TABLE OF CONTENTS

1. **CRITERIA**
2. **REVIEW AND SELECTION PROCESS**
3. **RECIPIENT QUALIFICATION**
4. **ANTICIPATED ANNOUNCEMENT AND AWARDS DATES**

F. AWARD ADMINISTRATION INFORMATION

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

G. AGENCY CONTACTS

I. OVERVIEW OF THE FUNDING OPPORTUNITY

A. REQUIRED OVERVIEW CONTENT

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

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

3. **Funding Opportunity Title:** Cyber Security (CS) Collaborative Research Alliance (CRA)

4. **Announcement Type:** Initial

5. **Funding Opportunity Number:** W911NF-13-R-0004

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 CRA Program Announcement (PA):

EVENT	ESTIMATED DATE/TIMEFRAME
PA released	14 March 2013
Whitepapers due	26 April 2013
Whitepaper Feedback/Invitation to Submit Full Proposal	22 April – 31 May 2013
Full Proposals due	19 July 2013
Award	30 September 2013

B. EXECUTIVE SUMMARY

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 U.S. Army Research Laboratory (ARL) has established an Enterprise approach to Cyber Security that couples multi-disciplinary internal research, analysis, and operations with extramural research and collaborative ventures. ARL intends to establish a new collaborative venture – The Cyber Security Collaborative Research Alliance (CRA) – that seeks to advance the theoretical foundations of cyber science in the context of Army networks.

This Collaborative Research Alliance will consist of academia, industry and government researchers working jointly to solve complex problems. The overall objective of the Cyber Security CRA is to develop a fundamental understanding of cyber phenomena, including aspects of human attackers, cyber defenders, and end users, so that fundamental laws, theories, and theoretically grounded and empirically validated models can be applied to a broad range of Army domains, applications, and environments.

To achieve the CRA's vision, a radical departure from current research models where research areas proceed independently along stovepipes is imperative. The Cyber CRA is expected to establish a new way of conducting cyber security collaborative research that breaks down research barriers, builds new collaborative relationships, and develops mutual understanding across organizations, technical and scientific disciplines, and Research Areas. ARL strongly believes that a joint collaborative approach by a multidisciplinary researcher team is required to make fundamental advances towards meeting the CRA goal to develop a fundamental understanding of cyber phenomena.

ARL has identified three interrelated aspects or Research Areas of cyber security that when jointly studied will advance the theoretical foundations of cyber science in the context of Army networks. 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. This Cross-Cutting Research Issue (CCRI) addressing Psychosocial Effects must be jointly studied in the context and the constraints of the three Research Areas. The Research Areas and CCRI for this 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. Risk assessment should take into account the context of the mission. Research in this area should lead to theoretically-grounded techniques and tools to synthesize, modify, adapt, or redesign algorithms that reliably compute risks imposed by new cyber threats to Army networks and changes to networks to counter or avoid such threats.

- **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. This research should inform development of approaches to rapid adaptation (potentially in the midst of a battle) of a detection technique or algorithm as new threats emerge.

- **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.

- **Psychosocial Effects.** Each of the three Research Areas must take into account the Psychosocial Effects Cross Cutting Research Issue. 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. Thus, since teams of human defenders will likely be the key link in cyber defense, a theoretical understanding of the socio-cognitive factors that impact the decision making of the user/Soldier, defender/analyst, and adversary needs to be developed. As examples: the Risk RA should leverage and develop theories of how users evaluate risk and make decisions regarding cyber security, both as individuals and as members of teams since effective cyber defense will require information sharing between users and defenders. The Detection RA must take into account the detectability and predictability of adversary activities. The Agility RA should take into account models of adversarial behavior. It is expected that the Psychosocial Effects will serve as an integrating factor across the three Research Areas.

An overarching goal of cyber security is to significantly increase the cost incurred by adversaries in undertaking cyber attack while minimizing the loss in performance (such as overhead and availability) incurred by our networks. CRA research should create a framework that effectively integrates the knowledge of our cyber assets and potential capabilities and approaches of our adversaries, and provides defense mechanisms that adjust dynamically to changes in mission, assets, vulnerability state, and defense mechanisms. Comprehensive cyber situation awareness ultimately leads to effective defense.

Risk, Detection, Agility, and Psychosocial Effects are intricately linked and must be studied jointly. The proposed research must develop appropriate mathematical representations, metrics, models and analysis techniques. Expected outcomes are principled theories leading to autonomous anticipation of, and adaptation to threats which

can eliminate costly, labor-intensive defensive measures and repairs to networks, thus significantly simplifying the complexity of cyber security management while minimizing the impact on Army operations. Validation of theories through principled experimentation should be a critical aspect of the proposed research.

Collaboration between the Consortium and the Government is integral to the execution and success of the CRA. It is ARL's strong belief that work conducted under the Cyber Security CRA cannot be successful either in whole or in part without collaboration. That is, collaboration among the members of the Consortium and the Government Members of the Alliance is integral to the execution of the research program, especially the Psychosocial Effects CCRI and to jointly address the challenges associated with cyber security risk, detection, and agility.

Award Instrument: This PA is expected to result in the award of a cooperative agreement (CA) as defined at 31 U.S.C. 6305 for the execution of the program. The CA will be awarded to a Consortium of organizations that may include academic, industrial and non-profit organizations. To assure the creation of a well-focused research program, the number of partners should balance the need for expertise in all three Research Areas and the crosscutting research initiative with the need to maintain a focused, cohesive, well-integrated research program.

The Consortium must be led by an academic institution charged with spearheading the focused basic research program. This organization will be designated as the Lead Research Organization (LRO), with one or more additional organizations adding to the research expertise and collaboration. ARL will award under a separate Broad Agency Announcement a contract for experimentation and applied research to mature cyber security research for the ARL Cyber Security Enterprise. After award of this contract, the contractor selected for award (hereinafter referred to as the "BAA Partner") will be added as a Member to the Consortium selected as a result of this PA in accordance with the provisions to add a new member under the Articles of Collaboration (see PART II.A.). The Consortium will allocate $350K per year of the annual CA funding for this member's participation once selected and added to the agreement. The role of the BAA Partner in the Consortium will be to conduct cyber security research and unclassified experimentation of CRA research results. In addition this member will support the Consortium through its efforts under the contract by conducting sensitive and classified experimentation including extended empirical analysis for these experiments as part of an applied research effort.

Additionally, it is a goal that "covered educational institutions" (to include Historically Black Colleges and Universities and Minority-Serving Institutions or HBCU/MSIs – see also **PART II.C.1** below) will receive 5% of the annual CA funding. The Consortium will function as a collective of equal partners deciding upon all Consortium matters. It is anticipated that the Consortium may be enhanced by additional researchers and research organizations chosen jointly by the Consortium and the Government to foster new ideas/innovation and thus complement research already undertaken. These researchers and research topics, while part of the Biennial Program Plan, will be Subawardees to the LRO and not part of the Consortium proper. The government reserves the right to direct

ten percent (10%) of the annual CA funds in each research area to ensure flexibility in exploring high-risk research initiatives conducted by Subawardees.

Proposal Submission: The application process (see **PART II.D)** consists of a Whitepaper stage and a Proposal stage. The purpose of requesting Whitepapers is to minimize the effort associated with the production of detailed proposals for those 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 that is expected to substantially improve their Proposal submissions. **If Offerors have NOT submitted a Whitepaper, they may NOT submit a Proposal for consideration for funding.** Offerors should note that there are page limitations and other requirements associated with the submission process, both the Whitepaper and the Proposal. Proposals submitted in connection with this PA are due by the date and time specified in **PART II.D**.

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

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

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

Profit/Fee: Profit/fee is not permitted under the CA.

Cost Sharing: To be responsive to this PA, cost sharing is encouraged but not required except for Federally-Funded Research and Development Centers (FFRDCs) and National Laboratories. During the evaluation of proposals, cost sharing will be evaluated as it relates to the evaluation factors listed in the PA, based on the degree to which the proposed cost sharing enhances the proposal to result in added benefits to the Cyber Security CRA Program. For a proposed cost sharing to receive appropriate credit, each

proposal should express a firm commitment to provide such cost share and evidence **a process for integrating the cost share into the collaborative research program.**

Evaluation and Award: Evaluation and Award in connection with this PA will be performed in accordance with **PART II.E.** Whitepapers and Proposals that are in compliance with the requirements of the PA will be evaluated in accordance with the evaluation factors using an adjectival and color rating system. A Source Selection Evaluation Board (SSEB) will evaluate the Whitepapers and Proposals. The SSEB consisting of qualified groups of scientists, managers, and cost specialists, will evaluate each Whitepaper and Proposal and provide the results of that evaluation to the Source Selection Authority (SSA). The SSA will make decisions concerning the Whitepaper downselection and award selection.

II. DETAILED INFORMATION ABOUT THE FUNDING OPPORTUNITY

A. FUNDING OPPORTUNITY DESCRIPTION

1. 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 U.S. Army Research Laboratory (ARL) has established an Enterprise approach to Cyber Security that couples multi-disciplinary internal research, analysis, and operations with extramural research and collaborative ventures. ARL intends to establish a new collaborative venture – The Cyber Security Collaborative Research Alliance (CRA) – that seeks to advance the theoretical foundations of cyber science in the context of Army networks. This Collaborative Research Alliance will consist of academia, industry and government researchers working jointly to solve complex problems. The overall objective of the Cyber Security CRA is to develop 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.

