CYBER ASSURANCE TECHNOLOGIES

Solicitation Number: BAA-11-01-RIKA
Agency: Department of the Air Force
Office: Air Force Materiel Command
Location: AFRL - Rome Research Site

Complete View

Original Synopsis
Presolicitation
Dec 13, 2010 11:24 am

Changed
Jan 19, 2011 2:59 pm

Changed
Feb 01, 2011 9:25 am

Changed
Dec 22, 2011 8:10 am

Changed
Mar 15, 2012 10:08 am

Return To Opportunities List
Watch This Opportunity

Solicitation Number:
BAA-11-01-RIKA

Notice Type:
Modification/Amendment

Synopsis:
Added: Mar 15, 2012 10:08 am
The purpose of this modification is to include the following changes: (1) Section I Funding Opportunity Description: add additional Focus Area for FY12; (2) Section II, Award Information: last sentence revised for this focus area ONLY; (3) Section IV, APPLICATION AND SUBMISSION INFORMATION, paragraph 3, SUBMISSION DATES AND TIMES, is revised to read as follows for this specific focus area ONLY; and (4) Section VII, AGENCY CONTACTS, for this specific focus area ONLY have been changed. No other changes have been made to this BAA.

(1) Insert the following under Section I, FUNDING OPPORTUNITY DESCRIPTION:

GENERAL INFORMATION

Notice Type:
Modification/Amendment

Original Posted Date:
December 13, 2010

Posted Date:
March 15, 2012

Response Date:
-

Original Response Date:
-

Archiving Policy:
Manual Archive

Original Archive Date:
-

Archive Date:
-

Original Set Aside:
N/A

Set Aside:
N/A

Classification Code:
A -- Research & Development

FY 12 SPECIFIC FOCUS AREA: PROTECTED REPOSITORY FOR THE DEFENSE OF INFRASTRUCTURE AGAINST CYBER THREATS (PREDICT)

NAICS Code:
541 -- Professional, Scientific, and Technical Services/541712 -- Research and Development in the Physical, Engineering, and Life Sciences (except Biotechnology)

Background:

The Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) will serve as a large-scale, privacy-protected, dataset repository of real network and system traffic for use by the cyber security research community, both in the U.S. and internationally, to accelerate design, production, and evaluation of next-generation cyber security solutions, including commercial products. The Air Force Research Lab and the Department of Homeland Security (DHS) are collaborating to foster continued support to provide research relevant Internet data to the cybersecurity community.

Objective:

The objective is to focus development in two technical areas: Data Hosts (DHs) and Data Providers (DPs). Data Providers provide the data that it owns or has a right to control and disclose to researchers. Similarly, Data Hosts maintain computing infrastructure to store data received from one or more data providers, as well as mechanisms to distribute media if needed. To support the evaluation of next-generation cyber security solutions, including commercial products, PREDICT DHs and DPs will make the types of data described below available to the research community and potentially to international entities.

The types of data to be made available include but are not limited to:

Address Space Allocation Data: Address allocation data is internet data that contains internet protocol (IP) addresses that have properties that can be used to characterize internet topology. The IP addresses in this dataset are typically determined from measurement traffic and not actual sender-receiver communications and are not associated with specific individuals.

Border Gateway Protocol (BGP) Routing Data: BGP routing data capture "snapshots" of the topological state of the internet by archiving Border Gateway Protocol (BGP) routing tables from internet routers in many locations around the world (i.e., Internet Exchange Points). Each routing table expresses the "view" of the internet from that router's point in the overall topology. These datasets contain only topology information; they do not contain any packet header information or information which relates to individuals.

Blackhole Address Space Data: Blackhole address space data is collected by monitoring routed but unused IP address space that does not host any legitimate networked devices (e.g., hosts or routers). To standardize the terminology "blackhole address space" is used to refer to any unoccupied internet address space, which elsewhere may be referred to as: darkspace, darknets, sinkholes, and background radiation. Domain Name System (DNS)Data: The Domain Name System (DNS) is a distributed hierarchical naming system that at its most fundamental level provides a mapping between IP addresses and names. DNS data includes: DNS traffic (e.g., queries and/or responses); DNS server logs; DNS related metadata. These datasets may be collected at or near clients, from DNS recursive resolvers, or

DNS servers for an enterprise, top-level, or root domain.

Intrusion Detection System and Firewall Data: Intrusion Detection System (IDS) and firewall data refers to firewall and IDS configuration data, IDS firewall logs and policies and may include protective actions or alerts.

Infrastructure Data: Infrastructure data is information and metadata about the internet's physical systems and architecture. Infrastructure data includes, but is not limited to: Internet Exchange Point (IXP) lists; directories of international telecommunications cables; telecommunications system configuration data, such as locations of landing points, cable capacity, dates of construction and expansion, and logs of known outages.

Internet Topology Data: Internet topology data consists of raw and curated topology data gathered from across the internet. Internet topology data may be obtained from traceroute probes and could include IP addresses on machines that a packet traverses along the forward path to a target destination. Additionally, internet topology datasets may be organized into router-level or Autonomous System-level.

Internet Protocol (IP) Packet Headers: Internet Protocol (IP) packet header datasets are comprised of IP headers containing information such as source and destination IP addresses and other transport protocol (e.g., TCP, UDP, ICMP, SCTP) header fields. No packet contents are included.

Performance and Quality Measurements:

Performance and quality measurement datasets characterize performance or quality of networks and network services, including response times, throughput, goodput, reliability and resilience, mean-times-between-failure, jitter, diurnal variations, and other measurements, and indicators of Internet quality. Presently the PREDICT project provides VOIP data in this category where the datasets are composed of end-to-end data that characterizes the quality of the paths that VOIP telephone calls take and contains Session Initiation Protocol (SIP) teardown messages collected from both ends of the conversation.

