: Times New Roman, no smaller than 11 point. Graphic presentations, including tables, while not subject to the same font size and spacing requirements, shall have spacing and text that is easily readable.
- Page Limits. Whitepapers shall not exceed the stipulated page limits. Pages in excess of the page limits will be removed and not evaluated.

Whitepapers will consist of:

- **Project Summary/Abstract (limit 2 pages)**. A summary of the Consortium team, research program and collaboration plans.

- **Research Program (limit 25 pages)**. The Whitepaper should include an overview of the research strategy to be employed to advance the state-of-the-art in IoBT; a short description and justification for 2-, 5-, and 10-year research goals of the proposed effort; and a short technical discussion stating the background and objectives of the proposed research, the overall technical approaches to be pursued, the potential techniques to be used to validate the models and theories developed in this CRA. This technical discussion should include a proposed breakdown of research tasks and short description of the technical approaches for each task. A discussion on the relevance of the research, strategy for validation of models, and linkages between research in the RAs and CCRI should be included. Where the Whitepaper proposes research topics outside the scope described in this PA, justification for such variance is required. The Whitepaper should clearly identify specific scientific challenges and research barriers that relate to fundamental understanding of the root cause of difficult IoBT-related problems. The Whitepaper should clearly highlight the innovations proposed and how they may lead to substantial advances in foundational understanding of IoBT-related phenomena and highlight how the proposed research is expected to feed, be fed by, or in some other way link with, research being performed elsewhere within the Consortium. This only covers the Core Research Program and its funding.

- **Collaboration Plan and Program Management (limit 5 pages)**. The Whitepaper must include general information on previous successful relevant collaborations and general plans for how researchers will collaborate within each Research Area and between Research Areas and how this collaboration will result in outcomes and further the goals of the program. The Whitepaper must include a summary of collaboration plans (processes and supporting toolsets), synergies gained from

these collaborations, and examples of how researchers have successfully collaborated in the past and the outcomes. The Whitepaper must include a summary of the overall plan for leadership and management of the Consortium. The Whitepaper must include the identification of the Program Manager, key leadership personnel and an overall plan for leadership, efficient management of the IoBT CRA Program and creation of an effective collaborative environment. The Whitepaper must describe an overall strategy for adjusting the research plans in response to research insights gained, advances in the state of the art, and new collaboration opportunities.

- **Biographical Sketches**. Biographical sketches shall be limited to 1 page per individual, with no limit on the number of individuals. The Whitepaper must include the names, brief biographies, and general availability of the key personnel who will be involved in the research. Such credentials, as documented on the biographical sketches, must include, among others, a record of seminal publications in the scientific literature with a citation index and a record of successful research in the relevant research area(s) of the CRA. For the Program Manager it must provide evidence of successful leadership of collaborative research.
- **Cost Summary Tables**. For the Whitepaper only, two cost estimate tables shall be provided to provide a broad idea of the participant's relative level-of-effort for the Core Program funding only. This information will be used in the evaluation of the research program. One table lists the estimated first year funding by organization for each RA (see Table 1). A column for Other can be used for management or other costs. The final line is to be used for an estimate of costs across the Research Areas addressing the CCRI. Another table lists the estimated funding per organization for each of the five years (see Table 2).

Table 1. Year 1 Budget Estimates by Research Area/CCRI ($K)

Organization	RA 1	RA 1	RA 3	Other	Total
LRO					
Org A					
Org B					
Org C					
Org D					
Org E					
Org F					
Org G					
CCRI Portion					

Table 2. 5-Year Budget Estimates ($K)

Organization	Year 1	Year 2	Year 3	Year 4	Year 5	Total
LRO						
Org A						

Org B						
Org C						
Org D						
Org E						
Org F						
Org G						
Total						

Proposal:

Application forms and instructions will be available at Grants.gov. To access these materials, go to http://www.grants.gov, select "Apply for Grants", and then select "Download an Application Package." Enter the funding opportunity number, W911NF-17-S-0005. REMINDER: Only proposals submitted by Applicants given an invitation to submit a Proposal, after a favorable Whitepaper evaluation, will be considered.

Applicants must complete the mandatory forms and any optional forms (e.g., SF-LLL Disclosure of Lobbying Activities) in accordance with the instructions on the forms and the additional instructions below. The required fields should be completed in accordance with the "pop-up" instructions on the forms. To activate the instructions, turn on the "Help Mode" (icon with the pointer and question mark at the top of the form). Files that are attached to the forms must be in Adobe Portable Document Form (PDF) unless otherwise specified in this announcement.