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 Supervisory Control and Data Acquisition (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: Large attack surface, relatively disadvantaged assets, large scale and high dynamics, and advanced persistent threats.

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[1] [NITRD 2012]. 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 Security CRA is the lack of understanding of cyber phenomena, particularly the fundamental laws, theories, and

[1] [NITRD 2012] *The Networking and Information Technology Research and Development (NITRD) Program: 2012 Strategic Plan*. Executive Office of the President, National Science and Technology Council, July 2012. Online at: www.nitrd.gov/pubs/strategic_plans/2012_NITRD_Strategic_Plan.pdf

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[2]. 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 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, 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

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 strongly believes that a joint collaborative approach by multidisciplinary researchers is required to make fundamental advances towards meeting the CRA goal to develop a fundamental understanding of 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 context 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 Cross-Cutting Research Issue (CCRI) addressing Psychosocial Effects must be jointly studied in the context and the constraints of the three Research Areas. It is expected that other CCRIs will emerge as the research progresses.

---

[2] *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development* Program, Executive Office of the President -National Science and Technology Council, December 2011. Online at http://www.nitrd.gov/fileupload/files/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

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 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 PA 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. This research must develop appropriate mathematical representations, metrics, models, and analysis techniques. Expected outcomes are autonomous anticipation of, and adaptation to threats which can eliminate costly, labor-intensive defensive measures and repairs to networks, thus significantly simplifying the complexity of cyber security management and of 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 should be a critical aspect of the proposed research.

The CRA is intended to create a collaborative environment that enables an Alliance of participants from the Consortium and Government to advance the state of the art and assist with the transition of research to enhance the performance of cyber technologies of interest to the U.S. Army. The CRA will work collaboratively with ARL's internal research program and other ARL-led collaborative ventures, to identify areas where joint, multi-disciplinary, collaborative cyber security research can advance ARL's Cyber Security Enterprise long-term vision. Collaborative research, as well as transition links among the CRA and the ARL internal program, will also be pursued and defined through continuous collaboration, technical exchanges, site visits, staff rotations, and mutual participation in formulating the program, performing the research, and in technical reviews during the period of performance. This will strengthen the relevance of CRA research and enable the transition of research results.

2. ARL Internal Mission and Related Programs

The Cyber Security CRA will become an integral part of ARL's Enterprise in Cyber Security. Collaboration with the internal cyber security research program is critical to its success, and interactions with other related ARL research programs may bring different insights to bear on the CRA's research problems. Moreover, interactions with ARL's analysis and operations elements may increase relevance of CRA research and eventually lead to transition of research results.

ARL's Internal Mission

The U.S. Army Research Laboratory (ARL) is the Army's corporate research 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 CRA researchers will collaborate with researchers in these Directorates. ARL will specifically fund in-house staff to foster direct highly collaborative partnerships between Consortium and Government researchers.

ARL's Army Research Office (ARO) serves as the Army's premier extramural basic research agency and it is expected that there may be opportunities to interact with their extramural programs. 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 serve not only to provide protection from sophisticated cyber threats, but also as an experimental laboratory that 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, and 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

[3] www.arl.army.mil

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 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 insure 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. The ARL/ARO program also includes Multi-Disciplinary Research Initiatives (MURIs). Two topics from the FY13 call of potential relevance to this CRA are: Reduced Cyber-system Signature Observability by Intelligent and Stochastic Adaptation; and Controlling Collective Phenomena in Complex Networks[4].

- **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 to be 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 in order to allow an 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.

[4] http://www.arl.army.mil/www/pages/8/research/12-020.pdf

Related Program at ARL.

- **Network Science (NS) Collaborative Technology Alliance (CTA)[5].** 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 Security CRA should leverage the developments in the work on Trust and social/cognitive networks in the NS CTA.

- **Cognition and Neuroergonomics CTA (CAN CTA)[6]**. 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 Alliance 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. Collaborations between researchers in the Cyber Security CRA and the CAN-CTA may be beneficial.

- **Mobile Networks Modeling Institute (MNMI).** The Institute 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

[5] www.ns-cta.org
[6] www.cancta.net.

be employed. The goals of the Institute 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 Security CRA to provide the ability to simulate, emulate, and test large-scale, highly mobile, *ad hoc* networks with enough fidelity to quantify the performance both technically and operationally.

3. CRA Programmatic Strategy

The CRA is intended to foster collaborative basic research (Budget Activity 1-see definition below) involving the Consortium and the Government. ARL's strategy is to continue exploiting research and expertise where it exists through the issuance of a single award through this Program Announcement (PA) to a Consortium of academic, industrial partners, and/or non-profits entities. This Consortium will work in collaboration with ARL scientists and engineers to advance cyber security research of relevance to the Army. ARL and the Consortium selected for award will establish an Alliance to address research topics critical to cyber security. Additionally, other government agencies (both domestic and possibly international) may participate in the CRA and contribute their technical expertise, personnel and facilities. A significant goal of this effort will be to create a critical mass of collaborating academic, private sector and government scientists and engineers focused on solving the research challenges outlined within the scope of the CRA. This intellectual synergy is also expected to include sharing equipment, personnel and facilities to promote efficiency and collaboration.

ARL will award under a separate Broad Agency Announcement a contract for experimentation and applied research efforts to mature cyber security research for the ARL Cyber Security Enterprise. After award of this contract, the contractor selected for award (hereinafter referred to as the "BAA Partner") will be added as a Member to the Consortium selected as a result of this PA in accordance with the provisions to add a new member under the Articles of Collaboration (see PART II.A.). The Consortium will allocate $350K per year of the annual CA funding for this member's participation once selected and added to the agreement. The role of the BAA Partner in the Consortium will be to conduct cyber security research and unclassified experimentation of CRA research results. In addition this industrial member will support the Consortium through its efforts under the contract by conducting sensitive and classified experimentation including extended empirical analysis for these experiments as part of an applied research effort. This will be used to inform the Government as to the applicability and technology transferability of research results from the CRA.

Based upon the gaps discussed in Section 4 and the resources identified in Section 7, the research and collaboration strategy developed by the Offeror should adopt a systematic approach to fundamental research focused on understanding cyber phenomena, leading to

an elucidation of fundamental laws, theories and theoretically grounded and empirically validated models that enable design of cyber defense tools. Offerors must carefully choose research topics to ensure a critical mass of researchers addressing the challenges proposed. Offerors are expected to apply relatively equal resources to each of the three Research Areas: Risk, Detection, and Agility. Further, a portion (approximately 15%) of the research dedicated to each area must address the Psychosocial Effects CCRI. The CCRI resources are an integral part of the Research Area efforts.

It is the intent of this PA to solicit the most creative, innovative, and flexible approaches to the ultimate goal of generating and exploiting research to solve pressing research gaps and issues impacting both the military and commercial sectors. This PA seeks Whitepapers (and Proposals from those who receive a subsequent invitation to submit a Proposal based on their Whitepaper submission) from self-formed consortia, each led by an academic institution, which will result in the award of a single cooperative agreement. In response to the PA, Offerors will be required to:

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

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

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

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

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

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

This programmatic strategy provides the structure for the desired comprehensive and cohesive outcome of the basic research performed under the CRA. The core basic

research program will be initially funded under Budget Activity 1 (basic research) funding. However, the CRA will also allow participation from other Government agencies and may result in additional Budget Activity 1 (basic research) funding as well as Budget Activity 2 (applied research) funding (**see discussion of Enhanced Program below**). Therefore, the research proposed and performed must comply with the definition for Budget Activity 1 or Budget Activity 2 funding (as appropriate) as outlined in the DoD Financial Management Regulation (FMR), Volume 2B, Chapter 5 (September 2012) as follows:

- **Budget Activity 1: Basic Research.** Basic research is systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind. It includes all scientific study and experimentation directed toward increasing fundamental knowledge and understanding in those fields of the physical, engineering, environmental, and life sciences related to long-term national security needs. It is farsighted high payoff research that provides the basis for technological progress. Basic research may lead to: (a) subsequent applied research and advanced technology developments in Defense-related technologies, and (b) new and improved military functional capabilities in areas such as communications, detection, tracking, surveillance, propulsion, mobility, guidance and control, navigation, energy conversion, materials and structures, and personnel support. Program elements in this category involve pre-Milestone A efforts.

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

4. CRA Research Strategy

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 PA are as follows.

- **Cyber Security**: For the purposes of this PA, 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 CRA will necessarily focus only on a few carefully circumscribed aspects.

- **Cyber Science**: What exactly would constitute "cyber science" remains a topic of growing discourse to which this CRA will be an important contribution. For the purposes of this PA, 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 operate in this constrained 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. Research Areas (RAs) and Cross Cutting Research Issue (CCRI)

To achieve the CRA's vision, a radical departure from current research models where research areas proceed independently along stovepipes is imperative. The Cyber CRA is expected to establish a new way of conducting cyber security collaborative research that breaks down research barriers, builds new collaborative relationships, and develops mutual understanding across organizations, technical and scientific disciplines, and Research Areas.

The three Research Areas and CCRI for this 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. Risk assessment should take into account the context of the mission. Research in this area should lead to theoretically-grounded techniques and tools to synthesize, modify, adapt, or redesign algorithms that reliably compute risks imposed by new cyber threats to Army networks and imposed by changes to networks to counter or avoid such threats.

