Buyers: Login | Register Vendors: Login | Register Accessibility



Capabilities for Cyber Resiliency Solicitation Number: BAA-RIK-14-07 Agency: Department of the Air Force Office: Air Force Materiel Command Location: AFRL/RIK - Rome

Notice Details

Packages

Print

Link

Original Synopsis Aug 01, 2014

11:07 am

Return To Opportunities List Watch This Opportunity

Solicitation Number: Notice Type: BAA-RIK-14-07 Presolicitation

Synopsis:

Added: Aug 01, 2014 11:07 am

NAICS CODE: 541712

FEDERAL AGENCY NAME: Department of the Air Force, Air Force Materiel Command, AFRL - Rome Research Site, AFRL/Information Directorate, 26

Electronic Parkway, Rome, NY, 13441-4514

TITLE: Capabilities for Cyber Resiliency

ANNOUNCEMENT TYPE: Initial announcement

FUNDING OPPORTUNITY NUMBER: BAA-RIK-14-07

CFDA Number: 12.800 and 12.910

I. FUNDING OPPORTUNITY DESCRIPTION:

This BAA is a contracting tool directly responsive to Air Force Research Laboratory (AFRL) cyber science & technology (S&T) strategic goals.

To support these strategic goals, this BAA seeks to procure proactive cyberspace defense capabilities for avoiding threats through understanding the cyber situation, assessing potential impacts, and implementing deterrence and effects-based defensive methodologies. As such, it supports work in the areas of trusted hardware, trusted software, trusted data, secure systems/architectures, maneuverability, mission awareness, mission assurance, and survivability and recovery techniques.

Other applicable areas of technology include, but are not limited to, attack attribution/geolocation, novel protocols, cloud architectures/security, mobile device security, secure computer/processor architectures, virtualization security, cyber technology evaluation techniques, cyber modeling, simulation, metrics, and

GENERAL INFORMATION

Notice Type: Presolicitation

Posted Date: August 1, 2014

Response Date:

-

Archiving Policy: Manual Archive

Archive Date:

-

Original Set Aside:

N/A

Set Aside:

N/A

Classification Code:

A -- Research & Development

NAICS Code:

541 -- Professional, Scientific, and Technical Services/541712 --Research and Development in the Physical, Engineering, and Life Sciences (except Biotechnology) measurements, cyber data mining/understanding, next generation BIOS Security, and cyber visualization.

NOTE: White Papers for the above will be accepted over the life of this BAA.

The following Specific Focus Areas are only open for the fiscal years noted.

FY14 - FY17 SPECIFIC FOCUS AREA: ASSURED BY DESIGN

Background: Many cyber solutions currently focus on detecting attacks after they occur and then attempt to apply security mechanisms to existing hardware and software. This type of solution is inefficient and keeps systems and networks in a constant state of "react". A more proactive approach is preventing and avoiding rather than detecting after the fact. This area seeks to develop mathematically rigorous tools and techniques that modify the cyber domain in favor of mission assurance.

Objective: To formally verify that hardware and software implementations meet mathematical specifications that prove correctness of secure designs and to lead research in technologies to mitigate new and emerging threats that could degrade capabilities by developing innovative solutions through science and engineering applications to national security problems. Results of this work would place missions orthogonal to threats. This focus area is not interested in concepts, approaches, and techniques that rely on detection and reaction. The Assured by Design area is divided into three main thrusts: Science of Mission Assurance, Engineering Assured Systems, and Domain Modification.

The goal of the Science of Mission Assurance thrust is to develop a security engineering culture that mathematically represents the specifications of critical mission essential functions and verifies their implementation in a contested cyber domain.

The Engineering Assured Systems thrust intends to research hardware assisted security, formal methods, and validation to provide prevention techniques to current and future systems through specialized hardware and software systems. Deliverables should include foundational research with demonstration of software and hardware prototypes. Research seeks to create and verify the "mission layer" and produce a design framework to create assured cyber systems.

Domain Modification capitalizes on novel, out-of-the-box approaches to provide successful execution of mission essential functions. Interest is in techniques that modify the domain in favor of mission assurance and increase the cost to the adversary to exploit systems. The focus is on preventing and avoiding vulnerabilities in missions.

