U.S. ARMY RESEARCH LABORATORY

BROAD AGENCY ANNOUNCEMENT

FOR

CYBER SECURITY
APPLIED RESEARCH & EXPERIMENTATION PARTNER

W911NF-14-R-0001

07 February 2014

ISSUED BY:
U.S. Army Contracting Command-Aberdeen Proving Ground
Research Triangle Park Division
4300 S. Miami Blvd.
Durham, NC 27703
I. OVERVIEW OF FUNDING OPPORTUNITY

A. REQUIRED OVERVIEW CONTENT

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

2. **Issuing Acquisition Office:** U.S. Army Contracting Command – Aberdeen Proving Ground, Research Triangle Park Division, 4300 S. Miami Blvd., Durham, NC 27703

3. **Funding Opportunity Title:** Cyber Security (CS) Applied Research and Experimentation Partner (AR&EP) Broad Agency Announcement (BAA)

4. **Announcement Type:** Initial

5. **Funding Opportunity Number:** W911NF-14-R-0001

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

7. **Dates:** The following is a summary of the events and dates associated with the CS AR&EP BAA:

<table>
<thead>
<tr>
<th>EVENT</th>
<th>ESTIMATED DATE/TIMEFRAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA released</td>
<td>7 February 2014</td>
</tr>
<tr>
<td>Information Webinar</td>
<td>18 February 2014</td>
</tr>
<tr>
<td>Whitepapers due</td>
<td>5 March 2014, 3:00PM (EST)</td>
</tr>
<tr>
<td>Whitepaper Feedback/Invitation to Submit Full Proposal for Highly Rated Whitepapers</td>
<td>April 2014</td>
</tr>
<tr>
<td>Full Proposals due</td>
<td>June 2014</td>
</tr>
<tr>
<td>Award</td>
<td>August 2014</td>
</tr>
</tbody>
</table>

B. EXECUTIVE SUMMARY

This Broad Agency Announcement (BAA) is issued under section 6.102(d)(2), Use of Competitive Procedures, of the Federal Acquisition Regulation (FAR), which provides for the competitive selection of research Proposals. Proposals submitted in response to this BAA and selected for award are considered to be the result of full and open competition and in full compliance with the provision of Public Law 98-369, "The Competition in Contracting Act of 1984" and subsequent amendments.

NOTE: Under this BAA, the Government is NOT looking for whitepapers or Proposals for existing Cyber solutions to employ, NOR is the Government looking for whitepapers or Proposals to select a contractor to perform a broad range of cyber related services as required by the Government. Whitepapers and invited Proposals in response to this BAA will be evaluated ONLY if they include innovative approaches for scientific study and experimentation.
directed toward advancing the state of the art or increasing knowledge and understanding in the areas of scientific interest cyber security research included in this BAA. Further, each Whitepaper and invited proposal received will be subject to a scientific or peer review as delineated later in this document.

1. Background:

The US Army has a critical need to develop a theoretical and scientific understanding of the cyber domain. Past basic research approaches aimed at understanding specific cyber phenomena in narrowly focused studies did not consider the inter-disciplinary nature of cyber systems. The US Army Research Laboratory (ARL) has recently established a Cyber Security Collaborative Research Alliance (Cyber CRA) that seeks to advance the theoretical foundations of cyber security in the context of Army networks, making fundamental advances in understanding cyber phenomena. The Cyber CRA couples multi-disciplinary internal research, analysis, and operations with extramural research and collaborative ventures. A cooperative agreement was awarded for the joint collaborative efforts of the Cyber CRA to a multi-disciplinary research team, which includes academic and government partners.

Under the Cyber CRA, ARL has identified three interrelated aspects, or Research Areas (RAs), of cyber security, that when jointly studied will advance the theoretical foundations of cyber science in the domains specific to Army networks. In addition to these three RAs, advancing the fundamental understanding of the science of cyber requires a trans-disciplinary approach that takes into account the human element of the network. This human element of the network is being addressed in the Cross-Cutting Research Issue (CCRI), Psychosocial Effects, and is being jointly studied in the context and the constraints of the three RAs. The RAs and CCRI for the Cyber CRA are as follows:

- **Risk.** The Risk Research Area seeks to develop theories and models that relate fundamental properties and features of dynamic risk assessment algorithms to the fundamental properties of dynamic cyber threats, Army’s networks, and defensive mechanisms.

- **Detection.** The Detection Research Area seeks to develop theories and models that relate properties and capabilities of cyber threat detection and recognition processes/mechanisms to properties of a malicious activity and of properties of Army networks.

- **Agility.** The Agility Research Area seeks to develop theories and models to support planning and control of cyber maneuver (i.e., “maneuver” in the space of network characteristics and topologies) that would describe how control and end-state of the maneuver are influenced by fundamental properties of threats, such as might be rapidly inferred from limited observations of a new, recently observed threat.

- **CCRI: Psychosocial Effects.** Although comprehensive monitoring and network adaptation are far beyond the ability of human defenders to perform manually, it must be
assumed that network analysts charged with maintaining and defending the network and the Soldiers who rely on the network will need to be kept aware of the threat and of any recommended or implemented changes in the network that may affect their ability to carry out their mission. A theoretical understanding of the social-cognitive factors that affect decision-making of the user/Soldier, defender/analyst, and adversary needs to be developed.

In order to successfully advance the fundamental understanding of cyber phenomena, the RAs must be linked and studied jointly under the Cyber CRA.

The networks and information systems deployed and utilized by the US Army are unique, highly dynamic and complex in nature. The Army leverages strategic and tactical assets that are connected to the Army’s cyber domain, to include software defined radios, sensing devices, and computing devices embedded in vehicles, which can make securing the network difficult. The Army’s growing reliance on information systems and networks ultimately increases the attack surface available to adversaries, both internally and externally, to disrupt, deny, and degrade Army operations. The nature and sophistication of attacks targeting Army networks will continue to increase in the foreseeable future and will not only target individual systems and networks, but also the humans operating on the systems and networks. To defend such a complex environment, a fundamental knowledge of cyber security is necessary to minimize, monitor, manage, and maneuver in the cyber domain. The Cyber CRA will produce mathematically formulated models and theories that can characterize the overall security of the Army’s complex networks in the presence of sophisticated threats and a variety of defensive mechanisms. The ability to experimentally validate the models and theories developed by the Cyber CRA utilizing relevant data (simulated and operational) is critical to advancing the fundamental understanding of cyber security.

To provide a foundation to begin studying the stated cyber security research areas and human effects in the Army’s highly complex and dynamic tactical and strategic environments, the Cyber CRA has developed an operations model. It forms the conceptual core of the Cyber CRA technical approach. The operations model provides a formal structure for reasoning about cyber maneuvers and security goals and strategies. These models are decomposable in ways that make analysis tractable (both formal and otherwise). Operations are broken into subtasks that progress temporally to a final mission success end-state. Each subtask is defined by a set of security requirements, security outcomes (the change in security state consequent of the subtask completion), risks, costs, and payouts. This approach allows one to reason about strategies that achieve goals while maintaining the security requirements of the mission.

The purpose of this Broad Agency Announcement (BAA) is to select an Applied Research and Experimentation Partner (AR&EP) for the Cyber CRA. The goal is for the AR&EP to bridge the cyber security knowledge gap between Army strategic and tactical cyber domains by developing an innovative applied research and experimentation program that can assess the validity of the Cyber CRA basic research while measuring the psychosocial effects on operators. The
AR&EP efforts to enhance the Cyber CRA are expected to be categorized by the following roles/types of efforts:

- **Role 1**: Research and develop new and innovative approaches and processes to evolve basic (6.1) research results to experimental validation (6.2 applied research), as well as perform the identified experimentation in simulated, realistic, and operationally relevant environments. Provide experimental validation of the models and theories developed by the Cyber CRA 6.1 (basic) research; design and execute a comprehensive series of innovative experiments; and return experimental results to ARL & Cyber CRA researchers, as classification permits.

- **Role 2**: Perform applied research into innovative approaches to sufficiently represent the complexity of the Army’s cyber domain, its dynamics, and cyber security events in test beds; develop processes and approaches with the goal of improving the accuracy, impact, realism, repeatability, predictability, and relevance of the experimental processes. Identify new and innovative means to design experiments.