The following formatting applies to the Proposal:

- Page size when printed: 8 ½ x 11 inches
- Margins: 1 inch minimum
- Spacing and Page Numbers: At least single-spaced with numbered pages utilizing one side per page.
- Font: Times New Roman, no smaller than 10 point. Graphic presentations, including tables, while not subject to the same font size and spacing requirements, shall have spacing and text that is easily readable.
- Page Limits. Proposals shall not exceed the stipulated page limits. Pages in excess of the page limits will be removed and not evaluated.

Form: SF 424 (R&R) (Mandatory). Complete this form first to populate data in other forms. Authorized Organization Representative (AOR) usernames and passwords serve as "electronic signatures" when your organization submits applications through Grants.gov. By using the SF 424 (R&R), Applicants are providing the certification required by 32 CFR Part 28 regarding lobbying.

Form: Research & Related Other Project Information. Complete questions 1 through 6 and attach files.

- **Project Summary/Abstract** (Field 7 on the form) - The Project Summary should be a brief abstract that summarizes the content of the Basic research of the proposal. **The project summary must not exceed 5 pages.** Pages in excess of the page limit may be removed for the evaluation of the proposal.

- **Project Narrative** (Field 8 on the form) - Chapters and Numbers of pages – Field 8 is to contain the chapters set forth below and may not exceed the stipulated page counts for those chapters. Pages in excess of the page limits may be removed for the evaluation of the proposal.

- **Chapter 1: Research Program**. The pages included in Chapter 1 shall be numbered. Applicants are advised that Chapter 1 **shall not exceed 40 pages**, utilizing one side of the page.

  The Proposal should include a discussion of the research strategy to be employed to advance the state-of-the-art in IoBT; a detailed description and justification for 2-, 5-, and 10-year research goals of the proposed effort; and a detailed technical discussion. The technical discussion should include the background and objectives of the proposed research, the technical approaches to be pursued, the validation techniques and metrics to be used to validate the models and theories developed in this CRA, and the parties involved and the level of effort to be employed (demonstrating that researchers are collaborating and substantially and meaningfully engaged in the research efforts). Where the proposal includes research topics not listed in this PA, a rationale must be provided. The Proposal should also clearly:

  - Identify specific scientific challenges and research barriers that relate to fundamental understanding of the root cause of difficult IoBT-related problems and should provide evidence that the proposed technical approaches can address these challenges in a measured approach across the near- and far-term.
  - Explain in substantial detail the specific scientific plans that will be employed, and provide ample evidence that the approaches are likely to substantially advance the underlying science.
  - Highlight the innovations proposed and how they may lead to an understanding of IoBT-related phenomena particularly fundamental laws, theories, and validated models.
  - Show how the proposed research is expected to feed, be fed by, or in some other way link with, research being performed elsewhere within the Consortium and within the ARL.

- **Chapter 2: Collaboration Plan**. The pages included in Chapter 2 shall be numbered. Applicants are advised that Chapter 2 of the proposal **shall not exceed 10 pages**,

utilizing one side of the page. The Proposal must include plans for how researchers will collaborate within each Research Area and across the Research Areas and describe how this collaboration will further the goals of the program. The Proposal must describe the processes and toolsets to facilitate collaboration and the document/information controls to be employed. The Proposal must describe the strategy for collaborating with ARL and propose collaborative opportunities with ARL. The Proposal must include examples of how researchers have successfully collaborated previously in similar programs.

- **Chapter 3: Program Management**. The pages included in Chapter 3 shall be numbered. Applicants are advised that Chapter 3 of the proposal **shall not exceed 10 pages**, utilizing one side of the page. The Proposal must include a detailed plan for leadership and efficient management of the IoBT CRA Program, creation of a collaborative environment, and organizational structures. The Proposal must identify metrics for success, how they will be used, and how they will further the goals of the program. Where available, evidence for the success of these strategies is to be described. The Proposal must describe approaches to adjusting the research plans in response to research insights gained, advances in the state of the art, and new collaboration opportunities. The Proposal must include a strategy for identifying, establishing, and exploiting collaborations with other related ARL research programs. The Proposal must describe processes for external communication of research outputs.