Questions regarding this focus area can be directed to:
Dr. Sarah Muccio
(315) 330-4016
sarah.muccio@us.af.mil

FY15 - FY17 SPECIFIC FOCUS AREA: SURVIVAL AND RECOVERY OF MISSION ESSENTIAL FUNCTIONS

Background: Despite many security enhancements, systems are not resilient and are unable to provide the continuation of Mission Essential Functions (MEFs) in the face of disruption by a sophisticated adversary or a non-malicious fault. Cyber resilience comprises the ability to withstand, minimize, survive, and recover from

the negative effects of adversity, whether man-made or natural, under all circumstances of use. Resilient systems must not only mitigate vulnerabilities, they must also fight through successful attacks to assure MEFs continue without disruption. Resilient systems must also possess the ability of a computer system to regain or even exceed its initial operating capability. While continuing MEFs, damaged systems must recover any lost services, components, and data. These systems must discover their own vulnerabilities and regenerate themselves with immunity to improve their ability to deliver critical services.

Objective: To focus on technology solutions that increase the probability of assuring Mission Essential Functions (MEF) during successful cyber attacks.

AFRL seeks ideas and concepts in the following thrust areas:

- 1. Self-protecting software systems Systems that use domain knowledge and mission needs to defend against malicious attacks or failures and have the ability to anticipate and mitigate future security threats.
- Machine Generated Repair Automatically generate repairs to code and automatically repair corrupted data and state to recover with immunity.
- Cyber Defense Metrics Identification of metrics as a method of quantifying resiliency, security, and mission readiness.
- 4. Infrastructure Virtualization Enabling secure multiplexing of computing resources among multiple organizations and controlled information sharing among organizations with end-to-end trust in the infrastructure with data integrity.

Questions regarding this focus area can be directed to: David Climek (315) 330-4123 david.climek.1@us.af.mil

FY15 - FY16 SPECIFIC FOCUS AREA: CYBER DECEPTION

Background: Deception is a deliberate act to conceal activity on our networks, create uncertainty and confusion against the adversary's efforts to establish situational awareness and to influence and misdirect adversary perceptions and decision processes. Military deception is defined as "those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission." Military forces have historically used techniques such as camouflage, feints, chaff, jammers, fake equipment, false messages or traffic to alter an enemy's perception of reality. Modern day military planners need a capability that goes beyond the current state-of-the-art in cyber deception to provide a system or systems that can be employed by a commander when needed to enable deception to be inserted into defensive cyber operations.

Relevance and realism are the grand technical challenges to cyber deception. The application of the proposed technology must be relevant to operational and support systems within the DoD. The DoD operates within a highly standardized environment. Any technology that significantly disrupts or increases the cost to the standard of practice will not be adopted. If the technology is adopted, the defense system must appear legitimate to the adversary trying to exploit it.

Objective: To provide cyber-deception capabilities that could be employed by commanders to provide false information, confuse, delay, or otherwise impede

cyber attackers to the benefit of friendly forces. Deception mechanisms must be incorporated in such a way that they are transparent to authorized users, and must introduce minimal functional and performance impacts, in order to disrupt our adversaries and not ourselves. As such, proposed techniques must consider how challenges relating to transparency and impact will be addressed. The security of such mechanisms is also paramount, so that their power is not co-opted by attackers against us for their own purposes. These techniques are intended to be employed for defensive purposes only on networks and systems controlled by the DoD.

Advanced techniques are needed with a focus on introducing varying deception dynamics in network protocols and services which can severely impede, confound, and degrade an attacker's methods of exploitation and attack, thereby increasing the costs and limiting the benefits gained from the attack. The emphasis is on techniques that delay the attacker in the reconnaissance through weaponization stages of an attack and also aid defenses by forcing an attacker to move and act in a more observable manner. Techniques across the host and network layers or a hybrid thereof are of interest in order to provide AF cyber operations with effective, flexible, and rapid deployment options.