- **Role 3**: Join and participate in the Cyber CRA as a Consortium Member and collaborate with Cyber CRA researchers on the 6.1 (basic) research. Actively collaborate with Cyber CRA researchers in documenting the results of Cyber CRA and AR&EP efforts in technical publications, such as journal and conference papers and reports, at an appropriate classification level. Develop approaches and processes for the migration of research results from the Cyber CRA basic research (6.1) to the AR&EP experimentation, and the migration of AR&EP experimentation back to the Cyber CRA basic researchers. Ensure an effective feedback loop from the experimental validation while maintaining consideration for the classification of the experimental results and the potentially uncleared status of the majority of the researchers as well as the involvement of foreign nationals.

These Roles/Types of Efforts are discussed further in the Programmatic Strategy and Research Strategy Sections set forth later in this document.

2. **Award Instruments**: As a result of this BAA, the Offeror selected for award will: (1) be awarded a procurement contract to perform the AR&EP efforts; and (2) be added to the existing Cyber CRA cooperative agreement award as a Consortium Member.

The contract award vehicle for the AR&EP efforts will be a single indefinite delivery/indefinite quantity (IDIQ) contract as defined at 10 U.S.C. 2304A for the execution of the program. Under this IDIQ contract, Task Orders will be issued for the applied research, validation and experimentation efforts, based on the Offeror’s innovative approach to the program requirements and how that approach manifests itself during performance, given the interaction with the Cyber CRA and the opportunities presented as a result of performance. Each individual Task Order Proposal will be subject to a scientific or peer review prior to the issuance.
of each Task Order. Immediately after contract award the first Task Order is expected to be issued as described later in this document.

In additional to the award of the AR&EP contract, the Offeror selected for award under this BAA will be required to join the Consortium for the Cyber CRA. This means the selected Offeror will be required to be a signatory to the Cooperative Agreement (and any/all modifications issued at that time) and also a signatory to the Articles of Collaboration which govern how the members of the Consortium engage each other related to membership, intellectual property and other consortium-related issues. Further, the Cyber CRA Consortium will allocate $350K per year of the annual Cyber CRA funding for the AR&EP member’s participation in the Cyber CRA basic research program. (NOTE: Offerors invited to submit proposals under this BAA will be provided information concerning the Cyber CRA Cooperative Agreement and Articles of Collaboration with their invitation to submit a Proposal.)

In summary, the Cyber CRA is a cooperative agreement with some funding set aside for the selected AR&EP to collaborate on basic research tasks. Under the contract funds will be provided for the AR&EP to provide testbeds, design and conduct experiments to validate theories and models, provide feedback to the Cyber CRA Members. To clarify, when the work flows from the AR&EP to the Cyber CRA Members, funding comes from the contract for this BAA. Conversely, when the work flows from the Cyber CRA Members to the AR&EP, funding is provided by the cooperative agreement.

3. Proposal Submission: The application process consists of a Whitepaper stage and a Proposal stage. The purpose of a Whitepaper is to minimize the effort associated with the production of detailed Proposals for those Offerors 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. An Offeror that does NOT receive an invitation from the Government to submit a Proposal will NOT be eligible to submit a Proposal and will NOT receive feedback or a “debriefing” of their White paper. An Offeror invited to submit a Proposal will receive feedback on their Whitepaper to improve their Proposal submission. An Offeror invited to submit a Proposal may also be afforded an opportunity to visit one or more Government facilities that may be engaged during performance under any award resulting from this BAA. If an Offeror has NOT submitted a Whitepaper, the Offeror may NOT submit a Proposal for consideration for funding. Offerors should note that there are deadlines, page limitations and other requirements associated with the submission process, for both the Whitepaper and the Proposal.

4. Information Webinar and Questions on the BAA: On 18 February 2014, at 1:30PM EST, there will be an information webinar concerning this BAA. There is no requirement for Offerors to participate in this webinar. During this webinar, presentations will be made by the Government to discuss the various requirements in this BAA. Further, timely questions received concerning the BAA are expected to be addressed during this webinar.
Offerors electing to participate in this webinar can register at: http://www.arl.army.mil/reviews/arep.

Offerors with questions concerning this BAA can submit them at: http://www.arl.army.mil/www/default.cfm?page=2342.

In order for questions to be addressed during the Webinar they need to submitted by 11:59PM EST, 13 February 2014. Answers to any questions received after that time will be provided at: http://www.arl.army.mil/www/default.cfm?page=2342, but these questions will not be addressed during the webinar. All presentations made during the webinar will be posted at: http://www.arl.army.mil/reviews/arep.

Please note that information provided or discussed during the information webinar does NOT change the requirements stated in this BAA. Should this BAA require changes, such changes will be made through the issuance of an amendment to this BAA posted in FedBizOps.gov.

5. Period of Performance: The period of performance for the contract award made as a result of this BAA will be for five years. Individual Task Orders issued will include an appropriate period of performance for the effort to be conducted under that individual Task Order. The period of performance for the Cyber CRA cooperative agreement is specified in accordance with the terms and conditions of that agreement.

6. Place of Performance: The place of performance for the contract awarded under this BAA is expected to be a mixture of performance at Government and Contractor facilities, as appropriate, given the nature and sensitivity level of work. Facilities of Cyber CRA Members may also be utilized as appropriate. Any contractor facility to be used for classified and/or sensitive processing must be approved by the Government. Individual Task Orders are expected to include a discussion on the place of performance as necessary and appropriate for that effort.

7. Profit/Fee: Profit/Fee will be negotiated under each Task Order that is issued under the AR&EP contract in accordance with DFARS 215.404-4. No profit or fee will be paid on travel or material/equipment/supply purchases for any Task Order issued under this contract award. Please also note that under the Cyber CRA, Consortium Members are not permitted to earn a profit or fee on their costs.

8. Evaluation and Award: Whitepapers (and invited Proposals) that are in compliance with the requirements of this BAA will be evaluated in accordance with the evaluation factors set forth in this BAA using an adjectival and color rating system. A Source Selection Evaluation Board (SSEB) will evaluate the Whitepapers and invited Proposals. The SSEB will evaluate each Whitepaper and Proposal and provide the results of that evaluation to the Source Selection Authority (SSA). The SSA will make a decision concerning the most highly rated Whitepapers selected and invited for proposal submissions and the award selection.
II. DETAILED INFORMATION ABOUT THE FUNDING OPPORTUNITY

A. Definitions, Scope, Rationale

Discussions of cyber security, cyber science and the network contexts in which they must apply vary widely. Definitions of cyber security and cyber science, and the context of the networks in which the foundational science that apply to this BAA are as follows:

- **Basic Research (6.1):** Systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and/or observable facts without specific applications toward processes or products in mind.

- **Applied Research (6.2):** Systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met.

- **Cyber Security:** For the purposes of this BAA, we restrict the meaning of this term to security against the activities, usually performed by malicious software (autonomous or human-controlled malware), against friendly networked computing devices and operating in the interests of an adversary. These activities aim to enter and propagate malware through the network, to position it at strategic locations, to defeat friendly counter-malware defenses, to disrupt or degrade the functions of the network, to discover and disclose friendly information to the adversary, to distort information, etc. Given the breadth of this domain, the Cyber CRA and the AR&EP will necessarily focus only on a few carefully circumscribed aspects.

- **Cyber Science:** What exactly constitutes "cyber science" remains a topic of growing discourse to which the Cyber CRA and the AR&EP will be important contributors. For the purposes of this BAA, it suffices to say that progress in scientific understanding of cyber phenomena should manifest itself in development of models that 1) are mathematically formulated; 2) explicitly and formally specify assumptions, simplifications and constraints; 3) involve characteristics of threats, defensive mechanisms and the defended network, to include quantifiable attributes of the human; 4) are at least partly theoretically grounded; 5) yield experimentally testable predictions of characteristics of security violations, e.g. the probability that malware M will remain undetected while executing action A; and 6) are experimentally validated.

- **Domain of Army Networks:** Future Army networks will be heterogeneous and convergent, comprising a wide variety of fixed wired networks, mobile cellular networks, and mobile ad hoc networks. Nodes will consist of diverse computing devices, networked computers, software defined radios, smart phones, sensing devices, computing devices embedded in vehicles, weapon systems, munitions, clothing, etc. Links will be similarly diverse with fiber, copper, radio links, optical links, satellite
communications, etc. Army cyber security is further complicated as it must use and defend networks that it neither owns nor directly controls (e.g., mobile, fixed and SCADA networks of a host nation); must construct mission networks with a variety of partners and allies; and must adapt to rapidly changing technologies, tactics, and threats. Broad challenges with Army networks include:

1) **Large attack surface.** The Army often operates in very close physical proximity and with extensive interactions with allied and local civilian personnel and with known and unknown adversaries, comprising a complex cyber ecosystem. Forward-deployed network assets are vulnerable to cyber entry or physical capture and subversion of information and devices. Fixed enterprise networks are particularly vulnerable to insider threats and the increasing global connectivity makes the Army’s assets more vulnerable.