- **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 malicious activity, and of properties of

Army networks. This research should inform development of approaches to rapid (potentially in the midst of a battle) adaptation of a detection technique or algorithm as new threats emerge.

- **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.

- **Psychosocial Effects.** Each of the three Research Areas must take into account the Psychosocial Effects Cross Cutting Research Issue. 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. Thus, since teams of human defenders will likely be the key link in cyber defense, a theoretical understanding of the socio-cognitive factors that impact the decision making of the user/Soldier, defender/analyst, and adversary needs to be developed. As examples: the Risk RA should leverage and develop theories of how users evaluate risk and make decisions regarding cyber security, both as individuals and as members of teams since effective cyber defense will require information sharing between users and defenders. The Detection RA must take into account the detectability and predictability of adversary activities. The Agility RA should take into account models of adversarial behavior. It is expected that the Psychosocial Effects will serve as an integrating factor across the three Research Areas.

An overarching goal of cyber security is to significantly increase the cost incurred by adversaries in undertaking cyber attack while minimizing the loss in performance (such as overhead and availability) incurred by our networks. CRA research should create a framework that effectively integrates the knowledge of our cyber assets and potential capabilities and approaches of our adversaries, and provides dynamic defense mechanisms that adjust dynamically to changes of mission, assets, vulnerability state, and defense mechanisms. Comprehensive cyber situation awareness ultimately leads to effective defense.

Research proposed should be substantially different from classical approaches, and they must fit coherently together. Research should not be stove-piped as there are significant inter-dependencies between Risk, Detection and Agility. As examples, agile changes in the friendly network make detection of malicious activity more challenging; Risk to a network is diminished with stronger detection mechanisms; and one could trade off risk for agility. The proposed research must be supported by a principled experimentation

validation plan. While elements of such a plan may be specific to a research area, it is expected that a cohesive validation plan would span all research.

The research goals to be addressed by the Offeror in each of the research areas are discussed in the following sections. Research in each of the areas of Risk, Detection, and Agility must be performed in the context and constraints of complementary research in the other areas. Collaborative crosscutting research that spans the three Research Areas should lead to insights on the underlying human elements intrinsic to cyber security as well as insights into the interrelationships and interdependencies between the research areas that are the focus of this CRA. Crosscutting research should lead to deep, persistent, and meaningful collaboration among the Alliance and should harmonize vocabularies, ontologies, metrics, structures, and processes to build understanding across the three Research Areas.

c. Risk Research Area

The ability to assess risk to cyber systems is critical to defending and restoring networks. The term "risk" is used as shorthand for a broader ensemble of research issues, including but not limited to anticipation and characterization of vulnerabilities and susceptibilities, exploitable dynamic networks, relations between threat characteristics, defense mechanisms, network features and properties, and the likely mission impact. Risk assessment is essential to determining the criticality of cyber assets, effectiveness of defense systems (including the detection of threats), provisioning of resilience (such as agility measures), and meeting mission assurance requirements. Commanders seek to understand cyber risks to their networks and cyber assets and their impact on the mission in order to make effective decisions.

In general, risk is defined as the probability that an adverse event or action occurs and results in a negative impact or consequence. In the context of cyber security, risk refers to the expected likelihood and consequences of threats or attacks on cyber assets. Risk assessment involves identifying threats and vulnerabilities, computing the likelihood of threats, and then determining the impact and consequences of an adversary exploiting these vulnerabilities. Risk management is basically the process of first assessing risk and then taking necessary actions to avoid, transfer, mitigate, or control it to an acceptable level by considering the costs and benefits of the actions [DHS 2011][7].

In current practice, the result of risk assessment is seen as enumeration of system assets along with associated vulnerabilities and threats. Most current risk assessment methodologies are grounded in threat identification and classification, vulnerability identification, and determination of impact.

Current risk assessment approaches are based on known vulnerabilities and static system behavior, and the typical result of a risk assessment is an enumeration of system assets

[7] [DHS2011] "Risk Management Fundamentals," US Dept of Homeland Security, April 2011, http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf

along with associated vulnerabilities and threats. Such static approaches cannot cope with high dynamism in a real-time situation with changing threats and attacks, network conditions and structure, and attack-defense dynamics especially at the tactical edge. Systems of interest to this CRA are typically very large, complex and inter-connected, so that obtaining precise, complete and timely state information is infeasible. Additional sources of uncertainty arise from the inherent randomness of the systems, inaccuracies in the detection of threat, and the dynamics of the adversary-defender interactions. It is expected that the stochastics exhibited by such systems will not be linear or stationary. Risk assessment schemes should adapt to new threats, and should have the capability to anticipate and react to unforeseen circumstances. As of yet, very little risk assessment research has looked at unknown or zero-day attacks and their likelihood, potential impact, and remediation.

Furthermore, current methods do not take into account potential unknown threats and vulnerabilities, attack-defense interchanges, non-linear vulnerability exploitation, and adversary intent and capability. They do not scale well with network size and complexity. In this context, there is also a need to develop appropriate metrics.

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

- Lack of models of psychosocial effects related to risk including adversary intent, capabilities, goals, etc. and defender and user comprehension of estimated/predicted risk, uncertainty, and impact to network performance and capabilities.
- Inadequate metrics for calculating and validating risk.
- Lack of theoretical principles focusing on risk associated with impact on broad network function rather than individual components
- Lack of approaches analyzing on-the-fly risk analysis with real-time attacks and changing threats, network conditions and structure, and attack-defense dynamics
- Lack of approaches to assess risk in the face of unknown system vulnerabilities

Research in this area must take into account the tradeoff between risk and detection, and risk and agility, and it also must take into account psychosocial factors (such as adversary's intent, capabilities, goals) related to risk. More precisely, assessment of risk must be informed by the adversary's intent, capabilities and goals. It is affected by the agility of defensive maneuvers and, in turn, it dictates the tempo of such maneuvers. Proposed research must develop the basic science, driven by empirically derived models and validation.

The following paragraphs contain a required topic (the first topic listed) to be addressed and some suggested topics and issues for consideration. Except for the required topic, this should be understood as suggested topics and issues for consideration in formulating the research to fill some of the above-identified gaps, rather than being definitive or exhaustive. Indeed, it is expected that competitive proposals will contain other

innovative topics and approaches, and may identify other gaps. The inherent nature of the problem calls for a multi-disciplinary approach.

- The Offeror will develop new holistic conceptualizations and definitions of risk, resiliency and robustness under an adversarial setting.

- Risk frameworks that cope with the stochastics of the system which are not expected to be linear or stationary. The many sources of uncertainty in the system coupled with the dynamics of the adversary-defender actions and interactions call for a new robust risk and resiliency framework, perhaps exploiting game- or control-theoretic perspectives.

- Risk assessment approaches that effectively deal with uncertainty and scale with partial and inaccurate knowledge. Cyber systems of interest to this PA are generally very large and complex, and precise or complete system information is infeasible.

- Approaches to develop a principled assignment of trust to risk computations. May consider data provenance to help these computations and in information integration.

- Decision theory may be of value in characterizing the psychosocial effects in risk assessment.

d. Detection Research Area

Detection of malicious network and host-based activities is integral to the assessment of risk and reconfiguration of cyber defense mechanisms. The term "detection" is used as shorthand for a broad ensemble of research issues, including but not limited to discovery of novel types of malicious attacks and other activities on friendly networks; analysis, recognition and characterization of the malicious activity; and elements of forensic analysis of the activity. Detection of malicious cyber activities, often known as intrusion detection, is a central concern in this research area, and has been the much studied topic.

Most intrusion detection systems (IDS) are based on signature-based techniques, which match observed activity against specific rules or patterns of known malicious behavior. This has the advantage of high accuracy but cannot detect new attacks (no known signature). Anomaly detection techniques identify what is abnormal or out of place, and thus can potentially cope with new attacks, but suffer from poor accuracy and often rely on sensitive or unavailable data about normal activities. Differentiating between normal anomalous behavior and that due to malicious activities is a critical challenge.

Approaches to improve the performance of anomaly detectors include narrowing the scope of the detector, providing side information, or the use of multiple detectors[8].

While tools such as Snort are employed to aid detection of well-known threats, algorithmic approaches have not been able to match the cognitive capability of human analysts to intuitively detect new threats and recognize the type of threat observed[9]. Algorithmic approaches such as data mining, clustering and outlier detection do not yet capture the analyst's cognitive process. This is partly due to gaps in the underlying knowledge as to how analysts perform their tasks (i.e., the neuroscience and psychosocial models are lacking). Thus, modeling cognitive processes of both individual and teams of analysts, with the aim of algorithmic implementation, is of interest.

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

- Lack of theoretical models relating the manifestations of malicious activity to underlying fundamental properties of the activity, and its relationship with properties of friendly and adversarial networks.
- Limited principled approaches for the detection and analysis of advanced persistent threats.
- Lack of a theoretical framework to detect new and emerging threats.
- Limited understanding of the cognitive processes of analysts and of how these processes can be modeled algorithmically to improve threat detection.
- Incomplete characterization of threats, threat types, and their identification, particularly advanced persistent threats.