This focus area is currently envisioned to consist of two phases running approximately 12 months each. The first phase (Concept Development) will consist of one to three study efforts that will examine potential deception technologies that could be developed. This will focus on the description, design and development of techniques and technologies that could be employed in an Air Force network. These efforts will be brought to a proof-of-concept level, and the implementations will be evaluated at the end of this phase. In the second phase (Prototyping), also lasting approximately 12 months, one or more of the concepts that show promise will be further developed to produce a prototype system capable of demonstration in a relevant environment. The system(s) developed by the end of this phase will be evaluated. At the end of this second phase, a "go/no-go" decision will be made to determine if the prototype(s) will undergo further refinement, evaluation, and potential integration with an eye toward transition.

Questions regarding this focus area can be directed to: Anthony Macera (315) 330-4480 anthony.macera.1@us.af.mil

FY15 - FY17 SPECIFIC FOCUS AREA: CYBER AGILITY

Background: Currently, adversaries can plan their attacks carefully over time by relying on the static nature of our networks, and launch their attacks at the times and places of their choosing. The DoD needs new tools and technologies to reverse the current asymmetry that favors our cyber adversaries, by forcing them to spend more, cope with greater levels of complexity and uncertainty, and accept greater risks of exposure and detection due to the significantly increased requirements for reconnaissance and intelligence collection on our networks.

AFRL is seeking science & technology for defensive cyber maneuver and agility to disrupt adversary cyberspace operations, including adversary attack planning and execution.

Objective: To reduce attacks by making it harder for a determined adversary to succeed. Increasing agility, diversity, and redundancy will result in disrupting attack planning and execution. Agility mechanisms must be incorporated in such a way that they are transparent to authorized users, and must introduce minimal functional and performance impacts, in order to disrupt our adversaries and not ourselves. As such, proposed techniques must consider how challenges relating to transparency and impact will be addressed. The security of such mechanisms is also paramount, so that their power is not co-opted by attackers against us for

their own purposes.

Questions regarding this focus area can be directed to: Walt Tirenin (315) 330-4429 wladimir.tirenin@us.af.mil

FY15 - FY17 SPECIFIC FOCUS AREA: EMBEDDED SYSTEM RESILIENCE AND AGILITY

Background: Technology trends and growth indicate a highly interconnected environment with an increasing reliance on system autonomy and embedded systems. Embedded systems may be viewed as an electronic device that contains a microprocessor (one or more), along with purpose-built software to perform specific functions within a larger community. Embedded system software, data, and memory often contain high-value information and control key assets. With this level of criticality, security provisions are crucial across the full-spectrum of embedded systems. Embedded systems require dedicated effort to infuse strong security and time-critical performance with limited resources and storage constraints. Within many applications, embedded systems are employed within platforms which are vulnerable to intentional or unintentional hazards or attacks. Any event, intentional or not, may compromise the reliability of a system and become a mission critical security threat.

Objective: To research and demonstrate preemptive and proactive defense approaches, along with reactive techniques protecting assets, key functions, and data through recovery and adaptation. The focus of this research is protection of resources vice networking. The embedded system solution may include hardware, software, and advanced techniques to protect critical assets against cyber threat vectors either onboard or from external vectors. One specific use case for this focus area is the command and control of Unmanned Aerial Systems.

Additionally, embedded systems must support real-time, guaranteed performance in safety and security-critical applications. Within cyber-physical systems, the joint behavior of the "cyber" and "physical" elements of the system is critical-computing, control, sensing, and networking are deeply integrated into every component, and the actions of components and systems must be carefully orchestrated, tested, and verified. Thus, system testing will be critical.

This focus area will be comprised of 2 initial phases. Phase 1 is Analysis of Alternatives (AoA), security analysis, and system design. Phase 2 is prototype development and test. Successful completion of Phase 1 is a strong indicator of progression into Phase 2.

Phase 1: Analysis of Alternatives (AoA), Security Analysis, and System Design

Embedded security techniques are characterized by awareness of and protection against threats, minimization of vulnerabilities, computation of optimal assurance solutions, and protection of critical functions/information. These techniques should proactively deter adverse events as well as allow for real-time mitigation, leading to system recovery and adaption to the event. This phase investigates the mix of commercial and government solutions to present a cost-effective and high-assurance embedded system platform. Assessment of solutions against industry standards and internal/external threats should be included.