2) **Relatively disadvantaged assets.** Soldiers’ computing and communication devices are energy- and weight-constrained with limited bandwidth and computational capacity. Cyber security techniques must function within the constraints of the Soldiers’ operational environment.

3) **Large scale and high dynamics.** Soldiers and their assets often operate in a highly mobile environment in complex terrain with highly dynamic propagation and connectivity. These networks are often interspersed with civilian, allied, and adversarial networks. Coupled with high mission tempo, these factors create very large, highly complex networks that are difficult to comprehend, monitor, defend and restore.

4) **Advanced persistent threats:** Army networks are targeted by highly sophisticated adversaries with evolving strategies and tactics. These adversaries often execute their threats and attacks over very long periods of time.

**B. ARL Cyber Security Vision**

Cyber security is critical to the Army due to the growing number and sophistication of attacks on military cyber networks, coupled with the ever increasing reliance on cyber systems to conduct the Army’s mission. The Army’s operational environment has changed dramatically due to technology convergence - the blending of computer and telecommunications networks with commercial applications and military systems. The Army’s operational environment encompasses both strategic and tactical networks, at home and abroad, and its enterprise networks may reach from forward operating bases to the Pentagon, providing links between mission command and tactical units with near-real time situational awareness. The modern operational environment emphasizes the importance of the many facets of information on the battlefield and the need to protect it as well as the communications medium. A wide variety of adversaries present multiple continuous and simultaneous threats to cyber systems and the information they process and transmit. ARL recognizes that a unified research and innovative experimentation program is needed to advance the
state of cyber security. The Cyber CRA will focus on developing a fundamental understanding of cyber phenomena (including human aspects) 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. The AR&EP will use its innovative experimentation techniques to validate or invalidate those theories and models.

The dynamics, scale, and complexity of Army networks coupled with evolving, advanced, persistent threats makes cyber security a grand challenge. While evolutionary system hardening and software patching may be needed to deal with legacy systems, they can only deal with known identified threats. Foundational basic research is needed to advance our fundamental knowledge of cyber security so that generalizable theories and models can enable inherently stable, secure, self-adapting networks.

The foundational problem to be addressed by the Cyber CRA is the lack of understanding of cyber phenomena, particularly the fundamental laws, theories, and theoretically-grounded concepts and empirically validated models that would enable rapid design of cyber defense tools and predictive analysis of their efficacy. Lack of such fundamental knowledge – and its importance – has been specifically highlighted. Put succinctly, the cyber security community lacks a science of cyber security. What exactly constitutes "cyber science" remains a topic of growing discourse to which this Cyber CRA will make important contributions. Progress in scientific understanding of cyber phenomena should manifest itself in development of models that:

1) Are mathematically formulated
2) Explicitly and formally specify assumptions, simplifications and constraints
3) Involve characteristics of threats, defensive mechanisms and the defended network, to include quantifiable attributes of the analyst/defender, the user/Soldier, and the adversary
4) Are at least partly theoretically grounded
5) Yield experimentally testable predictions of characteristics of security violations (e.g. the probability that malware M will remain undetected while executing action A)
6) Are experimentally validated by the AR&EP.

The ongoing explosive growth of diverse cyber threats to our armed forces, defense community and national security, combined with rapid accumulation of new observations, techniques and tools for cyber defense provide the empirical basis that will help make significant progress in addressing this foundational problem.

ARL has established a joint collaborative approach of multidisciplinary researchers to make fundamental advances towards meeting the Cyber CRA goal to develop a fundamental understanding of cyber phenomena. ARL has identified three Research Areas,
interrelated aspects of cyber security, that when jointly studied will advance the theoretical foundations of cyber science in the tactical and strategic contexts of Army networks.

- Assessing vulnerabilities and risks of cyber networks to malicious activities
- Anticipating, detecting and analyzing malicious activities
- Undertaking agile cyber maneuver to thwart and defeat malicious activities

In addition to these three Research Areas (RAs), advancing the theoretical foundations requires a trans-disciplinary approach that takes into account the human element of the network (adversary/attacker, defender/analyst, user/Soldier). This human element of the network is being addressed in the Cross-Cutting Research Issue (CCRI), Psychosocial Effects, and is to 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.

Humans play an important role in cyber security and are critical to understanding cyber phenomena. A variety of people influence cyber security including the adversary/attacker, defender/analyst, and user/Soldier. The attacker attempts to compromise data, resources, or availability. For the purposes of this BAA and the Cyber CRA, the attacker mostly invokes zero-day attacks executed persistently over long periods of time (weeks to months), though other types of attacks and timescales may apply. The attacker is concerned with avoiding detection and can originate an attack either internally or externally to the organization. The network analyst is an individual, working alone or more likely as members of cyber defense teams, that defends a data network, regardless of its form, by examining and analyzing collected and streaming network traffic, device data, and other sources of information. Network analysts identify vulnerabilities, classify threats, detect and recognize intrusions, perform forensics analysis, and validate malicious activity to defend against attacks and to mitigate risk/damage. The end user is the consumer of network and device resources in conducting their mission. The end user is often the target of social engineering attacks and their practices relative to established security policies can impact the security of cyber systems. Throughout this BAA, these terms are used interchangeably and the Offeror should specify how the proposed research considers human elements.

Risk, Detection, Agility, and Psychosocial Effects are intricately linked and must be studied jointly. The research performed by the Cyber CRA must develop appropriate mathematical representations, metrics, models, and analysis techniques for experimentation and validation by the AR&EP. Expected outcomes of this contract award are experimental designs leading to validation, or invalidation of theories and models representing the autonomous anticipation of, and adaptation to threats. Quantifiable success can be evidenced by the elimination of costly, labor-intensive defensive measures and repairs to networks, thus significantly simplifying the complexity of cyber security management and the information security information that needs to be comprehended, approved by, and/or applied correctly to users and defenders. Validation of theories through principled experimentation is a critical aspect of the AR&EP’s role. The AR&EP’s innovative
experimentation processes will provide independent validation of the Cyber CRA research and its detailed feedback may expedite identification of needed adjustments in the Cyber CRA research areas. The Cyber CRA research aims to broaden knowledge and understanding of observable facts while the AR&EP efforts are geared towards testing the theories and models to investigate the applicability to Army’s cyber security needs in both tactical and strategic environments.

C. ARL, CERDEC, and Related Programs

ARL and the Communications Electronics Research, Development and Engineering Center (CERDEC) work closely to provide the Warfighter with advanced capabilities to assure communications, information and cyber dominance. ARL’s basic and applied research products are integrated by CERDEC with their C4ISR technologies to provide state-of-the-art functionality to the Warfighter. The Cyber CRA will become an integral part of ARL’s Enterprise in Cyber Security and will contribute to CERDEC’s cyber programs. The AR&EP, as a Cyber CRA Consortium member, will collaborate with the Cyber CRA Researchers to ensure that validation results are communicated in a way that drives and tunes the research. Collaboration and cooperation at this level are critical to the overall success of the Cyber Security research programs, and interactions with other related ARL research, and CERDEC programs may bring different insights to bear on the Cyber CRA’s research problems and experimentation results produced by the AR&EP.

1. ARL’s Mission

The U.S. Army Research Laboratory (ARL) is the Army’s corporate research lab whose mission is to provide the underpinning science, technology, and analysis that enable full-spectrum operations\(^3\). Two Directorates of ARL -- the Computational and Information Sciences Directorate (CISD) and the Human Research and Engineering Directorate (HRED) – conduct research related to cyber security and it is expected that Cyber CRA researchers and the AR&EP will collaborate with researchers in these Directorates. ARL and CERDEC will specifically fund in-house staff to foster direct highly collaborative partnerships between Consortium, Government researchers, and the AR&EP.

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. The Survivability/Lethality Analysis Directorate (SLAD) performs information assurance/computer network operations and electronic warfare analyses of Army systems to identify potential vulnerabilities and recommend mitigation techniques. CISD’s Computer Network Defense Service Provider (CNDSP) operations provide protection from sophisticated cyber threats, and as an experimental laboratory, supports cyber research relevant to the Army. It is expected that interactions with ARL’s analysis and operations personnel will provide context for the Army cyber security problem.