Research in this area must not be stove-piped and must inform and be informed by the developments in the other two research areas given the strong inter-dependencies between the three Research Areas. Detection research should take into account the richness of interactions between different approaches to enhancing cyber security. For instance, an assumption associated with cyber maneuver is that dynamically changing the visible attack surface of the network will improve the overall defense of the network. Research in Detection should take into account the potential impact of this changing network environment on the ability of the cyber defense analysts to identify and correlate events for the detection of threats. The reliance on network analysts underlines the importance of psychosocial factors, for instance: How will developed techniques affect the analyst working alone or as part of a team? How can we develop techniques to improve the effectiveness of the cyber analyst? Can we model the cognitive processes of

[8] Such an example is described in the SBIR topic OSD12-IA4 Novel Detection Mechanisms for Advanced Persistent Threat. http://www.acq.osd.mil/osbp/sbir/solicitations/sbir20123/osd-re123.htm

[9] For example, *usable security* and *insider threat* are focal points of a recent Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD) Broad Agency Announcement (BAA).

the best analysts and capture them algorithmically? The interplay between detection and risk is clear (improved detection can increase the confidence in risk assessment and higher tolerance for risk can lower detection requirements).

The following paragraphs contain a required topic (the first topic listed) to be addressed and some suggested topics and issues for consideration. Except for the required topic, this should be understood as suggested topics and issues for consideration in formulating the research to fill some of the above-identified gaps, rather than being definitive or exhaustive. Indeed, it is expected that competitive proposals will contain other innovative topics and approaches, and may identify other gaps. The inherent nature of the problem calls for a multi-disciplinary approach. Detection models should be general enough to include network environments that are not commonly studied today, such as tactical ad-hoc mobile networks, cloud computing, SCADA networks, networks executing cyber maneuvers, etc.

- The Offeror will develop a foundational science leading to theory and techniques for effective non-signature based detection of advanced persistent threats. This will require a broad view of the attacker world: history of prior attacks; related techniques of other attackers, trends; psychosocial characteristics of attackers and defenders, both formal and informal, organized groups and individuals.

- Development of models that relate manifestations of malicious activity to fundamental underlying properties of the activity and that of friendly and adversarial networks.

- Threat models and characterization of threats and their attacks that can differentiate between malicious activities and benign anomalies. Recognition and characterization of threats and their levels of sophistication.

- Novel techniques for adaptively compressing the data and for adaptive collection, taking into account the network characteristics and impact on accuracy and complexity. Data collection in a bandwidth constrained environment is particularly challenging, especially as the network size and threat frequency increase.

- Modeling of cognitive processes of analysts leading to improved threat detection theories and algorithms.

- It is unlikely that the following lines of research would be productive for the purposes of this CRA: ad-hoc development of visual displays for detection; signature-based detection techniques; approaches limited to currently known threats; approaches limited to current or static network environments.

e. Agility Research Area

In the face of a perceived threat, and risk assessment that indicates potentially major degradation and dislocations of the friendly network, the network can be reshaped (i.e., "maneuver" in the space of network characteristics and topologies) so as to alter the real and apparent vulnerability surface perceived by an adversary. This maneuver should minimize the network's further vulnerability to observed and anticipated threats, while maximizing its utility for mission success. The maneuver should also take into account the accuracy of the threat detection, the confidence in the risk assessment, and the impact that the maneuver may have on adversary strategies and our subsequent ability to detect them. Solutions to this maneuver problem are handicapped by a lack of fundamental theories relating properties of the system, the available controls, and stability of the network, and exposures and vulnerabilities incurred during the maneuver. Research must take into account the multiple time and network scales at which malicious cyber activities occur.

The increasing complexity of modern cyber systems has led to standardization of services and components which eases the complexity of maintenance and management, but this has also led to static and reactive defense mechanisms. Homogeneity and static defenses increase vulnerability, particularly in the face of advanced persistent threats. Recent research efforts have attempted to tackle both fronts: make the systems (apparently) more heterogeneous to the attacker and the defenses more agile. Examples of randomization and enumeration are discussed in [ARL2011][10], [ARL2013][11] a series of papers resulting from an ARL organized workshop on Moving Target Defense. The DHS Cyber Security Roadmap [DHS2011][12] describes research challenges that are still relevant. Related programs are DARPA X, DARPA CRUSH and IARPA STONESOUP. Moving Target Defense has been identified as one of four strategic thrusts in the strategic plan for cyber security developed by the Cyber Security and Information Assurance Research and Development Senior Steering Group of the National Science and Technology Council[13].

The hypothesis behind `maneuver' is that randomization makes the attack surface stochastic, thus increasing the cost to the adversary. Randomization or intentional diversity increases the spatio-temporal entropy of the attack surface and it potentially increases the time required for the adversary to learn the network configuration and thus

---

[10] [ARL 2011] S. Jajodia, A.K. Ghosh, V. Swarup, C. Wang, X.S. Wang, Eds., *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*, Springer Advances in Information Security, vol. 54, Berlin, 2011.

[11] ARL 2013] S. Jajodia, A.K. Ghosh, V.S. Subrahmanian, V. Swarup, C. Wang, X.S. Wang, Eds., *Moving Target Defense: Application of Game Theory & Adversarial Modeling*, Springer Advances in Information Security, vol. 100, Berlin, 2013.

[12] [DHS2011] "Risk Management Fundamentals," US Dept of Homeland Security, 2011, https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=257736.

[13] [CSIA 2011] D. Maughan and W. Newhouse, *Trustworthy cyberspace: strategic plan for the federal security research and development program*; Executive Office of the President; National Science and Technology Council; CSIA R&D SSG, December 2011. Online at http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

decreases the opportunity for the adversary to effectively exploit whatever vulnerabilities it may have assessed, and it potentially thwarts the spread of adversarial actions in space and time.

Absent from the current work, however, is a system theoretic approach that takes a holistic view of adaptation at different layers, at different time scales, and across the network. Randomization clearly entails a cost: in terms of overhead for effecting maneuver and the resulting complexity of network management as well as potentially degraded services, perhaps measured by delay or availability, as different parts of the network adapt differently to locally perceived threats. The last point implies that both microscopic as well as macroscopic models need to be developed. Randomization, as described above, is one element of deception and obfuscation, and a complete theory of deception and obfuscation needs to be developed, taking into account psychosocial factors.

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

- Lack of firm theoretical foundations for stochastic, adaptive and proactive cyber maneuver.
- Limited models that take into account the impact of the human, both the adversaries (objectives and strategies) and the defenders (strategies and performance metrics).
- Lack of theories and models that analytically describe the dynamic control laws that will result in the desired end state, given the partially known adversarial and friendly environments. This includes a lack of knowledge of what can and cannot be controlled, and the impact on network properties.
- Inadequate metrics to measure effective cyber security, and thus lack of understanding of fundamental limits and tradeoffs between the cost of a maneuver (to both friends and foes) and effective cyber security.
- Absence of a systems approach that quantitatively describes the tradeoffs between increase in adversary's workload and increased cost incurred by the friendly network.

A successful research program would lay the scientific foundations for a theory of cyber maneuver by combining new developments in theory, innovative extensions/exploitation of existing theory, computationally efficient modeling and simulation techniques, empirically driven model development, and principled experimental validation. Research in this area must not be stove-piped and it must inform and be informed by the developments in the other two research areas given the strong inter-dependencies between the three Research Areas. Agility in defense requires deep understanding of cyberspace, and solutions must be linked to our ability to detect threats and to assess risk. Scenarios and problems considered must be relevant to Army networks.

The following paragraphs contain a required topic (the first topic listed) to be addressed and some suggested topics and issues for consideration. Except for the required topic, this should be understood as suggested topics and issues for consideration in formulating the research to fill some of the above-identified gaps, rather than being definitive or exhaustive. Indeed, it is expected that competitive proposals will contain other innovative topics and approaches, and may identify other gaps. The inherent nature of the problem calls for a multi-disciplinary approach. The inherent nature of the problem calls for a multi-disciplinary approach which may include (in addition to traditional constructs from computer science, mathematics and network security):

- The Offeror will develop novel mathematical theories and models leading to algorithms to affect a desired maneuver end-state, in a non-stationary setting, with partially known dynamics and deliberate obfuscation attempts by the adversary.
- Learning techniques to ascertain the adversary's utilities, strategies and motives that use only partial and inaccurate information and that evolves. On-line learning could draw upon social and behavioral sciences, and non-cooperative game theory may provide insights.
- Composability of disparate randomization mechanisms that work at different spatio-temporal scales, perhaps via a systems approach.
- A theory of deception for cyber maneuver, beyond the use of honeynets, tar traps and rabbit holes, taking into account psychosocial factors behind deception.
- Insights on the design of distributed defenses for a complex system against previously unknown attacks. Bio-inspired concepts may be applicable and include distributed control, multi-layered protection, and diversity.

f. Psychosocial Effects as a Cross-Cutting Research Issue (CCRI)

The human is central to cyber security, as a significant part of the problem as well as the solution. In the cyber security domain there are three human elements: the user/Soldier, attacker/adversary and the analyst/defender. Current approaches to cyber defense have focused on the defender and developing tools and techniques to enable the defender to detect and prevent cyber attacks, to include methods for improving end user compliance with established security policies. There is a significant research gap as the user and adversary elements have been inadequately addressed in the current theoretical models and theories used in cyber security. All three human elements will influence the calculation of risk, the interpretation of detected events, and the selection and timing of the agility measures instituted manually or recommended by automated systems. Understanding the cognitive processes underlying individual and analyst team performance will open new avenues for algorithmic development. Similarly understanding the attacker, their processes, and their strategies is critical to developing effective defense strategies. Further, characteristics of user and analyst team personality (such as risk aversion), perceptual abilities, stress level, and workload will influence their ability to interpret information about a threat both individually and as part of an effective

cyber defense team and take appropriate proactive and defensive actions[14,15]. Thus, enhanced understanding of all three human elements is important to ensure effective cyber security in the face of dynamics in a fundamentally adversarial cyber domain.