Key technical areas of this phase may include, but not limited to:

- 1. Trusted monitoring, awareness, and control down to hardware-level
- 2. Techniques to reduce vulnerable attack surface; protect critical functions and

data

- 3. Embedded system agility, diversity, and internal moving target concepts
- 4. Advanced fault tolerance/techniques to continue critical functions
- 5. Monitoring and reasoning of system events to determine and apply recovery and adaption techniques
- Integration of software techniques onto enabling hardware for subsystem/system prototyping

Phase 2: Prototype Development and Test

The objective of this phase is the production of an embedded system prototype based on phase 1. This prototype should be subjected to functionality testing and vulnerability analysis, and should meet and exceed (where applicable) standards. Robust validation and verification is a critical component of this phase.

Key concepts of this phase may include, but are not limited to:

- Resilience metrics, measurement, and understanding of improved models of complex systems of systems, control and authority, levels of autonomy, systemsystem interactions, and new integrated analytical and decision-support tools through static and dynamic testing
- 2. Advanced testing techniques, to include autonomy and machine-learning, which stresses security, safety, runtime performance and vulnerabilities
- Advanced methods for obtaining and extrapolating measurements to predict system behavior

Questions regarding this focus area can be directed to: Douglas Schafer (315) 330-4323 douglas.schafer.6@us.af.mil

NOTE: The POC for each focus area is provided for QUESTIONS ONLY. See Section IV Paragraph 2 for submission details.

II. AWARD INFORMATION:

1. FUNDING: Total funding for this BAA is approximately \$49M. The anticipated funding to be obligated under this BAA is broken out by fiscal year as follows: FY14 - \$1M; FY15 - \$11M; FY16 - \$11M; FY17 - \$11M; FY18 - \$8M; and FY19 - \$7M. Individual awards will not normally exceed 36 months with dollar amounts normally ranging between \$100K to \$1M per year. There is also the potential to make awards up to any dollar value. NOTE: Some funding has been set aside in FY14, however it is more likely that any awards will be made starting in FY15.

The Government reserves the right to select all, part, or none of the proposals received, subject to the availability of funds. All potential Offerors should be aware that due to unanticipated budget fluctuations, funding in any or all areas may change with little or no notice.

- 2. FORM: Awards of efforts as a result of this announcement will be in the form of contracts, grants, cooperative agreements or other transactions (OT); both OTs for prototype and research will be considered depending upon the nature of the work proposed.
- BAA TYPE: This is a two-step open broad agency announcement. This announcement constitutes the only solicitation.

As STEP ONE - We are only soliciting white papers at this time. DO NOT SUBMIT A FORMAL PROPOSAL. Those white papers found to be consistent with the intent of this BAA may be invited to submit a technical and cost proposal, see Section VI of this announcement for further details regarding the proposal.

III. ELIGIBILITY INFORMATION:

All qualified offerors who meet the requirements of this BAA may apply.

Foreign or foreign-owned offerors are advised that their participation is subject to foreign disclosure review procedures. Foreign or foreign-owned offerors should immediately contact the contracting office focal point, Gail E. Marsh, Contracting Officer, telephone (315) 330-7518 or e-mail Gail.Marsh@us.af.mil for information if they contemplate responding. The e-mail must reference the BAA-RIK-14-07 and the BAA title.

IV. APPLICATION AND SUBMISSION INFORMATION: All responses to this announcement must be addressed to the <u>Technical point of contact (POC)</u> listed in SECTION VII. <u>DO NOT</u> send white papers to the Contracting Officer.

 SUBMISSION DATES AND TIMES: While white papers will be accepted over the life of this BAA, it is recommended that they be received by the following dates to maximize the possibility of award:

FY15 by 5 Sep 2014 FY16 by 1 Mar 2015 FY17 by 1 Mar 2016 FY18 by 1 Mar 2017 FY19 by 1 Mar 2018

White papers will be accepted until 2pm Eastern time on 30 Sep 2019, but it is less likely that funding will be available in each respective fiscal year after the dates cited. This BAA will close on 30 Sep 2019.