- **Chapter 4: Biographical Sketches.** Biographical sketches **shall be limited to two (2) pages per individual**, with no limitation on the number of individuals. The Proposal must include the names, biographies, and availability of the key personnel who will be involved in the research and management of the program. Such credentials, as documented on the biographical sketches, must include, among others, a record of seminal publications in the scientific literature with a citation index and a record of successful research in areas relevant to the IoBT CRA. For the Program Manager it must provide evidence of successful leadership of collaborative research. The proposal is to demonstrate how the aggregate of skills/expertise across the Consortium provides the required breadth and depth to effectively carry out the proposed program of research.

- **Bibliography and References Cited** (Field 9 on the form) - Attach a listing of applicable publications cited in above sections.

- **Facilities and Other Resources** (Field 10 on the form) - The Applicant is to include a listing of facilities and other resources available to support the proposal. Attach this information at Field 10. The Proposal must include a description of the facilities to be used for the research and experiments, a description of who will have access to these facilities, and how these facilities will enhance the research efforts proposed. Where new research facilities are to be created for the purposes of the IoBT CRA, the development and verification plans are to be described.

- **Equipment** (Field 11 on the form) - The Applicant is to include a listing of equipment available to support the proposal. Any Government equipment

necessary for performance is to be clearly identified. Attach this information at Field 11.

- **Other Attachments** (Field 12 on the form) are as follows:

  1. Attached the completed Proposal Cover Sheet. (See **PART II.D.6** below)
  2. Attached the completed certifications. (See **PART II.F.2** below)
  3. Attach any exceptions or conditions to the Model Cooperative Agreement. (A model CA will be provided to Applicants with their invitation to submit a Proposal.)
  4. Attach the signed Articles of Collaboration for all Members. (A model AoC will be provided to Applicants with their invitation to submit a Proposal.)
  5. Attach the Cost Proposal. **The Cost Proposal must include 2 separate budgets for the first five years of performance: one for the Core Research Program and one for the Enhanced Research Program. The Cost Proposal for the Core Research Program MUST address all requirements for the Core Research Program. (The Recipient will be requested to provide a complete cost proposal for the optional five-year period of performance as part of the evaluation to be completed prior to making the decision concerning this optional period)** The cost portion of the proposal shall contain cost estimates sufficiently detailed for meaningful evaluation. For budget purposes, assume a performance start date of 1 October 2017**.** The proposed amounts shall not exceed the funding ceilings identified for the Core Research Program and Enhanced Research Program of this PA. The co.st proposal should include the following budget elements and support

     - Direct Labor. Individual labor category or person, with associated labor hours and unburdened direct labor rates. For each person or position, provide the following information:

       i. The basis for the direct labor hours or percentage of effort (e.g., historical hours or estimates);

       ii. The basis for the direct labor rates or salaries. Labor costs should be predicted upon current labor rates or salaries. These rates may be adjusted upward for forecast salary or wage cost-of-living increases that will occur during the agreement period. The cost proposal should separately identify the rationale applied to base salary/wage for cost-of-living adjustments and merit increases. Each must be fully explained;

       iii. The portion of time to be devoted to the proposed research, management activities, divided between academic and non-academic (summer) terms, when applicable;

       iv. The total annual salary charged to the CRA; and

v. Any details that may affect the salary during the project, such as plans for leave and/or remuneration while on leave.

- Indirect Costs. Fringe benefits, overhead, G&A, etc. (must show base amount and rate). Include a copy of current rate agreements.

- Costs Share. Amounts or percentages, expected benefits to the CRA as a result, and parameters institutional parameters for providing cost share.

- Travel. Number of trips, destination, duration, etc. Justify and include basis for costs. This should include anticipated travel between Consortium Member locations and ARL sites as well as conference attendance.

- Subaward. A Cost Proposal, as detailed as the Applicant's Cost Proposal, will be required to be submitted by each proposed subrecipient.

- Consultant. Provide consultant agreement or other document that verifies the proposed loaded daily/hourly rate. Include a description of the nature of and the need for any consultant's participation. Provide budget justification.

- Materials. Specifically itemized with costs or estimated costs. An explanation of any estimating factors, including their derivation and application, shall be provided. Include a brief description of the Applicant's procurement method to be used (competition, engineering estimate, market survey, etc.). Justify.

- Other Directs Costs. Particularly any proposed items of equipment or facilities. Equipment and facilities generally must be furnished by the recipient (justifications must be provided when Government funding for such items is sought). Include a brief description of the Applicant's procurement method to be used (competition, engineering estimate, market survey, etc.). Justify.