The preceding sections have articulated the importance of psychosocial factors to the areas of risk, detection, and agility. Since psychosocial factors affect all aspects of cyber defense, it emerges as a unifying cross-cutting theme. Rather than treating psychosocial factors as a distinct research area, Offerors must propose a cross-cutting research problem that spans the three research areas with significant focus on psychosocial factors.

As with the three research areas, research proposed under this CCRI must develop the basic science with theoretically driven and empirically-validated models of the psychosocial factors and their roles and impacts in Risk, Detection and Agility. These models must capture the behaviors of individuals and teams of defenders, of adversaries, and of the end users, and must take the assumption that not all aspects of risk, detection, and agility will occur autonomously or transparently or without incurring some cost to the Soldier reliant on the network for operations. It is expected that these models will to inform the research in the three RAs.

If a human being is the key link in cyber defense then a theoretical understanding of the socio-cognitive factors that impact the decision making of the user, defender, and adversary needs to be ascertained. Who makes a good user, defender and adversary? What attributes of effective teams of defenders will most impact the three Research Area of Risk, Detection, and Agility? The consideration of individual factors may elucidate this question (e.g., cognitive styles, biases, culture factors, and motivation).

Effective cyber security requires detailed models of human decision-making with respect to risk, detection, and network agility. Can we build a model of who is guarding or breaking into our networks? Factors that might influence adversarial intent are motivation, capability, process, techniques, and potential impact of the intended action. If we are able to successfully model the intent of the attacker and thereby predict likely next actions, our agile networks may be able to prevent or greatly diminish the effectiveness of the attack. The user is actively engaged with networked systems and interacts, albeit indirectly, at many points in time with the defender. An in depth model of how users and defenders, either individually, in groups, or collaboratively evaluate risk and make decisions regarding cyber security is needed, particularly when such actions must be made under conditions of uncertainty, based on the output of complex models and algorithms, and may have adverse effects on network performance.

The following paragraphs contain a required topic (the first topic listed) to be addressed and some suggested topics and issues for consideration. Except for the required topic, this should be understood as suggested topics and issues for consideration in formulating the research to fill some of the above-identified gaps, rather than being definitive or

[14] Department of Homeland security (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD) Broad Agency Announcement (BAA). http://www.cyber.st.dhs.gov/

[15] STTR topic OSD12-T08: Effective Cyber Situation Awareness (CSA) Assessment and Training.

exhaustive. Indeed, it is expected that competitive proposals will contain other innovative topics and approaches, and may identify other gaps. The inherent nature of the problem calls for a multi-disciplinary approach.

- Offerors will develop theoretical models of the cyber defender, emphasizing teams of defenders rather than solely individuals, leading to improved cyber defender effectiveness. These models should aid development of algorithms directly representative of and supportive of these cognitive processes.
- Unifying theories and models exemplifying the relationships and impacts between cyber security capability, cyber defense analysts, end users, and attackers.
    - The relationship between human perception, cognition, and biases for the decision making process of the user to avoid risk.
    - Factors that make a user vulnerable and/or resistant to cyber attacks.
    - The role of agility, both individually and collectively, in responses to a cyber attack or network changes.
- Theories of cyber attack and defense strategies under partial and imperfect observations
- Detectability and predictability of attacker activities under given conditions or in response to defenders' actions
- Models of attacker decision-making in its organizational or social setting in the context of cyber attack.
- Models for inferring attacker intent and capabilities based on observed behavior and inferred motivation and goals, for predicting likely future (immediate, near, and longer term) action, and for identifying the attacker based on such inferred higher-order "signatures."

A successful research program in this CCRI would develop theories and models describing the effects of psychosocial processes on risk, detection, and agility.

5. Collaboration

a. Background

This program continues the ARL concept of creating Alliances (Army Collaborative Technology Alliances (CTAs) and Collaborative Research Alliances (CRAs)) to facilitate a close collaborative relationship between ARL and its partners. Experience has shown that persistent collaboration between government, academia, and industry enhances innovation and has a high return on investment. Therefore, collaboration between Consortium and Government researchers is integral to the execution and success of the CRA. It is ARL's strong belief that work conducted under the Cyber

Security CRA cannot be successful either in whole or in part without collaboration. That is, collaboration among the members of the Consortium and the Government Members of the Alliance is integral to the execution of the research program, especially the Psychosocial Effects CCRI and to jointly address the challenges associated with cyber security risk, detection, and agility. Creation of an environment that is conducive to collaboration is therefore a critical element in establishing the Alliance. This section describes collaborative opportunities and potential avenues to collaborate under the CRA. The implementation of the collaboration with ARL will be through the proposed Initial Program Plan (IPP) and the subsequent Biennial Program Plan (BPP). Offerors are invited to suggest additional new and innovative avenues for fostering collaboration among Alliance partners.

b . Collaboration Opportunities

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

c. Staff Rotation

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

All salary and travel costs associated with the rotation of Government personnel will be borne by the Government. All salary and travel costs associated with staff rotations of

Consortium members will be funded under the CA or may be provided by the Consortium member as cost-share. There should be a balance of staff rotations across all the partners in the Consortium and across all the research areas. It is anticipated that some portion of the Consortium's scientific labor-years will be in staff rotations.

d. Lectures, Workshops, and Research Reviews

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

6. Management

a. Background

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

b. Overall Management Concept

ARL and the Consortium will establish a Collaborative Research Alliance. Additionally, other Government agencies may be invited to join this Alliance and to contribute, as appropriate, their technical expertise, personnel, access to research facilities and funding. The Alliance will strive for a focused, yet flexible research environment. To accomplish this, the consortium should consist of a small number of academic and industrial organizations, optimally sized with no more than six members (including the Lead Research Organization (LRO) and BAA Partner to be added after award of contract as described in PART II.A.3), possessing significant expertise in one or more of the research areas covered by the CRA, led by a single organization, the LRO, with the ability to integrate the broad palette of research required to realize the goals of the CRA. Each of these entities will be a full Member of the consortium and possess equal voting rights in accord with the Articles of Collaboration.

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

c. Technical Guidance and Oversight

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

- The **Lead Research Organization (LRO)** is expected to provide research leadership, create and foster deep and persistent multidisciplinary research, perform lightweight administrative duties, and conduct fundamental research in cyber security. This includes participating in the research, promoting research to technology, distributing Government funding to Consortium Members in accordance with the approved IPP/BPP under the agreement, and maintaining proper research invoicing.

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

- **Program Manager (PM).** The CRA Program Manager (PM) is the Consortium's scientific representative charged with the Consortium's overall responsibility for management and guidance of the cooperative agreement. The PM will be designated by the LRO and be a member of that organization. The CRA is expected to be the primary responsibility of the individual assigned as PM and a commitment of time commensurate with this responsibility is also expected. The PM is required to be an eminent scholar in the field of Cyber Security and have the stature, experience and leadership skills to successfully execute the CRA program. The PM may need to reduce any teaching schedule commitments commensurate with the duties required to manage the CRA. It is also recognized

that the PM may require staff support to manage and execute the cooperative agreement, and this should be included in the CRA submission.

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

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

d. Articles of Collaboration (AoC)

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

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

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

are hereby informed that such changes must be acceptable to the Government for the Offeror to be eligible for award.

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

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

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

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

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

- Changes in the scope or the objective of the program, IPP/BPP, or research milestones;
- Change in the key personnel specified in the IPP/BPP;

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

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

- Changes to the Articles of Collaboration if such changes substantially alter the relationship of the parties as originally agreed upon;
- Solicitation or acceptance of funding under the agreement from sources other than ARL; and
- Changes in Consortium membership. It is expected membership will change as technical efforts progress and resource levels change.

f. Collaboration and Technical Review Meeting

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

g. Evaluation For Five-Year Extension

The CRA will be awarded for a five-year period beginning in FY13. There will be an option to extend the CRA for an additional five years. At the end of the fourth year, a comprehensive program review will be conducted as directed by ARL. This review will consider cumulative performance metrics, the Consortium's vision for the additional five-year period of performance (to be submitted by the Consortium at the end of the fourth year), funding availability and the current research needs and goals of the US Army. Performance metrics are expected to include items that provide an indication of the CRA's accomplishments, the number of refereed journal and conference articles, invited presentations, patents, relevance of the work to ARL, collaboration, and staff rotation. The decision as to whether to exercise the option is expected to be based on the results of the review and evaluation described above.

h. Distribution of Funding

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

7. Funding

The estimated funding levels for the CRA over the projected period of performance, including options years, is shown in the top part of Table 1. The funding includes all known costs associated with the CA, i.e. the costs for research, program management, experimentation, travel, etc. The key assumption is that the CA will be awarded in the 4th quarter of FY13. Proposed guidance for unfunded Enhanced Program funding is also depicted in the bottom part of Table 1.