All offerors submitting white papers will be contacted by the technical POC, referenced in Section VII of this announcement. Offerors can email the technical POC for status of their white paper/proposal but it is requested that this be no earlier than 45 days after submission.

2. CONTENT AND FORMAT: Offerors are required to submit a 4 to 5 page white paper <u>electronically to the technical POC email address provide in SECTION VII</u> summarizing their proposed approach/solution. CONFIRMATION OF RECEIPT IS THE RESPONSIBILITY OF THE OFFEROR. The Government is not responsible for lost submissions.

The white paper will be formatted as follows:

- a. <u>Section A</u>: Title, Period of Performance, Estimated Cost, Name/Address of Company, Technical and Contracting Points of Contact (phone, fax and email)(this section is NOT included in the page count);
 - b. Section B: Task Objective; and
 - c. Section C: Technical Summary and Proposed Deliverables.

All white papers/proposals shall be double spaced with a font no smaller than 12 point. In addition, respondents are requested to provide their Commercial and Government Entity (CAGE) number, their Dun & Bradstreet (D&B) Data Universal Numbering System (DUNS) number, a fax number, an e-mail address, and reference BAA-RIK-14-07 with their submission.

Multiple white papers within the purview of this announcement may be submitted by each offeror. If the offeror wishes to restrict its white papers/proposals, they must be marked with the restrictive language stated in FAR 15.609(a) and (b).

3. HANDLING AND MAILING INSTRUCTIONS:

a. CLASSIFICATION GUIDANCE. All Proposers should review the NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL, (NISPOM), dated February 28, 2006 as it provides baseline standards for the protection of classified information and prescribes the requirements concerning Contractor Developed Information under paragraph 4-105. Defense Security Service (DSS) Site for the NISPOM is: http://www.dss.mil/.

In the event of a possible or actual compromise of classified information in the submission of your white paper or proposal, immediately but no later than 24 hours, bring this to the attention of your cognizant security authority and AFRL Rome Research Site Information Protection Office (IPO):

Vincent Guza 315-330-4048 0730-1630 Monday-Friday 315-330-2961 Evenings and Weekends

Email: vincent.guza@us.af.mil

b. CLASSIFIED SUBMISSIONS. AFRL/RIGA will accept classified responses to this BAA when the classification is mandated by classification guidance provided by an Original Classification Authority of the U.S. Government, or when the offeror believes the work, if successful, would merit classification. Security classification guidance in the form of a DD Form 254 (DoD Contract Security Classification Specification) will not be provided at this time since AFRL is soliciting ideas only. Offerors that intend to include classified information or data in their white paper submission or who are unsure about the appropriate classification of their white papers should contact the technical point of contact listed in Section VII for guidance and direction in advance of preparation.

c. MAILING INSTRUCTIONS. **Unclassified** electronic submissions to the TPOC at baa-rik-14-07@us.af.mil will be accepted. Encrypt or password-protect all proprietary information prior to sending. Offerors are responsible to confirm receipt with the technical POC listed in Section VII. AFRL is not responsible of undelivered documents.

All classified responses to this announcement must be sent U.S. Postal Service, registered mail and addressed to AFRL/RIGA, 525 Brooks Road, Rome NY 13441-4505, and reference BAA-RIK-14-07. Use classification and marking guidance provided by previously issued security classification guides, the Information Security Regulation (DoD 5200.1-R), and the National Industrial Security Program Operating Manual (DoD 5220.22-M) when marking and transmitting information previously classified by another original classification authority. Classified information at the Confidential and Secret level may be mailed via U.S. Postal Service (USPS) Registered Mail. For proposals of higher classification levels or for alternate submission mechanisms please contact the technical POC listed in Section VII. When mailing, ensure the response is appropriately marked, sealed, and mailed in accordance with the classified material handling procedures. The classified mailing address is:

Ref: BAA RIK-14-07 AFRL/RIGA 525 Brooks Road Rome NY 13441-4505

Questions can be directed to the technical POC listed in Section VII.