A brief description of ARL’s Cyber Security Enterprise follows.
• **CISD.** ARL's Computational and Information Sciences Directorate (CISD) serves as the principal Army organization for basic and applied research and technology focused on information processing, network and communication sciences, information assurance, battlespace environments, and advanced computing that create, exploit and harvest innovative technologies to ensure current and future US military superiority. CISD's technologies provide the strategic, operational, and tactical information dominance across the spectrum of operations. CISD, in collaboration with academic and industry partners, conducts basic and applied research resulting in technologies that support state-of-the-art capabilities in the distribution and/or assimilation of real or simulated digitized battlespace information. CISD leads the Network Science Collaborative Technology Alliance, the Network & Information Sciences International Technology Alliance with the United Kingdom, the Army High Performance Computing Research Center, and the Mobile Network Modeling Institute. CISD manages and executes a Department of Defense Supercomputing Resource Center (DSRC) for the High Performance Computing (HPC) Modernization Office. CISD coordinates technologies within the Army, other services and their laboratories, industry, and academia to leverage basic and applied research opportunities for the benefit of the Army.

Major areas of research include novel methods for exploiting data; exploitation of information fusion techniques; network science, information sciences, novel communication modalities and communication networks; asset behavior and control (autonomy); multilingual computing (machine translation methods and metrics); intelligent optics; network attack detection and cyber defense; signal processing for complex environments; HPC physics based calculations technology and emerging technology in heterogeneous computing; atmospheric sensing for intelligence, surveillance and reconnaissance (ISR); and atmospheric modeling applications and dynamics.

• **HRED.** ARL’s Human Research and Engineering Directorate (HRED) executes all Human Dimension and Simulation and Training Technology related programs for ARL. HRED is organized to conduct a broad-based program of scientific research and technology development directed into three focus areas: (1) enhancing the effectiveness of Soldier performance and Soldier-machine interactions in mission contexts; (2) providing the Army and ARL with human factors integration leadership to ensure that Soldier performance requirements are adequately considered in technology development and system design; and (3) through advanced simulation technology capabilities, enhancing the Soldier experience in training environments, increasing training system performance and cost effectiveness, and increasing Army analysis capability.

Ongoing efforts within HRED related to cyber defense include: the Social/Cognitive Network Science Collaborative Technology Alliance research efforts, the simulation of cyber events for training systems development, task analysis of network analyst activities, usability assessments of visualization tools for cyber security network analyst, and Soldier modeling and simulation tool development.
• **ARO.** ARL’s Army Research Office (ARO) initiates the scientific and far-reaching technological discoveries in extramural organizations: educational institutions, nonprofit organizations, and private industry. The ARO mission is to serve as the Army’s premier extramural basic research agency in the engineering, physical, information and life sciences; developing and exploiting innovative advances to ensure the Nation’s technological superiority. ARO’s research mission represents the most long-range Army view for changes in its technology. The ARO research program consists principally of extramural academic research efforts consisting of single investigator efforts, university-affiliated research centers and specially tailored outreach programs.

• **SLAD.** ARL’s Survivability/Lethality Analysis Directorate (SLAD) provides integrated survivability and lethality analysis of Army systems and technologies across the full spectrum of battlefield threats and environments as well as analysis tools, techniques, and methodologies. SLAD conducts analytical investigations, modeling and simulations, and laboratory and field experiments to provide its analyses as well as technical advice, and is the subject-matter expert on survivability and lethality matters to program executive officers (PEOs) and program managers (PMs), users, testers, the Army’s independent evaluator, and other customers. SLAD’s Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) mission area is responsible for conducting survivability analyses of C4ISR systems in threat environments. ARL performs information assurance/computer network operations and electronic warfare analyses to identify potential vulnerabilities and recommend mitigation techniques.

• **CNDSP.** CISD’s Computer Network Defense Service Provider (CNDSP) operations serve not only to provide protection from sophisticated cyber threats, but also as an experimental laboratory that supports cyber research relevant to the Army. Particularly important areas of research at ARL include detection and analysis of advanced cyber malicious activities; forensics and threat analysis, and continuous monitoring of vulnerabilities and risk assessment. Developing next generation intrusion detection techniques targeted at advanced persistent threats requires advancing the state of the scientific underpinnings of existing techniques. To this end, ARL pays special attention to rigorous experimental characterization of existing techniques to support intelligent integration of existing intrusion detection techniques into an ensemble. Special challenges are found in cyber defense of complex, mobile networks, where a key goal is to provide Soldiers with actionable cyber assessment to detect and defeat malicious activities of adversaries on tactical networks and hosts. ARL also performs work in forensics and threat analysis that focuses on advanced, highly sophisticated, low-observable threats, taking into account the dynamics of adversarial behaviors on networks. Other areas of research include exploration of theories and models to support continuous monitoring of vulnerabilities and risk assessment and the development of advanced cyber sensors and data collection strategies.

2. **Related Programs at ARL**
• **Cyber Security Collaborative Research Alliance (Cyber CRA).** The primary objective of this Cyber CRA is to define fundamental laws, theories and models of cyber phenomena, including the human components of attacker, defender and end user. The Cyber CRA is focused on several research areas with a cross cutting psychosocial research initiative spanning each area: Risk, Detection and Agility.

• **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. Research in Cyber CRA should leverage the developments in the work on Trust and social/cognitive networks in the NS CTA.

• **Cognition and Neuroergonomics CTA (CAN CTA).** This CTA focuses on cognitive performance, which is generally considered the act of executing mental operations and is intrinsically dependent on task and environmental factors, in addition to the characteristics of the individual soldier. Specific objectives are to optimize information transfer between the system and the soldier, identify mental processes and individual differences that impact mission-relevant decision making, and develop technologies for individualized analyses of neurally-based processing in operational environments. To achieve this objective, the CTA is working to implement computational modeling and execute and link neuroscience based research from multiple levels to produce advances in fundamental science and technology, demonstrate and transition technology, and develop research demonstrators for warfighter experimentation.

• **Mobile Networks Modeling Institute (MNMI).** The MNMI mission is to develop multi-disciplinary expertise and software tools to transform the way in which DoD models, simulates, emulates, and experiments with dynamic reconfigurable mobile warfighter networks. The Institute’s vision is to exploit high performance computing (HPC) through the development of computational software that enables DoD to design and test networks at sufficient levels of fidelity and with sufficient speed to understand the behaviors of Network Centric Operations (NCO) technologies in the full range of conditions in which they will be employed. The goals of the MNMI include (1) developing scalable computational modeling, simulation, and emulation tools, (2)
delivering and supporting software and associated tools to the stakeholder and DoD user community, (3) establishing a new workforce trained across simulation, emulation, and experimentation for NCO with HPC as an enabling tool. The modeling capabilities of the MNMI should be considered for use by the Cyber CRA to provide the ability to simulate, emulate, and test large-scale, highly mobile, \textit{ad hoc} networks with enough fidelity to quantify the performance both technically and operationally.

3. Communications-Electronics Research, Development, and Engineering Center

The Communications-Electronics Research, Development, and Engineering Center (CERDEC) develops and integrates Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) technologies that enable the warfighter to sense the battle space; deny and disrupt enemy efforts; and remain “connected” to achieve information dominance and decisive lethality for the networked Warfighter. CERDEC further maintains a set of Government/world-unique facilities to support a broad range of technology research in support of command and control, communications, computers, Cyber/electronic warfare, and sensors. CERDEC is composed of six Science & Technology (S&T) research directorates to include: Command, Power & Integration (CPI); Intelligence and Information Warfare Directorate (I2WD); Space and Terrestrial Communication Directorate (S&TCD); Night Vision & Electronic Sensors Directorate (NVSD); Product Realization Directorate (PRD); and the Software Engineering Directorate (SED). Of these, two have significant ongoing S&T activities and investments within Cyber technologies.

- **Space and Terrestrial Communications Directorate** (S&TCD) performs research, development, and engineering functions in all aspects of terrestrial, avionics, and space-dependent communications technology to include adaptive, reliable seamless battlefield communications with full electronic counter-countermeasures capability and information security (INFOSEC). By harnessing the potential of communications systems technology, STCD is able to meet the near-term needs of our Soldiers, as well as prepare for the needs of the 21st Century Force. The Cyber Security / Information Assurance (CSIA) Division provides the Warfighter with the means to ensure the security, survivability, and continued operation of tactical and strategic information systems at all classification levels in the face of attack. CSIA focuses technology investments in Defensive Cyber Operations (DCO) RDT&E, Army Cryptographic Modernization and Key Management, Software Assurance, Cross Domain Solutions (CDS), secure mobile communications, Certification and Accreditation, and security systems engineering analysis.