- Profit/Fee: Profit/fee is not allowed for the recipient or subrecipient to an assistance instrument, where the principal purpose of the activity to be carried out is to stimulate or support a public purpose (i.e., to provide assistance), rather than acquisition (i.e., to acquire goods and services for the direct benefit of the Government). A subaward is an award of financial assistance in the form of money, or property in lieu of money, made under a DoD grant or cooperative agreement by a recipient to an eligible subrecipient. The term includes financial assistance for substantive program performance by the subrecipient of a portion of the program for which the DoD grant or cooperative agreement was made. It does not include the recipient's procurement of goods and services needed to carry out the program.

- Cost of Money (COM): If cost of money is proposed, a completed Contract Facilities Capital Cost of Money (FCCM) (DD Form 1861) is required.

All entities included in the cost proposal are to provide detailed information on all cost elements included in their proposed budgets as part of the proposal submission process. However, it is recognized that some entities may choose to submit their proprietary rate information directly to the Government in lieu of providing such information to the LRO for inclusion in the cost proposal submitted through grants.gov. In such a case, a separate submission can be made directly to the Government. Such a submission MUST include the PA Number, i.e. W911NF-17-S-0005, and the name of the LRO associated with the proposal on the mailing envelope submitted to the following address:

U.S. Army Contracting Center – Aberdeen Proving Ground
RTP Division
ATTN: W911NF-17-S-0005
P.O. Box 12211
800 Park Office Drive, Suite 4229
Research Triangle Park, NC 27709

NOTE: All such separate submissions must arrive NLT than the due date and time specified in **PART II.D.3** for the proposal submission through grants.gov to be considered. Further, for all such submissions summary cost information must be provided to the LRO for the grants.gov submission that is sufficient in detail for the Government to use in the evaluation of the cost proposal for cost realism, and can be clearly mapped to the proprietary rate information submitted directly to the Government.

- **SF-LLL: Disclosure of Lobbying Activities**. If applicable, attach a complete SF- LLL at Field 11 of the R&R Other Project Information form. Applicability: If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the grant/cooperative agreement, you must complete and submit Standard Form - LLL, "Disclosure Form to Report Lobbying."

3. Submission Dates and Times

Whitepapers are due by 3:00pm (local time in North Carolina, USA) on 8 May 2017. An email receipt will be provided for each Whitepaper submission received.

Proposals are expected to be due in 27 July 2017. (NOTE: The date and time of submission, as well as any additional instructions, will be provided with the invitation to submit a Proposal. As a reminder, only the most highly rated Whitepapers will receive an invitation to submit a Proposal.)

After a proposal is submitted through Grants.gov, the Authorized Organization Representative (AOR) will receive a series of three emails. It is extremely important that the AOR watch for and save each of the e-mails. Applicants will know that the proposal has been properly received when the AOR receives e-mail Number 3. The three emails are:

- Number 1. The AOR will receive a confirmation page upon completing the submission to Grants.gov and will receive a tracking number. This confirmation page is a record of the time and date stamp for the submission.
- Number 2. The AOR will receive an email indicating that the proposal has been validated by Grants.gov within a few hours of submission. (This means that all of the required fields have been completed.)
- Number 3. The third notice is an acknowledgment of receipt in email from Grants.gov. The email is sent to the AOR for the institution. The email notes that the proposal has been received. **THE PROPOSAL IS NOT CONSIDERED PROPERLY RECEIVED UNTIL THE AOR RECEIVES EMAIL #3.**

4. Intergovernmental Review - Not applicable

5. Funding Restrictions - See **PART II.A** above.

6. Other Submission Requirements

The following Proposal Cover Sheet is required to be submitted by each Applicant:

PROPOSAL COVER SHEET

1. **Information concerning the LRO (points of contact (POC)):**

   Research POC: _____
   Phone No.: _____
   Fax No.: _____
   Email Address _____

   Business POC _____
   Phone No.: _____
   Fax No.: _____
   Email Address: _____

2. **List the names and relationships of all organizations included in the Proposal:**

   LRO _____
   LRAOs - Other Consortium Member(s)
   _____
   Subawardee(s) _____

3. **Provide a point of contact for each organization included in the Cost Proposal. These individuals may be contacted for questions concerning the Cost Proposal:**

   Organization: _____
   POC: _____
   Phone No.: _____
   Email Address _____

4. **Signature of one person for the proposed LRO, and one person from each proposed LRAO (Other Consortium Members), authorized to submit a Proposal and bind that organization:** (These signatures may be provided on separate sheets.)