- 4. OTHER SUBMISSION REQUIREMENTS/CONSIDERATIONS:
 - a. COST SHARING OR MATCHING: Cost sharing is not a requirement.
- b. SYSTEM FOR AWARD MANAGEMENT (SAM). Offerors must be registered in the SAM database to receive a contract award, and remain registered during performance and through final payment of any contract or agreement. Processing time for registration in SAM, which normally takes forty-eight hours, should be taken into consideration when registering. Offerors who are not already registered should consider applying for registration before submitting a proposal. The provision at FAR 52.204-7, System for Award Management (Jul 2013) applies.
- c. EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT/
 SUBRECIPIENT AWARDS: Any contract award resulting from this announcement
 may contain the clause at FAR 52.204-10 Reporting Executive Compensation
 and First-Tier Subcontract Awards. Any grant or agreement award resulting from
 this announcement may contain the award term set forth in 2 CFR, Appendix A to
 Part 25 which can be viewed at: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?
 c=ecfr&sid=c55a4687d6faa13b137a26d0eb436edb&rgn=div5&view=
 text&node=2:1.1.1.41&idno=2#2:1.1.1.41.2.1.1
- d. ALLOWABLE CHARGES: The cost of preparing white papers/proposals in response to this announcement is not considered an allowable direct charge to any resulting contract or any other contract, but may be an allowable expense to the normal bid and proposal indirect cost specified in FAR 31.205-18. Incurring pre-award costs for ASSISTANCE INSTRUMENTS ONLY are regulated by the DoD Grant and Agreements Regulations (DODGARS).

V. APPLICATION REVIEW INFORMATION:

- 1. CRITERIA: The following criteria, which are listed in descending order of importance, will be used to determine whether white papers and proposals submitted are consistent with the intent of this BAA and of interest to the Government:
- (1) Overall scientific and/or technical merit including technical feasibility, degree of innovation, and understanding of the technical and operational approach for employment of the technology;
- (2) The effort's potential contribution and relevance to the U. S. Air Force's objectives;
- (3) The extent to which the offeror demonstrates relevant technology and domain knowledge, and
 - (4) Reasonableness and realism of proposed costs and fees (if any).

No further evaluation criteria will be used in selecting white papers/proposals. Individual white paper/proposal evaluations will be evaluated against the evaluation criteria without regard to other white papers and proposals submitted under this BAA. White papers and proposals submitted will be evaluated as they are received

2. REVIEW AND SELECTION PROCESS:

Only Government employees will evaluate the white papers/proposals for selection. The Air Force Research Laboratory's Information Directorate has contracted for various business and staff support services, some of which require contractors to obtain administrative access to proprietary information submitted by other contractors. Administrative access is defined as "handling or having physical control over information for the sole purpose of accomplishing the administrative functions specified in the administrative support contract, which do not require the review, reading, and comprehension of the content of the information on the part of non-technical professionals assigned to accomplish the specified administrative tasks." These contractors have signed general non-disclosure agreements and organizational conflict of interest statements. The required administrative access will be granted to non-technical professionals. Examples of the administrative tasks performed include: a. Assembling and organizing information for R&D case files; b. Accessing library files for use by government personnel; and c. Handling and administration of proposals, contracts, contract funding and queries. Any objection to administrative access must be in writing to the Contracting Officer and shall include a detailed statement of the basis for the objection.

3. ADEQUATE PRICE COMPETITION: The Government may simultaneously evaluate proposals received under this BAA from multiple offerors. In this case, the Government may make award based on adequate price competition, and offerors must be aware that there is a possibility of non-selection due to a proposal of similar but higher-priced technical approach as compared to another offeror.

VI. **STEP TWO** INFORMATION - REQUEST FOR PROPOSAL & AWARD:

1. AWARD NOTICES: Those white papers found to be consistent with the intent of this BAA may be invited to submit a technical and cost proposal. Notification by email or letter will be sent by the technical POC. Such invitation does not assure that the submitting organization will be awarded a contract. Those white papers not selected to submit a proposal will be notified in the same manner. Prospective offerors are advised that only Contracting Officers are legally authorized to commit the Government.