- **The Intelligence and Information Warfare Directorate** (I2WD) conducts Research, Development and Evaluation of ISR, EW and Cyber technologies in order to provide effective and proactive situational awareness, tracking, targeting and survivability solutions that transition into operational relevant capabilities for the Soldier. I2WD provides Army Science and Technology services to include System and System-of-Systems engineering design, analysis, testing, experimentation, and subject matter
expertise to Army program management offices in support of programs of record. I2WD further develops quick reaction capabilities to fill the urgent needs of the Soldiers in the field. Specific to the support of Cyberspace Operations, the Cyber Offensive Operation Division (CO2) conducts Research and Development activities of offensive cyber capabilities to include Counter C2 EW, SIGINT, Electronic Support and Geolocation, and OCO technologies.

D. Programmatic Strategy

The efforts in this BAA are aimed at maturing cyber security research produced by ARL’s recently awarded Cyber CRA through applied research (Budget Activity 2-see definition below). The AR&EP will provide innovative experimentation and empirical validation, covering the gamut from unclassified through secret. A primary goal will be to improve the quality of the basic research being performed by the Cyber CRA through a feedback loop instigated by the experimental results of the Cyber CRA research. Thus, the AR&EP must produce plans to identify when experimentation and validation cross security classification guidelines. The goal is not for the AR&EP to simply execute experiments but to propose and perform applied research using novel experimental approaches to improve the accuracy, impact, realism, repeatability, predictability, and relevance of the experimental processes themselves. This is critical due to existing limitations of experimentation associated with cyber security research. Current experimentation fails to incorporate realistic data, realistic network configurations, realistic scales, etc. These limitations directly limit the applicability to most techniques resulting from cyber security research to operational contexts, even when such techniques have undergone and passed rigorous testing and experimentation.

A significant goal of this effort will be to create a critical mass of collaborating academic, industry and government scientists and engineers focused on solving the research challenges outlined within the scope of the Cyber CRA and associated AR&EP. This intellectual synergy is also expected to include sharing equipment, personnel and facilities to accelerate the process of identifying viable theories and models which will assist in directing the research as well as maturing cyber security for the ARL Cyber Security Enterprise and CERDEC programs.

The roles of the AR&EP will be to:

- **Role 1**: Research and develop new and innovative approaches and processes to evolve basic (6.1) research results to experimental validation (6.2 applied research), as well as perform the identified experimentation in simulated, realistic, and operationally relevant environments. Provide experimental validation of the models and theories developed by the Cyber CRA 6.1 (basic) research; coordinate in the design and execution of a comprehensive series of innovative experiments; and return experimental results to ARL/CERDEC & Cyber CRA researchers, as classification permits.

- **Role 2**: Perform applied research into new and innovative experimental methods, processes and approaches with the goal of improving the accuracy, impact, realism, repeatability, predictability, and relevance of the experimental processes. Identify new
and innovative means to design experiments that can explore cyber phenomena to advance fundamental science by: validating and integrating research results across risk, detection, agility, while observing psychosocial effects; characterize the conditions where specific research approaches are more effective; assess and enhance military relevance using relevant, realistic, and potentially real data for both strategic and tactical environments. Experimentation should explore the full range of cyber challenges including the fundamental scientific or theoretical issues including but not limited to scaling, domains of applicability, factors that limit or promote accuracy of predictions or control, and interactions between risk, detection, agility, and psychosocial effects. The expectation is that experimental results will significantly improve and accelerate the basic research results.

- Role 3: Join and participate in the Cyber CRA as a member organization and collaborate with Cyber CRA researchers on the 6.1 (basic) research. Actively collaborate with Cyber CRA researchers in documenting the results of R&D efforts in technical publications, such as journal and conference paper, and reports, at an appropriate classification level. Develop approaches and processes for the migration of research results to/from basic (6.1) researchers. Ensure an effective feedback loop from the experimental validation while maintaining consideration for the classification of the experimental results and the potentially uncleared status of the majority of the researchers as well as the involvement of foreign nationals.

It is the intent of this BAA 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 related to cyber security. In response to the BAA, Offerors will be required to:

- Propose its unique approach and plans for the innovative experimentation and empirical analyses to validate/invalidate theories and methods developed by Cyber CRA Members in intersections of one or more of the Cyber CRA Research Areas.

- Provide plans for collaborating with Cyber CRA Researchers and a vision for managing those relationships

- Provide detailed plans for the design and development of a testbed prior to the end of the first year of this contract. (This will be the First Task Order to be issued under the contract.) The testbed design must be extensible in order to leverage research facilities at the AR&EP, ARL/CERDEC, and Cyber CRA member sites. The testbed must also be capable of providing a demonstration and data sets that are publically releasable.

- Scope the applied research and experimentation plans, appropriate to the overall funding of the Cyber CRA, ensuring all elements of the proposed applied research and experimentation are tightly integrated in a way that results of research in one area support and enhance the results in other areas. Sufficient resources should be allocated to ensure enough critical mass to make fundamental progress.
• Present the experience, qualifications and availability of the technical and scientific staff and the quality and relevance of research facilities. Also, indicate clearances held by staff as classified processing is required.

• 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.

E. Research Strategy

Offerors are required to address the three roles of the AR&EP as well as specific plans for the First Task Order under the contract in their Proposal. Offerors should carefully review the evaluation factors outlined below when preparing their Whitepaper/Proposal.

Role 1: Experimental validation of 6.1 research (to be performed under the AR&EP contract). Whitepapers and invited Proposal must address how the Offeror proposes to seek out and evolve theoretical research as applied to experimental validation; the plan should include a focus on proactively seeking input from basic researchers on what research to provide experimental validation. Offeror must identify how they will design experiments, based on state of the art in experiment design. The experimental approach must:

- Support tactical and strategic networks
- Generate reproducible and predictable results
- Consider the implications of interrelationships of the cyber research areas (risk, detection, agility, psychosocial effects)
- Integrate experiments into ARL, CERDEC, University, and the Offeror’s own facilities
- Support unclassified and classified experimentation

Offerors should consider the following challenges in their response:

- How do Offerors propose to move from theory to experimentation?
- Cyber security technologies need to be rigorously evaluated with respect to their effectiveness and return on investment. Approaches to such evaluations have not been well defined. Innovative means through security metrics, modeling and simulation, and assessing user trust should be developed.
- Army-relevant cyber security research within the context of the Cyber CRA is focused on complex, heterogeneous converged networks, i.e., both tactical and strategic, both wired and mobile wireless. Thus, the experimentation should address the complexity and heterogeneity of such networks and of cyber phenomena occurring in them.

Role 2: Applied Research into Innovative Experimental Approaches (to be performed under the AR&EP contract). Whitepapers/Proposal must include a plan for innovative experimental approaches to cyber security, as opposed to merely a plan for executing experiments. The Offeror’s response should include proposed plans for innovative research
into new experimental methods, processes, and approaches. The proposed innovative approach to cyber security experimentation should derive from the state of the art \[2,3,4\] and seek to improve accuracy, impact, realism, repeatability, predictability, etc. Also of interest is research into how to migrate experimentation results to transferrable technology packages for potential use in other research efforts within the ARL & CERDEC labs for the purpose of extending understanding of cyber phenomena. Offerors should consider the following challenges in their response:

- Comprehensive theory and practical techniques for rigorous scientific experimentation in cyber security are lacking.
- Practical requirements (e.g., portraying operationally relevant experiments (adequate network scale, realistic network traffic, realistic user activities, and realistic threat activities) are difficult to assure and validate and require innovative approaches.
- AR&EP must combine insight into theoretical results with creative approaches to operationalize research. While some research products offer an obvious path to application, others will be theoretical and esoteric nature.

Role 3: Participation in the Basic Research under the Cyber CRA (to be performed under the Cyber CRA cooperative agreement) As discussed above, the Offeror selected for award under this BAA will be required to become a Consortium Member of the Cyber CRA, and as such is required to actively collaborate with and contribute to the Cyber CRA basic research. To this end, Whitepapers and invited Proposals submitted in response to this BAA are requested to include a discussion of the Offeror’s proposed plans to collaborate under the Cyber CRA and are also requested to document the Offeror’s existing in-house capability to actively contribute to the Cyber CRA research. Offerors should identify their collaboration plans for each of the three Cyber CRA topic areas of risk, agility, and detection, as well as the cross-cutting area of psychosocial effects. The collaboration plan must:

- Identify how simulated, realistic, and operationally relevant data will be generated for use by the Cyber CRA researchers. This plan should include input and collaboration with ARL and CERDEC.
- Identify the Offeror’s plan to migrate data, algorithms, and theory to/from classified space.
- Develop procedures to return experimental results to researchers when the experiments are performed on classified data; i.e., the results will express the contents of the data.
- Develop processes to effectively communicate the complex scientific information so it is understood by Cyber CRA Members and vice versa.