Award will be made to the Consortium that offers the best value to the Government. Members must recognize and understand that there are no guarantees associated with the levels of funding for each Member during the period of performance. All Members may be expected to compromise and sacrifice anticipated funding to their organization as necessary and appropriate to meet the goals and objectives of the CRA as established through the collaborative planning process. The government reserves the right to direct ten percent (10%) of the annual research funds to ensure flexibility in exploring high-risk research initiatives.

Enhanced Program

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

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

Funding Category	Core Research Program ($M)* Fiscal Year										
	FY14	FY15	FY16	FY17	FY18	FY19	FY19	FY20	FY21	FY22	**Total (10yr)**
Basic Research (6.1)	3.0	3.1	3.1	3.2	3.2	3.3	3.3	3.4	3.4	3.5	**32.5**
Core Total	3.0	3.1	3.1	3.2	3.2	3.3	3.3	3.4	3.4	3.5	**32.5**
	Enhanced Research Program ($M)										
Basic Research (6.1)	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	**5.0**
Applied Research (6.2)	1.0	1.0	1.0	1.0	1.1	1.1	1.1	1.1	1.1	1.2	**10.7**
Enhanced Total	1.5	1.5	1.5	1.5	1.6	1.6	1.6	1.6	1.6	1.7	**15.7**
Total	4.5	4.6	4.6	4.7	4.8	4.9	4.9	5.0	5.0	5.2	**48.2**

Note: Total Funded 10 Year Core Program $32.5M
Total Funded 10 Year Core and Unfunded Enhanced Program $48.2M
*Includes $350K/year for the Lead Industrial Member, 5% for Covered Educational Institution(s) and may be reduced by the 10% for high-risk research initiatives

B. AWARD INFORMATION:

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

C. ELIGIBILITY INFORMATION:

1. Eligible Applicants

During performance, it is envisioned that there will be Consortium Members and possibly Subawardees performing under the CA. The LRO has specific leadership and management responsibilities and roles as outlined below. Consortium Members are expected to have significant involvement and input on a long-term basis as outlined below. It is anticipated that an optimally sized consortium would include no more than six members (including the LRO and the BAA Partner to be added after award of the BAA contract as described in PART II.A.3), but this should not be considered a hard limit. Whitepapers and Proposals that include more than six members must provide a rationale for the additional members. The Government reserves the right to withhold 10% of the funding for high-risk research initiatives. In addition, covered educational institutions must receive 5-10% of the CRA annual funding. Thus, Offerors are expected to consider carefully the construct of their proposed Consortium and effectively engage the appropriate Membership and Subawardee performance to achieve the goals of the CRA.

To be qualified to be a Consortium Member, potential applicants must:

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

In deciding whether a recipient is otherwise qualified, the Grants Officer will ensure that the potential recipient: is not identified in the Government-wide Excluded Parties List System (EPLS) as being debarred, suspended, or otherwise ineligible to receive the award; has provided all certifications and assurances required by Federal statute, Executive order, or codified regulation, unless they are to be addressed in award terms and conditions at the time of award; and meets any eligibility criteria that may

be specified in the statute authorizing the specific program under which the award is being made.

Discussion of Consortium Members and other Participants in the CRA:

- **Lead Member called the Lead Research Organization (LRO)**:

  The preferred LRO is an advanced degree-granting educational academic institution under the amended Higher Education Act of 1965. This institution is also expected to have doctoral level courses of study in scientific and research areas related to this CRA that can result in the granting of a doctoral degree. The LRO critical roles include administration, collaboration enabler, and research leadership vision for the basic research and maintaining cross-Consortium collaboration and integration. This Member is expected to articulate a vision for the CRA, promote collaboration among Consortium Members, and coordinate crosscutting themes with Alliance Members. This Member is required to administer the Consortium, participate in the research, and promote the transition of research and technologies resulting from the research program within the CRA. This includes distribution of Government funding to Consortium Members and subawardees in accordance with the approved IPP/BPP under the agreement. The LRO is responsible for timely billing (invoicing) of executed research for itself and the other Consortium Members to ensure proper disbursement of government funds.

- **Consortium Members:**

  Each Consortium Member may be an industrial, non-profit, or academic institution but must possess substantial experience and expertise in the research areas contained within the scope of the CRA. Under special considerations outlined below Federally Funded Research and Development Centers (FFRDCs) and National Laboratories may participate in the Consortium as a Member. Academic members are expected to be advanced degree-granting educational institutions under the Higher Education Act of 1965 as amended. Academic Members are also expected to have doctoral level courses of study in scientific and research areas related to this CRA that can result in the granting of a doctoral degree. Industrial members are expected to have the ability to conduct appropriate research activities utilizing in-house engineers, scientists and facilities. All Members are expected to demonstrate opportunities for substantive collaboration with ARL, including appropriate opportunities for staff rotations and research collaboration.

- **Covered Educational Institutions**:

  The FY10 Department of Defense (DoD) Authorization Act, Public Law 111-84, provides authority for the Secretary of each military department to carry out a

program to provide assistance to "covered educational institutions" to assist DoD in defense-related research, development, testing, and evaluation activities. The term "covered educational institution" is defined to mean an **(1)** an institution of higher education eligible for assistance under title III or IV of the Higher Education Act of 1965 (20 U.S.C. 1051 et seq.); or **(2)** an accredited postsecondary minority institution. As defined under title III or IV of the Higher Education Act, "covered educational institution" includes Historically Black Colleges and Universities/Minority-Serving Institutions (HBCU/MSIs).[16]

Accordingly, it is a goal that covered educational institutions receive 5-% of the annual funding under the CA. This may be accomplished through one of the following: (a) a covered educational institution submitting the proposal as the LRO; (b) a covered educational institution being included as a Member or Subawardee in a proposal; or (c) the proposal including a plan for how the LRO will work collaboratively with the Government to identify a covered educational institution for participation in the program.

- **BAA Partner.**

  As stated above, ARL will award under a separate Broad Agency Announcement a contract for experimentation and applied research to mature cyber security research for the ARL Cyber Security Enterprise. The role of this Member in the Consortium will be to conduct cyber security research and unclassified experimentation to support CRA research. In addition this industrial member will support the Consortium through its efforts under the contract by conducting sensitive and classified experimentation including extended empirical analysis as part of an applied research effort. These experiments will be used to inform the Government as to the applicability and technology transferability of research results from the CRA.

- **Subawardees:**

  Consortium Members may be augmented with Subawardees to conduct specific research projects as necessary and appropriate to meet the goals of the CRA, especially for the conduct of new and innovative research for which they are particularly qualified. Subawardees are organizations that (1) are not expected to provide strategic input concerning the goals and direction of the CRA and (2) may possibly have only a short term relationship with the Consortium.

- **Federally-Funded Research and Development Centers (FFRDCs) and National Laboratories:**

  FFRDCs and National Laboratories may participate as Consortium Members or Subawardees but may not be the LRO, and their participation must be within the

[16] See the definition of an "eligible institution" at 20 U.S.C. 1067q which includes historically Black colleges and universities and other minority-serving institutions.

scope of their charter or sponsorship agreements. Further, FFRDCs and National Laboratories must cost-share an amount at least equal to the funding to be provided to them under the CRA.

2. Cost Sharing or Matching

Except for FFRDC or National Laboratory Members of a consortium, cost sharing is encouraged, but not required, to be responsive to the PA. During the evaluation of proposals, cost sharing will be evaluated as it relates to the evaluation factors listed in the PA, based on the degree to which the proposed cost sharing enhances the proposal to result in added benefits to the CRA Program. In order for the proposed cost sharing to receive appropriate credit during the evaluation process, the proposal should evidence **a firm commitment** (for example a written commitment from a duly authorized person who can bind the organization to provide the cost share) to provide such cost share and evidence **a process for integrating the cost share into the collaborative research program**.

3. Dun and Bradstreet Universal Numbering System (DUNS) Number and Central Contractor Registration (CCR)

I. *Central Contractor Registration and Universal Identifier Requirements.*

A. *Requirement for recipients.* Unless you are excepted from this requirement under 2 CFR 25.110, you as the recipient must maintain the currency of your information in the Central Contractor Registration (CCR) until you submit the final financial report required under this award or receive the final payment, whichever is later.

B. *Requirement for subrecipients.* If you are authorized to make subawards under this award, you:

1. Must notify potential subrecipients that no entity (*see* definition in paragraph C of this award term) may receive a subaward from you unless the entity has provided its Data Universal Numbering System (DUNS) number to you and is registered in the CCR.
2. May not make a subaward to an entity unless the entity has provided its DUNS number to you and is registered in the Central Contractor Registration.

C. *Definitions.* For purposes of this award term:

1. *Central Contractor Registration (CCR)* means the Federal repository into which an entity must provide information required for the conduct of business as a recipient. Additional information about registration procedures may be found at the CCR Internet site (currently at *http://www.ccr.gov*).
2. *Data Universal Numbering System (DUNS) number* means the nine-digit number established and assigned by Dun and Bradstreet, Inc. (D&B) to uniquely identify business entities. A DUNS number may be obtained

from D&B by telephone (currently 866–705–5711) or the Internet (currently at *http://fedgov.dnb.com/webform*).