   Organization Name: _____
   Signature: _____
   Type Name/Title: _____
   Date (Proposal): _____

E. APPLICATION REVIEW INFORMATION

1. Evaluation Criteria

Whitepaper Evaluation Criteria. The following represents the evaluation criteria for this PA:

Factors 1.a, 1.b and 1.c: Scientific Merit and Relevance: (This includes Factor 1.a for Research Area 1, Factor 1.b for Research Area 2 and Factor 1.c for Research Area 3.) Evaluation of this factor will concentrate on the overall scientific and technical merit, military relevance, and innovation of the proposed research in light of the IoBT state-of-the-art. The scientific merit will be evaluated with regard to each of the three Research Areas of the CRA. The Cross Cutting Research Issue will be evaluated as an integral part of each of the three Research Areas and, therefore, will not be evaluated separately. Each Research Area will be assessed with regard to its overall scientific merit, innovation, potential degree of generality of the models, and strategy for validation. Evaluation of this factor will also concentrate on the long term relevance of the proposed research of each Research Area and the likelihood this proposed research will address scientific challenges and research barriers facing the Army.

Factors 2.a, 2.b and 2.c: Experience and Qualifications of Scientific Staff: (This includes Factor 2.a for Research Area 1, Factor 2.b for Research Area 2 and Factor 2.c for Research Area 3.) Evaluation of this factor will concentrate on the relevant qualifications, capabilities, availability, accomplishments, and experience of the Applicant's proposed research personnel as an indication of their ability to achieve the proposed technical objectives related to the proposed efforts for each of the three Research Areas. The Cross Cutting Research Issue will be evaluated as an integral part of each of the three Research Areas and, therefore, will not be evaluated separately.

Factor 3: Collaboration and Program Management: Evaluation of this factor will concentrate on the Applicant's strategies, plans and experience in fostering collaborative research and managing collaborative research programs. Evaluation of this factor will be based on evidence of previous successful relevant collaborative efforts and the Applicant's commitment and plans for collaboration. Evaluation of this factor will focus on the Program Manager's technical leadership and experience in managing large collaborative research programs and the Applicant's plans to meet the requirements of the overall management concept. This factor includes plans for an environment to foster collaboration and efforts to bring about a unity of vision for the Consortium and drive for results and benefits.

Relative Importance of the Evaluation Factors: The evaluation factors are listed in descending order of importance with Factor (1) being approximately equal importance with Factor (2) and Factor (3) combined, and Factors (2) and (3) being approximately equal.

Proposal Evaluation Criteria. The following represents the evaluation criteria for this PA:

Factors 1.a, 1.b and 1.c: Scientific Merit and Relevance: (This includes Factor 1.a for Research Area 1, Factor 1.b for Research Area 2 and Factor 1.c for Research Area 3.) Evaluation of this factor will concentrate on the overall scientific and technical merit, creativity, military relevance, and innovation of the proposed research in light of the IoBT state-of-the-art. The scientific merit will be evaluated with regard to each of the three Research Areas of the CRA. The Cross Cutting Research Issue will be evaluated as an integral part of each of the three Research Areas and, therefore, will not be evaluated separately. Each Research Area will be evaluated with regard to its overall scientific merit, creativity, innovation, degree of generality of the models, validation techniques, and likelihood of substantially advancing the current state-of-the-art in IoBT. Evaluation of this factor will also concentrate on the long term relevance of the proposed research of each Research Area and the likelihood this proposed research will address scientific challenges and research barriers facing the Army.

Factors 2.a, 2.b and 2.c: Experience and Qualifications of Scientific Staff and Quality of Research Facilities: (This includes Factor 2.a for Research Area 1, Factor 2.b for Research Area 2 and Factor 2.c for Research Area 3.) Evaluation of this factor will concentrate on the qualifications, capabilities, availability, proposed level of effort, and experience of both the Applicant's proposed research personnel (individually and as a whole), their relevant past accomplishments, and their ability to achieve the proposed technical objectives related to the proposed efforts for each of the three Research Areas. The Cross Cutting Research Issue will be evaluated as an integral part of each of the three Research Areas and, therefore, will not be evaluated separately. Key personnel are expected to be substantially and meaningfully engaged in the research and the proposed level of effort for key personnel should be commensurate with and demonstrate such. The extent to which the Applicant's proposed facilities and equipment will contribute to the accomplishment of the proposed research in each of the three Research Areas will be evaluated including the nature, quality, relevance, availability, and access to state-of-the-art research facilities and equipment.