Offerors should consider the following challenges in their response:

- Few Cyber CRA academic researchers will have clearances. AR&EP will have to develop skills, techniques and procedures appropriate for collaboration under these constraints.
- The basic researchers need realistic data. AR&EP will be challenged to provide data that
is publicly releasable. Real-world data is hard to anonymize and may be too sensitive to release without anonymization; real world properties are difficult to replicate in generated data.

- AR&EP must gain an understanding of the basic research, including theoretical elements.

First Task Order: Document Plan for Testbed Development (proposed to be performed at the first Task Order under the AR&EP contract to be issued immediately after contract award). The Offeror must document a plan for developing a testbed capable of generating results that are simulated, realistic, and operationally relevant. The complexities of the Army’s cyber environments are extremely difficult to reproduce in a testbed or test framework. Development of a cyber security testbed will require realistic hardware, software, traffic data and network models. The AR&EP will need to apply innovative techniques to design and develop the testbed and develop processes for experimentation with Cyber CRA-developed cyber theories and techniques. Results from these experiments and exercises will support the AR&EP in refining the testbed design and tuning future experiments.

This testbed must be designed and developed in coordination with ARL, CERDEC, and the Cyber CRA Members. The testbed design should provide for extensibility in order to include components from all organizations including the Offeror's own. The testbed design and plans for build out must be completed within the first year of this award. The testbed must be capable of being demonstrated in a publicly releasable and unclassified manner.

F. Coordination & Collaboration

The recently established Cyber CRA maintains the ARL concept of creating Alliances (Army Collaborative Technology Alliances (CTAs) and Collaborative Research Alliances (CRAs)) to facilitate a close working relationship between ARL and its partners. What creates an “Alliance” is the Government working collaboratively and in partnership with an organization or a group of organizations, e.g., in the Cyber CRA the Government is working with a Consortium of organizations that are bound together as members of the Alliance. Experience has shown that persistent collaboration between Government, academia, and industry enhances innovation and has a high return on investment. To further emphasize the importance of coordination and communication among the Alliance, the Cyber CRA team is structured so that each member is active in more than one research area. It is ARL's strong belief that work conducted under the Cyber CRA cannot be successful, either in whole or in part, without such collaboration and this success will also require masterful coordination by and with the AR&EP.

The role of the AR&EP is to conduct cyber security research and experimentation, both unclassified and classified, and extended empirical analysis to support Cyber CRA research. The AR&EP will incorporate its real-world experience, realistic materials (network traffic and intrusion data, detailed network maps, traffic generators, etc..) and its knowledge of state-of-the-art commercial tools to conduct innovative experimentation. The experimentation methods and testbeds used must represent the environments the Army operates within to satisfy the need for
generalizable techniques, as well as inform the Government when the research needs to be segregated into more controlled channels.

These experiments will be used to inform the Cyber CRA Members and Government of the validity of their 6.1 theories and models. Further, it is expected that subsequent Cyber CRA research will be driven by the results of the experimentation and empirical analyses. The interdependencies of the Cyber CRA research areas, combined with the ubiquity of the psychosocial aspects, and the diversity of Army’s tactical and strategic networking environments, make experimentation for foundational cyber science a highly dynamic and complex task. Using the outputs of the Cyber CRA researchers to conduct experiments, which will in turn become inputs to the Cyber CRA researchers, will require the AR&EP to have a solid understanding of the Cyber CRA research thrusts and also demonstrate significant skill in coordinating activities within its own team and other Cyber CRA Members.

The AR&EP will work with ARL & CERDEC to ensure stakeholder interests and priorities are well understood at the onset of the contract awarded through this BAA. Laboratory facilities at ARL/CERDEC (Adelphi and APG), and Cyber CRA Members, as well as the AR&EP’s own facilities, will be used to conduct experiments. The AR&EP will work with the Government to determine which facilities are most appropriate for use, considering factors such as existing infrastructure, availability, accessibility, and classification issues.

Collaboration among the members of the Cyber CRA, Government, & the AR&EP is integral to the execution of the research program, and to jointly address the challenges associated with cyber security risk, detection, and agility. This collaboration will require more than occasional meetings, email and telecons to coordinate the work. As stated previously, in addition to the effort to be performed under this BAA, the Cyber CRA will allocate $350K per year for the AR&EP’s collaboration efforts once award is made under this BAA and the selected Offeror is added to the Cyber Security cooperative agreement as a Consortium Member. The Cyber CRA has established an environment that is conducive to collaboration and the AR&EP must identify how they will:

- Perform Applied Research
  - Design/Provide appropriate framework/testbeds for experiments representative of the Army’s operational space and functions
    - Demonstrate the vision necessary to design testbeds that reflect the heterogeneous and convergent networks of the Army domain
    - Demonstrate ability to execute experiments at ARL/CERDEC and Cyber CRA Member facilities
    - Demonstrate ability to perform experiments in both unclassified and classified environments
  - Provide realistic network traffic, intrusion data, vulnerability data, etc.
  - Schedule facilities and appropriate personnel to conduct experiments in a manner synchronized with Cyber CRA Members’ milestones
  - Integrate with existing teams
Cyber CRA Members, and ARL/CERDEC Scientific & Engineering Staff
- Attend and/or otherwise participate in scheduled workshops and boot camps and annual technical review
- Collaborate on Basic Research
  - Demonstrate understanding of the Cyber CRA Research Areas via experiments that are designed to answer the questions of interest
  - Provide experimentation results to Cyber CRA Members and Government
    - Provide sufficient feedback to help researchers tune their models and theories with the goals of improving accuracy and analysis
  - Participate in authoring journal and conference publications

G. Management

As stated above, the intent for this BAA is to award a contract for experimental validation and applied research to augment the cyber security research efforts of the Cyber CRA, the ARL Cyber Security Enterprise and CERDEC’s cyber programs. The AR&EP’s role will be to conduct experimentation, unclassified and classified, and extended empirical analysis on these theories and models as part of an applied research effort. The AR&EP is expected to perform these experiments using various facilities; those of the AR&EP, ARL and/or CERDEC facilities, and those available via the Cyber CRA members. The selected Offeror will become a member of the Cyber CRA Consortium. The AR&EP will participate with the Cyber CRA researchers in documenting the results of these R&D efforts in technical publications such as journal articles and conference papers at the appropriate classification level.

The Cyber CRA Consortium is composed of a highly diverse yet complementary team of researchers in the areas of security, network, risk and psychosocial factors. The Consortium is led by Pennsylvania State University (also referred to as the Lead Research Organizations or LRO) which has leading senior faculty in security, systems and networking. The other Consortium Members include Carnegie Mellon University, Indiana University, University of California at Davis and University of California Riverside. Carnegie Mellon University and Indiana University members have been at the forefront of the study of human factors as it relates to security, as well as other areas in public policy, psychology, cognition, risk, security and privacy. Principal Investigators from University of California at Davis and University of California Riverside have broad experience in security, networking and formal methods.

The Cyber CRA consists of four focus teams whose efforts are centered on the Research Areas (RA) and the ubiquitous psychosocial aspects. The RA teams focus on their respective research agendas while the psychosocial team is distributed across the RAs. Research leadership is provided by the LRO, that serves as the central point of contact for research activities. RA team leads coordinate with the LRO on issues of resources and reporting.

RA teams rely on each other for results and the AR&EP will use those results as input and provide results from its innovative experimentation approach as inputs to the RA teams. The
LRO will augment information flow among teams via bi-monthly conference calls with team leaders and key team members. These calls are designed to ensure that results and status are clear to all members of the project, and to build consensus on the refocusing of research priorities as results dictate. As a full member of the Cyber CRA, the Offeror selected for award as a result of this BAA will participate in Consortium activities that are designed to serve as educational & research focus/results synchronization opportunities. Further, the Consortium will hold periodic research reviews to support the free exchange of ideas and research results, in particular those impacting any cross cutting research themes.

H. Funding

As stated above, as a result of this BAA, the Offeror selected for award will: (1) be awarded a procurement contract to perform the AR&EP efforts; and (2) be added to the existing Cyber CRA cooperative agreement award as a Consortium Member.