3. *Entity,* as it is used in this award term, means all of the following, as defined at 2 CFR part 25, subpart C:
   a. A Governmental organization, which is a State, local government, or Indian tribe;
   b. A foreign public entity;
   c. A domestic or foreign nonprofit organization;
   d. A domestic or foreign for-profit organization; and
   e. A Federal agency, but only as a subrecipient under an award or subaward to a non-Federal entity.

4. *Subaward:*
   a. This term means a legal instrument to provide support for the performance of any portion of the substantive project or program for which you received this award and that you as the recipient award to an eligible subrecipient.
   b. The term does not include your procurement of property and services needed to carry out the project or program (for further explanation, *see* Sec. __.210 of the attachment to OMB Circular A–133, ‘‘Audits of States, Local Governments, and Non-Profit Organizations’’).
   c. A subaward may be provided through any legal agreement, including an agreement that you consider a contract.

5. *Subrecipient* means an entity that:
   a. Receives a subaward from you under this award; and
   b. Is accountable to you for the use of the Federal funds provided by the subaward.

D. APPLICATION AND SUBMISSION INFORMATION

The application process consists of a Whitepaper stage and a Proposal stage. The purpose of requesting Whitepapers is to minimize the effort associated with the production of detailed proposals for those 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. **Offerors that do NOT receive invitations from the Government to submit a Proposal are NOT eligible to submit Proposals and will NOT receive any feedback or a “debriefing.”** Offerors invited to submit Proposals will receive feedback on their Whitepaper that is expected to substantially improve their Proposal submissions. **If Offerors have NOT submitted a Whitepaper, they may NOT submit a Proposal for consideration for funding.**

1. Address to Request Application Package

Whitepaper. Offerors are responsible for submitting electronic Whitepapers so as to be received at the Government site indicated in the PA no later than the date and time specified in PART II.D.3. Whitepapers shall be emailed to usarmy.rtp.aro.mbx.baa2@mail.mil and must include a subject line of "WHITEPAPER – CYBER SECURITY CRA" 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.

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

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

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

Registration Requirements for www.grants.gov: There are several one-time actions that an Offeror must complete in order to submit an application through Grants.gov (e.g., obtain a Dun and Bradstreet Data Universal Numbering System (DUNS) number, register with the System for Award Management (SAM), register with the credential provider, and register with Grants.gov). See www.grants.gov/GetRegistered to begin this process. Use the Grants.gov Organization Registration Checklist at www.grants.gov/Applicants/get-registered.isp to guide you through the process. Designating an E-Business Point of Contact (EBiz POC) and obtaining a special password called an MPIN are important steps in the CCR registration process. Applicants, who are not

registered with CCR and Grants.gov, should allow at least 21 days to complete these requirements. It is suggested that the process be started as soon as possible.

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

2. Content and Form of Application Information

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

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

Whitepapers will consist of:

- **Project Summary/Abstract (limit 2 pages)**. A summary of the Consortium team, research program, collaboration plans, and program management approaches.
- **Research Program (limit 20 pages)**. An overview of the research strategy to be employed; a short description and justification for research goals of the proposed effort (2, 5, and 10 year goals); and a technical discussion describing how the Offeror will address the research goals and advance the state-of-the-art in cyber security. This technical discussion should include a proposed breakdown of research tasks and short description of the technical approaches for each task. A discussion on the relevance of the research, strategy for validation of models, and linkages between research in the RAs and CCRI should be included. This only covers the Core Research Program and its funding.
- **Collaboration Plan and Program Management (limit 3 pages)**. A summary of collaboration plans, synergies gained from these collaborations, and examples of how researchers have successfully collaborated in the past. A summary of the overall plan for leadership and management of the Consortium.

- **Biographical Sketches**. Biographical sketches shall be limited to 1 page per individual, with no limit on the number of individuals.
- **Cost Summary Tables**. For the Whitepaper only, two cost estimate tables shall be provided to provide a broad idea of the participant's relative level-of-effort for the Core Program funding only. This information will be used in the evaluation of the research program. One table lists the estimated first year funding by organization for each RA including the portion related to the CCRI (see Table 1). A column for Other can be used for management or other costs. Another table lists the estimated funding per organization for each of the five years (see Table 2). The $350K for the BAA Partner should be allocated for each year and included in the other category and 5% should be allocated for covered educational institution(s)

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

	Risk RA	Detection RA	Agility RA	Other	Total	Total CCRI
LRO						
Psychosocial CCRI						
Organization A						
Psychosocial CCRI						
Organization B						
Psychosocial CCRI						
Organization C						
Psychosocial CCRI						
Organization D						
Psychosocial CCRI						
BAA Partner				350		
Total						
Total CCRI						

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

	Year 1	Year 2	Year 3	Year 4	Year 5	Total
LRO						
Organization A						
Organization B						
Organization C						
Organization D						
BAA Partner	350	350	350	350	350	
Total						

NOTE: Compatible versions of Adobe Reader are currently 8.1.1 and 8.1.2. You will be asked to specify your Operating System (examples: Windows, Mac) and Version (examples: XP, Vista, 10.4.9) be sure to specify Adobe Reader Version 8.1.2 to get the compatible version to apply for grants on Grants.gov. Click here to download version 8.1.2 from Adobe Website: http://www.adobe.com/products/acrobat/readstep2_allversions.htm.

Proposal. Application forms and instructions will be available at Grants.gov. To access these materials, go to http://www.grants.gov, select "Apply for Grants", and then select "Download an Application Package." Enter the funding opportunity number, W911NF-13-R-0004. REMINDER: Only proposals submitted by Offerors given an invitation to submit a Proposal, after a favorable Whitepaper evaluation, will be considered.

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

The following formatting applies to the Proposal:

- Page size when printed: 8 ½ x 11 inches
- Margins: 1 inch minimum

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

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

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

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

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

- **Chapter 1: Research Program**. The pages included in Chapter 1 shall be numbered. Offerors are advised that Chapter 1 **shall not exceed 50 pages**, utilizing one side of the page.

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

- **Chapter 3: Program Management**. The pages included in Chapter 3 shall be numbered. Offerors are advised that Chapter 3 of the proposal **shall not exceed 10 pages**, utilizing one side of the page.

- **Chapter 4: Biographical Sketches.** Biographical sketches shall be limited to two (2) pages per individual, with no limitation on the number of individuals.

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

- **Facilities and Other Resources** (Field 10 on the form) - The Offeror is to include a listing of facilities and other resources available to support the proposal. Attach this information at Field 10.

- **Equipment** (Field 11 on the form) - The Offeror is to include a listing of equipment available to support the proposal. Any Government equipment necessary for performance is to be clearly identified. Attach this information at Field 11.

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

  1. Attached the completed Proposal Cover Sheet. (See PART D.6 below)
  2. Attached the completed certifications. (See PART F.2 below)
  3. Attach any exceptions or conditions to the Model Collaborative Agreement. (See CRA website for this document)
  4. Attach the signed Articles of Collaboration for all Members. (See CRA website for a sample document)
  5. Attach the Cost Proposal. **The Cost Proposal must include 2 separate budgets for the first five years of performance: one for the Core Research Program and one for the Enhanced Research Program. The Cost Proposal for the Core Research Program MUST address all requirements for the Core Research Program. (The Consortium will be requested to provide a complete cost proposal for the optional five-year period of performance as part of the evaluation to be completed prior to making the decision concerning this optional period)** The cost portion of the proposal shall contain cost estimates sufficiently detailed for meaningful evaluation. For budget purposes, assume a performance start date of 1 October 2013**.** The proposed amounts shall not exceed the funding ceilings identified for the Core Research Program of this PA. For all proposals, the elements of the budget should include:

     - Direct Labor. Individual labor category or person, with associated labor hours and unburdened direct labor rates.

     - Indirect Costs. Fringe benefits, overhead, G&A, etc. (must show base amount and rate). Justify.

     - Travel. Number of trips, destination, duration, etc. Justify and include basis for costs.

     - Subaward. A cost proposal, as detailed as the Offeror's cost proposal, will be required to be submitted by each proposed subrecipient.

     - Consultant. Provide consultant agreement or other document that

verifies the proposed loaded daily/hourly rate. Include a description of the nature of and the need for any consultant's participation. Provide budget justification.

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

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

All entities included in the cost proposal are to provide detailed information on all cost elements included in their proposed budgets as part of the proposal submission process. However, it is recognized that some entities may choose to submit their proprietary rate information directly to the Government in lieu of providing such information to the LRO for inclusion in the cost proposal submitted through grants.gov. In such a case, a separate submission can be made directly to the Government. Such a submission MUST include the PA Number, i.e. W911NF-13-R-0004, and the name of the LRO associated with the proposal on the mailing envelope submitted to the following address:

U.S. Army Contracting Center – Aberdeen Proving Ground
RTP Division
ATTN: W911NF-13-R-0004/CREECH
4300 S. Miami Blvd.
Durham, NC 27703

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

- **SF-LLL: Disclosure of Lobbying Activities**. If applicable, attach a complete SF- LLL at Field 11 of the R&R Other Project

Information form. Applicability: If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the grant/collaborative agreement, you must complete and submit Standard Form - LLL, "Disclosure Form to Report Lobbying."

3. Submission Dates and Times

Whitepapers are due by 3:00pm (local time in North Carolina, USA) on 26 April 2013. An email receipt will be provided for each Whitepaper submission received.