Factor 3: Collaboration: Evaluation of this factor will concentrate on the Applicant's strategies, plans and experience in fostering collaborative research and managing collaborative research programs as set forth in this PA. Evaluation of this factor will include evidence of previous successful collaborative efforts, the Applicant's commitment and plans for collaboration within the Alliance, and the synergistic value of the collaborations among researchers.

Factor 4: Program Management. Evaluation of this factor will include the adequacy of the overall management plan, internal team structures, and composition with respect to achieving the research goals of the program. These approaches should be lightweight and will be evaluated for their flexibility to minimize overhead, yet ensure research relevance and proper oversight. Evaluation of this factor will also include the Applicant's general proposed plans should Enhanced Funding become available. Where available, evidence for

the success of these strategies is to be described. Evaluation of this factor will include a focus on the Program Managers' technical leadership and experience in managing large collaborative research programs and the Applicant's plans to meet the requirements of the overall management concept included in the PA.

Factor 5: Cost. While this area will not be weighted, evaluation of this area will consider cost realism, cost reasonableness, and affordability within funding constraints. The Government may make adjustments to the cost of the total proposed effort as deemed necessary to reflect what the effort should cost. These adjustments will consider the task undertaken and approach proposed. These adjustments may include upward or downward adjustments to proposed labor hours, labor rates, quantity of materials, price of materials, overhead rates and G&A, etc.

Relative Importance of the Evaluation Factors: The evaluation factors are listed in descending order of importance with Factors 5 not be weighted. Factor (1) is approximately equal importance with Factor (2) and Factor (3) combined. Factor (2) is approximately twice as important as Factor (3) and three times as important as Factor (4).

2. Review and Selection Process

All timely and compliant Whitepaper submissions will be evaluated in accordance with the evaluation criteria set forth in this PA. Whitepapers are expected to be evaluated by a group of qualified scientists and managers from the Government. However, the Government reserves the right to have Whitepapers evaluated by subject matter experts outside the Government. Should such outside evaluators be used, they will be required to sign a non-disclosure statement before being provided access to Whitepapers.

Only the most highly rated Whitepapers will receive an invitation to submit a Proposal as well as feedback on the Whitepaper. **Applicants that do NOT receive an invitation from the Government to submit a Proposal are NOT eligible to submit a Proposal and will NOT receive any feedback or "debriefing."** Applicants not receiving an invitation to submit proposals will be informed of such via email following the Whitepaper evaluations.

All timely proposal submissions from Applicants receiving an invitation to submit a proposal will be evaluated in accordance with the evaluation criteria set forth in this PA. All information necessary for the review and evaluation of a proposal must be contained within the proposal. No other material will be provided to those evaluating proposals. An initial review of the proposals will be conducted to ensure compliance with the requirements of this PA. Failure to comply with the requirements of the PA may result in a proposal receiving no further consideration for award.

Whitepapers and Proposals that are in compliance with the requirements of the PA will be evaluated in accordance with merit based, competitive procedures. These procedures will

include evaluation factors that will be evaluated using an adjectival and color rating system as follows:

> **OUTSTANDING (blue):** The proposal is evaluated as outstanding for this factor. The proposal includes **one or more significant strengths that are not offset by weaknesses.**
>
> **GOOD (purple):** The proposal is evaluated as good for this factor. The proposal includes **some strengths that are not offset by weaknesses.**
>
> **ACCEPTABLE (green):** The proposal is evaluated as acceptable for this factor. **Any strengths and weaknesses in the proposal balance out.**
>
> **MARGINAL (yellow):** The proposal is evaluated as marginal for this factor. While the proposal **may or may not contain some strengths, and strengths are more than offset by any weakness or weaknesses.**
>
> **UNACCEPTABLE (red):** The proposal is evaluated as unacceptable for this factor. While the proposal **may or may not contain some strengths, and strengths are offset by any significant weakness or weaknesses.**

A Review Team, consisting of a qualified group of scientists, managers and business specialists, will evaluate the Whitepapers and Proposals and provide the results of that evaluation to the decision maker for the Government. The decision maker will make both decisions concerning the Whitepaper down selection and award selection.