The contract award vehicle for the AR&EP efforts will be a single indefinite delivery/indefinite quantity (IDIQ) contract as defined at 10 U.S.C. 2304A for the execution of the program. The IDIQ contract will have a ceiling amount of $48.5M over a five year period. Under this IDIQ contract, Task Orders will be issued for the applied research, validation and experimentation efforts, based on the Offeror’s innovative approach to the program requirements and how that approach manifests itself during performance, given the interaction with the Cyber CRA and the opportunities presented as a result of performance. The Government is expected to provide a baseline of $1.5M in annual funding for Task Orders under this contract, with the First Proposed Task Order described in this BAA. The initial focus of the AR&EP will be on the design and implementation of an innovative cyber experimentation testbed that may leverage existing capabilities in current Army programs.

Cyber security research and experimentation is not only critical to the Army but the DoD as a whole. The $48.5 ceiling of the contract will provide a mechanism for growth and enhancement in collaboration with Cyber CRA partners and potential other Government partners with additional applied research and experimentation efforts, above the baseline annual amount of $1.5M. As the Cyber CRA develops we anticipate an increased focus on experimentation and validation of basic research focusing on the Cyber CRA research areas. In the remaining years, additional efforts will focus on experimentation involving human factors and operationally relevant data sets. The maximum funding level represents the belief that experimentation that can result in a significant pay-off will likely need access to operationally relevant data and end-users, which may be difficult to aggregate without a significant investment in applied research funds.

The majority of the funding expected to be provided for the AR&EP contract will be budget activity 6.2 defined as follows:

- **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.

In addition to the award of the AR&EP contract, the Offeror selected for award under this BAA will be required to join the Consortium for the Cyber CRA. The Cyber CRA Consortium will allocate $350K per year of the annual Cyber CRA funding for the AR&EP member’s participation in the basic research program.

The efforts to be performed by the AR&EP cooperative agreement will be budget activity 6.1 defined 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.

I. **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 Offerors 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. Offerors 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.” Offerors invited to submit Proposals will receive feedback on their Whitepapers to substantially improve their Proposal submissions. Offerors invited to submit Proposals may also be afforded an opportunity to visit one or more Government facilities that may be engaged during performance under any award resulting from this BAA. If an Offeror has NOT submitted a Whitepaper, the Offeror may NOT submit a Proposal for consideration for funding. Offerors should note that there are deadlines, page limitations and other requirements associated with the submission process, for both the Whitepaper and the Proposal.

1. **Whitepaper.** Offerors are responsible for submitting electronic Whitepapers so as to be received by the Government no later than the 3:00PM EST on 5 March 2014. Whitepapers shall be emailed to usarmy.rtp.aro.mbx.baa2@mail.mil and must include a subject line of “WHITEPAPER – AR&EP BAA” in order for the Whitepaper to be properly received. When sending electronic files, the Offeror shall account for potential delays in file transfer from the originator’s computer server to the Government website/computer server. Offerors 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. 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 for evaluation. Offerors will receive an email confirmation from the Government that their Whitepaper has been received within 24 hours of receipt of the Whitepaper submission.

**Whitepaper Content and Form**

- White Papers must be submitted electronically to usarmy.rtp.aro.mbx.baa2@mail.mil in the following format:
  - Single PDF file as an email attachment
  - Page Size: 8½ x 11 inches
  - Margins – 1 inch
  - Font – No smaller than Times New Roman, 12 point
  - Number of Pages – no more than twelve (12) single-sided pages. Any pages exceeding the twelve page limit will not be evaluated.
Whitepapers will consist of:

- **Unclassified, publicly releasable information only**
- Overview of Innovative Experimentation and Research Strategy (2 pages)
- Research and Experimentation Program (8 pages)
  - Outline innovative approach for experimentation to span CRA Research Areas & CCRI
    - Integration with and involvement in basic research
    - Identification of key components (not personnel) necessary for a successful experimentation process
    - Overview of a test-bed to experimentally validate basic research
  - Approach for deriving publicly releasable relevant data sets from sensitive/FOUO/classified environments
    - Description of unclassified facilities available for this contract (1 page).
  - Biographical Sketches (1 page per PI)

2. **Proposal.** Proposals in response to this BAA will be submitted **BY INVITATION ONLY.** Additional information concerning submission instructions and the content of such Proposals will be specified in the Invitation Letter from the Government.

J. **Application Review Information**

**Whitepaper Evaluation Criteria.** The following represents the evaluation criteria for Whitepapers submitted under this BAA:

**Factor 1: Technical and Scientific Merit and Relevance:** Evaluation of this factor will concentrate on the overall scientific and technical merit, military relevance, and innovation of the proposed efforts in light of the Cyber Security state-of-the-art. Factor 1 includes four subfactors as follows (and as discussed in the Programmatic Strategy and Research Strategy Sections above) for the Offeror's approach and proposed plans for:

- A. Role 1: Experimental validation of basic research
- B. Role 2: Applied Research into Innovative Experimental Approaches
- C. Role 3: Participation in the Basic Research under the Cyber CRA
- D. First Task Order: Testbed Development

The Whitepaper should include an overview of the innovative experimentation and research strategy to be employed to advance the state-of-the-art in cyber security as it relates to the three roles and First Task Order. The Whitepaper should include an outline of the innovative plans and approaches proposed for the research and experimentation program and how such is expected to lead to an understanding of cyber security phenomena. The Whitepaper should discuss plans for integration and involvement with basic research. Finally, the Whitepaper
should include an overview of the proposed approach and plans for the First proposed Task Order related to Testbed Development.

Factor 2: Experience and Qualifications of Scientific and Technical Staff: The qualifications, capabilities, availability, and experience of the Offeror's proposed personnel (individually and as a whole), their relevant past accomplishments, and their ability to achieve the proposed technical objectives will be evaluated. Demonstrated expertise in the Cyber CRA basic research areas, CCRI, and experience conducting experiments to observe cyber security phenomena should be included and will be evaluated. Any clearance status of personnel should also be indicated as the effort will include the handling of classified requirements up to the Secret level.

Factor 3: Facilities and Equipment: Evaluation of this factor will focus on the plans for the testbed and its planned capabilities with respect to the Cyber CRA research areas (Agility, Detection and Risk), and the CCRI. The Whitepaper should include a description of the facilities and equipment available for the research and demonstrations, who will have access to these facilities, and the readiness to perform classified processing up to Secret. The Whitepaper should include a narrative describing how the Offeror's facilities and equipment will be used to provide simulated, realistic, and operationally relevant environments for experimentation and generation of data sets.

Relative Importance of the Evaluation Factors: The Evaluation Factors are listed in descending order of importance with Factors 2 and 3 being approximately equal. Within Factor 1, the Subfactors are in descending order of importance with Subfactors 1A, 1B and 1C being approximately equal.

Proposal Evaluation Criteria. The following represents the evaluation criteria for Proposals submitted under this BAA:

Factor 1: Technical and Scientific Merit and Relevance: Evaluation of this factor will concentrate on the overall scientific and technical merit, military relevance, and innovation of the proposed efforts in light of the Cyber Security state-of-the-art. Evaluation of this factor will also concentrate on the long-term relevance of the proposed efforts and the likelihood that these efforts will address research and technical challenges and barriers facing the Army.

Factor 1 includes four subfactors as follows (and as discussed in the Programmatic Strategy and Research Strategy sections above) for the Offeror's approach and proposed plans for:

A. Role 1: Experimental validation of Basic research
B. Role 2: Applied Research into Innovative Experimental Approaches
C. Role 3: Participation in the Basic Research under the Cyber CRA
D. First Task Order: Testbed Development

Under this proposal, offerors are requested to discuss their proposed strategy and approach to performing the three roles set forth in the Program Strategy for the AR&EP set forth as Subfactors A, B and C above. Further, Offerors are to propose more detailed and specific plans
for the First Task Order related to Testbed Development discussed in this BAA, set forth as Subfactor D above.

Technical merit will be evaluated with regard to the proposed experimental validation plan and proposed plan for testbed development (Subfactor A).

Scientific merit will be evaluated with regards to the proposed research into innovative experimental approaches and plan for participation in the Cyber CRA on basic research, as well as the specific plans for the First Proposed Task Order related to Testbed Development (Subfactors B, C and D).

The Proposal should include an overview of the research and technical strategy to be employed to advance the state-of-the-art in cyber security and a detailed technical discussion of the three Roles and First Task Order. The technical discussion should include the background and objectives of the proposed research and technical development plans, the overall technical approaches to be pursued, and the potential techniques to be used to validate the models and theories developed by the Cyber CRA.