Full Proposals are due by 3:00pm (local time in North Carolina, USA) on 19 July 2013. (NOTE: The date a time of submission, as well as any additional instructions, will be provided with the invitation to submit a Proposal. As a reminder, only the most highly rated Whitepapers will receive an invitation to submit a Proposal.)

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

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

4. Intergovernmental Review - Not applicable

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

6. Other Submission Requirements

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

PROPOSAL COVER SHEET

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

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

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

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

LRO _____
Consortium Member(s) _____
Subawardee(s) _____
Covered Educational Institution(s) _____

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

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

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

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

E. APPLICATION PROCESS AND REVIEW INFORMATION

1. Proposal Evaluation Criteria

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

Factor 1: Scientific Merit and Relevance: Evaluation of this factor will concentrate on the overall scientific and technical merit, military relevance, and innovation of the proposed research in light of the Cyber Security state-of-the-art. The scientific merit will be evaluated with regard to each of the Research Areas of the CRA (Risk, Detection, and Agility), including its Cross Cutting Research Issue (CCRI) in Psychosocial Effects that should span all three Research Areas. Each Research Area will be assessed with regard to its overall scientific merit, innovation, potential degree of generality of the models, and strategy for validation. Evaluation of this factor will also concentrate on the long term relevance of the proposed research and the likelihood that the proposed research will address scientific challenges and research barriers facing the Army.

The Whitepaper should include a overview of the research strategy to be employed to advance the state-of-the-art in cyber security; a short description and justification for 2-, 5-, and 10-year research goals of the proposed effort; and a short technical discussion stating the background and objectives of the proposed research, the overall technical approaches to be pursued, the potential techniques to be used to validate the models and theories developed in this CRA. The Whitepaper should clearly identify specific scientific challenges and research barriers that relate to fundamental understanding of the root cause of difficult cyber security problems. The Whitepaper should clearly highlight the innovations proposed and how they may lead to an understanding of cyber security phenomena and highlight how the proposed research is expected to feed, be fed by, or in some other way link with, research being performed elsewhere within the Consortium.

Factor 2: Experience and Qualifications of Scientific Staff: The qualifications, capabilities, availability, accomplishments and experience of the Offeror's proposed research personnel will be evaluated as an indication of their ability to achieve the proposed technical objectives.

The Whitepaper should include the names, brief biographies, and general availability of the key personnel who will be involved in the research. Such credentials, as documented on the biographical sketches, shall include, among others, a record of seminal publications in the scientific literature and a record of successful cyber security research.

Factor 3: Collaboration and Program Management: Evaluation of this factor will include evidence of previous successful collaborative efforts and the Offeror's commitment and plans for collaboration. The Whitepaper should include general information on previous collaborations and general plans for how researchers will collaborate within each Research Area and among Research Areas and how this collaboration will further the goals of the program. Evaluation of this factor will focus on the leadership provided by the Program Director and the Offeror's plans to meet the requirements of the overall management concept. This includes plans for an environment to foster collaboration and efforts to bring about a unity of vision for the Consortium. The Whitepaper should include the identification of the Program Manager, key leadership personnel and an overall plan for leadership and efficient management of the Cyber Security CRA and creation of a collaborative environment.

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

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

Factor 1: Scientific Merit and Relevance: Evaluation of this factor will concentrate on the overall scientific and technical merit, creativity, military relevance, and innovation of the proposed research in light of the Cyber Security state-of-the-art. The scientific merit will be evaluated with regard to each of the Research Areas of the CRA (Risk, Detection, and Agility), including its Cross Cutting Research Issue (CCRI) in Psychosocial Effects that should span all three Research Areas. Each Research Area will be assessed with regard to its overall scientific merit, creativity, innovation, degree of generality of the models, validation techniques, and likelihood of substantially advancing the current state-of-the-art in cyber science. Evaluation of this factor will also concentrate on the long term relevance of the proposed research and the likelihood that the proposed research will address scientific challenges and research barriers facing the Army.

The Proposal should include a discussion of the research strategy to be employed to advance the state-of-the-art in cyber security; a detailed description and justification for 2-, 5-, and 10-year research goals of the proposed effort; and a detailed technical discussion. The technical discussion should include the background and objectives of the proposed research, the technical approaches to be pursued, the validation techniques and metrics to be used to validate the models and theories developed in this CRA, and the parties involved and the level of effort to be employed (demonstrating that researchers are collaborating and

substantially and meaningfully engaged in the research efforts). The Proposals should also clearly:

- Identify specific scientific challenges and research barriers that relate to fundamental understanding of the root cause of difficult cyber security problems and should provide evidence that the proposed technical approaches can address these challenges in a measured approach across the near- and far-term.

- Explain in substantial detail the specific scientific plans that will be employed, and provide ample evidence that the approaches are likely to substantially advance the underlying science.

- Highlight the innovations proposed and how they may lead to an understanding of cyber security phenomena particularly fundamental laws, theories, and validated models.

- Show how the proposed research is expected to feed, be fed by, or in some other way link with, research being performed elsewhere within the Consortium and within the ARL.

Factor 2: Experience and Qualifications of Scientific Staff and Quality of Research Facilities: The qualifications, capabilities, availability, proposed level of effort, and experience of both the Offeror's proposed research personnel (individually and as a whole) their relevant past accomplishments, and their ability to achieve the proposed technical objectives will be evaluated. Key personnel are expected to be substantially and meaningfully engaged in the research and the proposed level of effort for key personnel should be commensurate with and demonstrate such. The extent to which the Offeror's proposed facilities and equipment will contribute to the accomplishment of the proposed research will be evaluated including the nature, quality, relevance, availability, and access to state-of-the-art research facilities and equipment.

The Proposal should include the names, biographies, availability and proposed level of effort of the key personnel who will be involved in the research. Such credentials, as documented on the biographical sketches, shall include, among others, a record of seminal publications in the scientific literature and a record of successful cyber security research. 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 will enhance the research efforts proposed.

Factor 3: Collaboration: Evaluation of this factor will focus on the proposed collaboration plans for the CRA in accordance with the collaboration requirements set forth in the PA. Evaluation of this factor will include evidence

of previous successful collaborative efforts, the Offeror's commitment and plans for collaboration, and the synergistic value of the collaborations among Consortium researchers and with ARL.

The Proposal should include plans for how researchers will collaborate within each Research Area and among Research Areas and describe how this collaboration will further the goals of the program. The Proposal should describe the strategy for collaborating with ARL and propose collaborative opportunities with ARL. The Proposal should include examples of how researchers have successfully collaborated previously in similar programs.

Factor 4: Program Management. Evaluation of this factor will focus on the leadership provided by the Program Director and the Offeror's plans to meet the requirements of the overall management concept, including timely submission of consortium invoices and research plan development. This includes plans for an environment to foster collaboration and efforts to bring about a unity of vision for the Consortium. Evaluation of this factor will include the adequacy of the overall management plan, internal team structures and composition with respect to achieving the research goals of the program. The management plan should also include the Offeror's plans and approach for enhanced research efforts should such funding become available during performance.

The Proposal should include a detailed plan for leadership and efficient management of the Cyber Security CRA, creation of a collaborative environment, and organizational structures. The Proposal should identify metrics for success, how they will be used, and how they will further the goals of the program.

Relative Importance of the Evaluation Factors: The evaluation factors are listed in descending order of importance. Factor (1) is approximately equal importance with Factor (2) and Factor (3) combined. Factor (2) is approximately twice as important as Factor (3) and three times as important as Factor (4).

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

Relative Importance of the Evaluation Factors: The evaluation factors are listed in descending order of importance with Factors 5 not be weighted.

2. Review and Selection Process

All timely and compliant Whitepaper submissions will be evaluated in accordance with the evaluation criteria set forth in this PA. Whitepapers are expected to be evaluated by a group of qualified scientists and managers from the Government. However, the Government reserves the right to have Whitepapers evaluated by subject matter experts outside the Government. Should such outside evaluators be used, they will be required to sign a non-disclosure statement before being provided access to Whitepapers. Only the most highly rated Whitepapers will receive an invitation to submit a Proposal as well as feedback on the Whitepaper. 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." Offerors not receiving an invitation to submit proposals will be informed of such via email following the Whitepaper evaluations.

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

Proposals that are in compliance with the requirements of the PA 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 qualified groups 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 decisions concerning the Whitepaper downselection, 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 before being provided access to proposals.

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 FPR 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 PA requirements. The Government will make award to the Offeror, conforming to the PA that offers the best value to the Government, cost and other factors considered. Further, award may be made to other than the Offeror who offers the lowest cost proposal. ARL reserves the right not to make an award should no acceptable offer be submitted.

3. Recipient Qualification - See **PART II.C.1** above.

4. Anticipated Announcement and Award Dates - See **PART I** above.

F. AWARD ADMINISTRATION INFORMATION

1. Award Notices

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

2. Administrative and National Policy Requirements

Offerors must comply with National Policy Requirements Matrix Appendix "C" found at http://www.nsf.gov/bfa/dias/policy/rtc/appc.pdf.

3. Reporting

Reporting requirements for the CA are contained in the Model CA which will be posted to the CRA website.

G. AGENCY CONTACTS

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

will be provided for potential Offerors to post their availability for teaming with others.