After Proposals are evaluated, the Government reserve the right to establish a competitive range and enter into negotiation discussions with those Applicants within the competitive range or award without discussions. Negotiation discussions may be conducted telephonically or face-to-face at the Applicant's facility. Any such meeting will be coordinated with the Applicant at the appropriate time. If a competitive range is established for negotiation purposes, then all Applicants in the competitive range will be invited to submit Final Proposal Revisions (FPRs). If FPRs are received, they will be evaluated using the same evaluation criteria as was used to evaluate the initial Proposals.

Award will be based on an integrated assessment of each Applicant's ability to satisfy the PA requirements. The Government will make award to the Applicant, whose proposal conforms to the PA that offers the best value to the Government, cost and other factors considered. Further, award may be made to other than the Applicant who offers the lowest cost Proposal. The ARL reserves the right not to make an award should no acceptable Proposal be submitted.

3. Recipient Qualification

i. The Grants Officer is responsible for determining a recipient's qualification prior to award. In general, a Grants Officer will award grants or cooperative agreements only to qualified recipients that meet the standards at 32 CFR 22.415. To be qualified, a potential recipient must:

> (1) Have the management capability and adequate financial and technical resources, given those that would be made available through the grant or cooperative agreement, to execute the program of activities envisioned under the grant or cooperative agreement;
>
> (2) Have a satisfactory record of executing such programs or activities (if a prior recipient of an award);
>
> (3) Have a satisfactory record of integrity and business ethics; and
>
> (4) Be otherwise qualified and eligible to receive a grant or cooperative agreement under applicable laws and regulations.

Applicants are requested to provide information with proposal submission to assist the Grants Officer's evaluation of recipient qualification. For the purposes of this PA, the recipients are identified as all Consortium Members, including the LRO and all LRAOs.

ii. In accordance with OMB guidance in parts 180 and 200 of Title 2, CFR, it is DoD policy that DoD Components must report and use integrity and performance information in the Federal Awardee Performance and Integrity Information System (FAPIIS), or any successor system designated by OMB, concerning grants, cooperative agreements, and TIAs as follows:

If the total Federal share will be greater than the simplified acquisition threshold on any Federal award under a notice of funding opportunity (see 2 CFR 200.88 Simplified Acquisition Threshold):

> (1) The Federal awarding agency, prior to making a Federal award with a total amount of Federal share greater than the simplified acquisition threshold, will review and consider any information about the applicant that is in the designated integrity and performance system accessible through SAM (currently FAPIIS) (see 41 U.S.C. 2313);
>
> (2) An applicant, at its option, may review information in the designated integrity and performance systems accessible through SAM and comment on any information about itself that a Federal awarding agency previously entered and is currently in the designated integrity and performance system accessible through SAM;

(3) The Federal awarding agency will consider any comments by the applicant, in addition to the other information in the designated integrity and performance system, in making a judgment about the applicant's integrity, business ethics, and record of performance under Federal awards when completing the review of risk posed by applicants as described in 2 CFR 200.205 Federal awarding agency review of risk posed by applicants.

F. AWARD ADMINISTRATION INFORMATION

1. Award Notices

Should your Proposal be selected for award, you will be contacted telephonically or via email by the Grants Officer or his/her representative. At that time, the Applicant will be asked to execute the CA. Award is not officially made until the CA is signed by each Member of the Consortium (included in the selected Applicant's proposal) and the Grants Officer.

2. Administrative and National Policy Requirements

Please refer to the DoD Research and Development General Terms and Conditions at http://www.onr.navy.mil/Contracts-Grants/submit-proposal/grants-proposal/grants-terms-conditions.aspx for national policy requirement that may apply.

3. Reporting

Reporting requirements for the CA are contained in the Model CA which will be provided to all Applicants that are invited to submit a proposal.

G. AGENCY CONTACTS

Questions or comments concerning this PA will be posted through the CRA website at www.arl.army.mil/cra/IoBT/. Questions and comments should be concise and to the point. In addition, the relevant part and paragraph of the PA should be referenced. Responses to questions received will be posted to the CRA website for the benefit of all interested parties. Should an Applicant have questions they believe are of a proprietary nature, the Applicant must clearly state so in the question when posed. Answers to questions of a proprietary nature will be provided via email directly to the poser of the question. A location on the website will be provided for potential Applicants to post their availability for teaming with others.