The Proposal should include the specific innovative plans and approach proposed for the three Roles and First Task Order and how such is expected to lead to an understanding of cyber security phenomena. Experimentation plans must provide enough detail to judge whether proposed experiments with human subjects will validate the research. The Proposal should include the proposed processes and methods for sharing insights related to classified results with uncleared Cyber CRA Members. Offerors must also be aware that Cyber CRA Members may be foreign nationals.

**Factor 2: Experience and Qualifications of Scientific and Technical Staff:** The qualifications, capabilities, availability, and experience of the Offeror's proposed personnel (individually and as a whole), their relevant past accomplishments, and their ability to achieve the proposed technical objectives will be evaluated. Demonstrated expertise in the Cyber CRA basic research areas, CCRI, and experience conducting experiments to observe cyber security phenomena should be included and will be evaluated. Any clearance status of personnel should also be indicated as the effort will include the handling of classified requirements up to the Secret level.

**Factor 3: Facilities and Equipment:** Evaluation of this factor will focus on the Offeror's proposed facilities and equipment to be used for the efforts as described in this BAA. This includes proposed facilities and equipment related to applied research and experimentation efforts, research efforts associated with the Cyber CRA as well as the specific facilities and equipment that will be made available to support the First Task Order in connection with testbed development. Evaluation of this factor will also include how the Offeror proposes to connect with and leverage the Army’s facilities at ARL and CERDEC to achieve the research and technical objectives. The Proposal should include a plan for how Offerors will provide simulated, realistic, and operationally relevant environments and data sets. The extent to which the
Offeror’s proposed facilities and equipment will contribute to the accomplishment of the proposed AR&EP efforts will be evaluated including the nature, quality, relevance, availability, and access to state-of-the-art research facilities and equipment; and the evaluation will include the ability to perform sensitive and classified experimentation. The Proposal should include a description of the facilities to be used for the research and demonstrations, who will have access to these facilities, and how such facilities will enhance the efforts proposed.

**Factor 4: Program Management:** Evaluation of this factor will focus on the Offeror’s plans for management of the efforts described in this BAA as well as the experience in managing similar efforts. In response to this BAA, Offerors are requested to provide a discussion of the intended approach to managing these multi-faceted relationships (both as a collaborative partner under the CRA and the AR&EP performing under the contract) among highly diverse researchers, involving multiple levels of security and multiple research facilities. Offerors are requested to describe the intended strategy for scheduling, tracking, and managing multiple task orders simultaneously, and for bringing the appropriate people to the appropriate facilities for experimentation purposes. Further, Offerors are to demonstrate their proposed channels of communication among the offeror, Cyber CRA Researchers and the ARL/CERDEC staff to ensure the most effective and efficient response to any issues that may arise. Offerors should include examples of relevant, successful and similar, current and previous working relationships with highly diverse, geographically dispersed team members.

**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 2, 3 and 4 being approximately equal. Factor 5 is not weighted. Within Factor 1, the Subfactors are in descending order of importance with Subfactors 1A, 1B and 1C being approximately equal.

**Review and Selection Process**

All timely and compliant Whitepaper submissions will be evaluated in accordance with the evaluation criteria set forth in this BAA. Whitepapers are expected to be evaluated by Government scientists and managers. However, the Government reserves the right to have Whitepapers evaluated by subject matter experts outside the Government, which may include members of the Cyber CRA. Should such outside evaluators be used, they will be required to sign a non-disclosure statement with ARL before being provided access to Whitepapers and such outside evaluators will not be eligible to participate in any Whitepaper submission. The non-disclosure statement will subject the outside evaluators to 41 USC Chapter 21. Only the most highly rated Whitepapers will receive an invitation to submit a Proposal, as well as
feedback on their Whitepaper. Offerors 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” on their Whitepaper. Offerors not receiving an invitation to submit Proposals will be informed of this decision via email following the Whitepaper evaluations.

All invited timely Proposal submissions will be evaluated in accordance with the evaluation criteria set forth in this BAA. All information necessary for the review and evaluation of a Proposal must be contained within the Proposal. No other material will be provided or considered in by those evaluating the Proposals. An initial review of the Proposals will be conducted to ensure compliance with the requirements of this BAA. Failure to comply with the requirements of the BAA may result in a Proposal receiving no further consideration for award.

Proposals that are in compliance with the requirements of the BAA will be evaluated in accordance with the evaluation factors described above using an adjectival and color rating system. A Source Selection Evaluation Board (SSEB) will evaluate the Proposals. The SSEB consisting of scientists, managers, and cost specialists, will evaluate each Proposal and provide the results of that evaluation to the Source Selection Authority (SSA). The SSA will make a decision concerning the Whitepaper down selection, any competitive range selection, and the award selection. The SSEB is expected to be comprised of Government employees; however, the Government reserves the right to have Proposals evaluated by subject matter experts outside the Government. Should such outside evaluators be used, they will be required to sign a non-disclosure statement with ARL before being provided access to Proposals and such outside evaluators will not be eligible to participate in any Proposal submission. The non-disclosure statement will subject the outside evaluators to 41 USC Chapter 21.

After Proposals are evaluated, the Government reserves the right to establish a competitive range and enter into negotiation discussions or award without discussions. Negotiation discussions may be conducted telephonically or face-to-face at the Offeror’s facility. Any such meeting will be coordinated with the Offeror at the appropriate time. If a competitive range is established for negotiation purposes, then all Offerors 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 Offeror’s ability to satisfy the BAA requirements. The Government will make award to the Offeror whose Proposal conforms to the BAA, offering the best value to the Government, cost and other factors considered. Further, award may be made to other than the Offeror who offers the lowest cost proposal. ARL reserves the right not to make an award should no acceptable Proposal be submitted.

Other Award Information

**Recipient Qualification:** The Federal Awardee Performance and Integrity Information System (FAPIIS) will be checked prior to making an award. The web address is: [http://www.fapiis.gov/fapiis/index.jsp](http://www.fapiis.gov/fapiis/index.jsp). The applicant representing the entity may comment in this system on any information about itself that a Federal Government Official entered. The
information in FAPIIS will be used in making a judgment about the entity’s integrity, business ethics, and record of performance under Federal awards that may affect the official’s determination that the applicant is qualified to receive an award.

**Administrative and National Policy Requirements:** SAM - Successful applicants not already registered in the System for Award Management (SAM) will be required to register in SAM prior to any award resulting from this BAA. Information on SAM registration is available at www.SAM.gov.

**Subcontracting Plan:** This section is applicable to contracts (awarded to other than Small Businesses) where the dollar threshold is expected to exceed $650,000.00. Pursuant to Section 8(d) of the Small Business Act [15 U.S.C. 637(d)], it is the policy of the Government to enable small business concerns to be considered fairly as subcontractors under all research agreements awarded to prime contractors. The required elements of the Subcontracting Plan are set forth by FAR 52.219-9 and DFARS 252.219-7003. A Subcontracting Plan is not required with any Whitepaper submission in response to this BAA. Requirements for Subcontracting Plans associated with Proposal submission will be included with the Invitation Letter for the Proposal.

**Army Manpower Contractor Reporting:** The Department of Defense operates and maintains a secure data collection site where the contractor will report ALL contractor manpower (including subcontractor manpower) required for performance of a contract. The contractor is required to completely fill in all required data fields at http://www.ecmra.mil. The required information includes: (1) Contracting Office, Contracting Officer, Contracting Officer’s Technical Representative; (2) Contract number, including task and delivery order number; (3) Beginning and ending dates covered by reporting period; (4) Contractor name, address, phone number, e-mail address, identity of contractor employee entering data; (5) Estimated direct labor hours (including subcontractors); (6) Estimated direct labor dollars paid this reporting period (including subcontractors); (7) Total payments (including subcontractors); (8) Predominate Federal Service Code (FSC) reflecting services provided by contractor (and separate predominant FSC for each subcontractor if different); (9) Estimated data collection cost; (10) Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army Requiring Activity is responsible for providing the contractor with its UIC for the purposes of reporting this information); (11) Locations where contractor and subcontractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website); (12) Presence of deployment or contingency contract language; and (13) Number of contractor and subcontractor employees deployed in theater this reporting period (by country). As part of its submission, the contractor will also provide the estimated total cost (if any) incurred to comply with this reporting requirement. The reporting period will be the period of performance not to exceed 12 months ending 30 September of each Government fiscal year and must be reported by 31 October of each calendar year. Contractors may use a direct XML data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a
contractor’s systems to the secure web site without the need for separate data entries for each required data element at the web site. The specific formats for the XML direct transfer may be downloaded from the web site.