For additional information, a copy of the AFRL "Broad Agency Announcement (BAA): Guide for Industry," May 2012, may be accessed at: https://www.fbo.gov/index?

s=opportunity&mode=form&id=e68f832abb3a7341bb7328547c0e19c0&tab=core&_cview=0

2. ADMINISTRATIVE AND NATIONAL POLICY REQUIREMENTS:

Depending on the work to be performed, the offeror may require a SECRET or TOP SECRET facility clearance and safeguarding capability; therefore, personnel identified for assignment to a classified effort must be cleared for access to SECRET or TOP SECRET information at the time of award. In addition, the offeror may be required to have, or have access to, a certified and Government-approved facility to support work under this BAA.

This acquisition may involve data that is subject to export control laws and regulations. Only contractors who are registered and certified with the Defense

Logistics Information Service (DLIS) at http://www.dlis.dla.mil/jcp/ and have a legitimate business purpose may participate in this solicitation. For questions, contact DLIS on-line at http://www.dlis.dla.mil/jcp or at the DLA Logistics Information Service, 74 Washington Avenue North, Battle Creek, Michigan 49037-3084, and telephone number 1-800-352-3572. You must submit a copy of your approved DD Form 2345, Militarily Critical Technical Data Agreement, with your white paper/proposal.

3. DATA RIGHTS:

- a. SBIR RIGHTS. The potential for inclusion of Small Business Innovation Research (SBIR) or data rights other than unlimited on awards is recognized. In accordance with (IAW) the Small Business Administration (SBA) SBIR Policy Directive, Section 8(b), SBIR data rights clauses are non-negotiable and must not be the subject of negotiations pertaining to an award, or diminished or removed during award administration. Issuance of an award will not be made conditional based on forfeit of data rights. If the SBIR awardee wishes to transfer its SBIR data rights to the Air Force or to a third party, it must do so in writing under a separate agreement. A decision by the awardee to relinquish, transfer, or modify in any way its SBIR data rights must be made without pressure or coercion by the agency or any other party.
- b. NON-SBIR RIGHTS. Non-SBIR data rights less than unlimited will be evaluated and negotiated on a case-by-case basis. Government Purpose Rights are anticipated for data developed with DoD-reimbursed Independent Research and Development (IR&D) funding.
- 4. REPORTING: Once a proposal has been selected for award, offerors will be given complete instructions on the submission process for the reports.
- SUPPLY CHAIN RISK: The provision at DFARS 252.239-7017, Notice of Supply Chain Risk (Nov 2013) applies.

VII. AGENCY CONTACTS:

All white paper and proposal submissions and any questions of a technical nature shall be directed to the cognizant technical point of contact as specified below (unless otherwise specified in the technical area):

TPOC Name: Jeff DeMatteis
Telephone: (315) 330-7132
Email: baa-rik-14-07@us.af.mil

Questions of a contractual/business nature shall be directed to the cognizant contracting officer, as specified below (email requests are preferred):

Gail Marsh

Telephone (315) 330-7518 Email: gail.marsh@us.af.mil

The email must reference the solicitation (BAA) number and title of the acquisition.

In accordance with AFFARS 5301.91, an Ombudsman has been appointed to hear and facilitate the resolution of concerns from offerors, potential offerors, and others for this acquisition announcement. Before consulting with an ombudsman, interested parties must first address their concerns, issues, disagreements, and/or

recommendations to the contracting officer for resolution. AFFARS Clause 5352.201-9101 Ombudsman (Apr 2014) will be incorporated into all contracts awarded under this BAA. The AFRL Ombudsman is as follows:

Ms. Barbara Gehrs
AFRL/PK
1864 4th Street
Building 15, Room 225
Wright-Patterson AFB OH 45433-7130
FAX: (937) 656-7321; Comm: (937) 904-4407
barbara.gehrs@us.af.mil

All responsible organizations may submit a white paper which shall be considered.

Contracting Office Address:

26 Electronic Parkway Rome, New York 13441-4514 United States

Primary Point of Contact.:

Gail E. Marsh, Contracting Officer Gail.Marsh@us.af.mil Phone: 315-330-7518

Return To Opportunities List

Watch This Opportunity

For Help: Federal Service Desk Accessibility