Synthetically Generated Datasets: Synthetic datasets are datasets created on an artificial testbed using synthetically generated background traffic in conjunction with a foreground attack scenarios.

Unsolicited Bulk Email: Unsolicited bulk e-mail, or spam, datasets may include spam logs collected at individual organizations, reputation lists data, and e-mails, including both headers and contents, captured at spam traps or otherwise specifically identified as spam. The unsolicited bulk email datasets may also include IP addresses or e-mail addresses of suspected spammers and potentially known spam e-mail message contents.

Traffic Flow Data (e.g., netflow): Traffic flow datasets are internet traffic flows between two endpoints that have attributes such as source and destination IP address, source and destination port, protocol type, and packet and byte counts. The format of the traffic flow datasets are netflow, IPFIX, and argus.

Offerors are invited to submit proposals to participate in the PREDICT project by addressing one or both technical areas. In all cases, the offeror shall propose to provide datasets for publication and hosting that are compliant with all laws and regulations that are pertinent to the dataset content, to include AF and DHS privacy policies, and full compliance with the PREDICT legal framework (which includes international dissemination), also described above. Furthermore, the Government reserves the right to select one or more tasks per white paper/ proposal and to select individual PREDICT dataset types for any task proposed. An overarching requirement of all Data Providers (DPs) is an explicit assertion that they own or have a right to control and disclose to researchers the data they propose to provide, and that they will provide a legal and ethical risk assessment of each dataset they would provide (within thirty (30) days of selection). Lastly, to support measuring the utility of the data PREDICT provides, offerors will need to identify metrics to describe the utility, growth and management of the data they host or provide.

In addition, central to PREDICT management and operations is the PREDICT Coordinating Center (PCC). The PCC facilitates the release of datasets by data hosts to approved researchers, subject to the terms and conditions set forth by DHS, the PCC, data providers, and data hosts. In support of these activities, the PCC develops, hosts and maintains a web portal (see http://www.predict.org) that advertises the catalog of datasets available from the PREDICT program and automates the generation of appropriate agreements for and between PREDICT entities. Offerors for either the DP and/or DH technical area are required to

coordinate with the PCC to support the PREDICT legal framework. White papers/proposals for the PCC are not being solicited under this BAA.

Finally, the PREDICT project relies on program-wide collaboration and outreach efforts to the greater information technology research community. It is anticipated that there will be three (3) principal investigator (PI) meetings a year at performer locations in the United States, and offerors are encouraged to describe outreach activities that would be consistent with their proposals.

(2) Section II, AWARD INFORMATION, the last sentence is revised for this specific focus area ONLY to read as follows:

"Awards of efforts as a result of this announcement will be in the form of cooperative agreements only."

(3) Section IV, APPLICATION AND SUBMISSION INFORMATION, paragraph 3, SUBMISSION DATES AND TIMES, is revised to read as follows for this specific focus area ONLY:

"WHITE PAPER DUE DATE AND TIME: White papers will be accepted on or before 2 PM Eastern Standard Time, 6 April 2012 for this focus area ONLY. Late white paper submissions will not be accepted after this due date. Only white papers are due at this time. Full proposals will be requested by the Government from those Offerors selected in the white paper evaluation process.

(4) Section VII, AGENCY CONTACTS, for this specific focus area ONLY, the cognizant Technical Point of Contact (TPOC) is specified below:

TPOC Name: Robert Kaminski
Telephone: (315) 330-4459
Email: Robert.Kaminski@rl.af.mil

Contracting Office Address:
AFRL/Information Directorate
26 Electronic Parkway
Rome, New York 13441-4514

Primary Point of Contact.:
Lynn G. White,
Contracting Officer
Lynn.White@rl.af.mil
Phone: (315) 330-4996
Fax: (315) 330-8120

Return To Opportunities List
Watch This Opportunity

For Help: Federal Service Desk Accessibility

CYBER ASSURANCE TECHNOLOGIES

Solicitation Number: BAA-11-01-RIKA
Agency: Department of the Air Force
Office: Air Force Materiel Command
Location: AFRL - Rome Research Site

Note: There have been modifications to this notice. To view the most recent modification/amendment, click here

Complete View

Original Synopsis
Presolicitation
Dec 13, 2010 11:24 am

Changed
Jan 19, 2011 2:59 pm

Changed
Feb 01, 2011 9:25 am

Changed
Dec 22, 2011 8:10 am

Changed
Mar 15, 2012 10:08 am

Return To Opportunities List
Watch This Opportunity

Solicitation Number:
BAA-11-01-RIKA

Notice Type:
Modification/Amendment

Synopsis:
Added: Dec 22, 2011 8:10 am
The purpose of this modification is to republish the original announcement, incorporating all previous modifications, pursuant to FAR 35.016(c). This republishing also includes the following changes: (a) Section IV, Application and Submission Information, Paragraph 5: Added new URL for National Industrial Security Program Operating Manual (NISPOM); and (b) Section VII, Agency Contacts: Made changes to reflect new AFRL Ombudsman. No other changes have been made.
NAICS CODE: 541712

FEDERAL AGENCY NAME: Department of the Air

GENERAL INFORMATION

Notice Type:
Modification/Amendment

Original Posted Date:
December 13, 2010

Posted Date:
December 22, 2011

Response Date:
-

Original Response Date:
-

Archiving Policy:
Manual Archive

Original Archive Date:
-

Archive Date:
-

Original Set Aside:
N/A

Set Aside:
N/A

Force, Air Force Materiel Command, AFRL - Rome Research Site, AFRL/Information Directorate, 26 Electronic Parkway, Rome, NY, 13441-4514

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)

TITLE: Cyber Assurance Technologies

ANNOUNCEMENT TYPE: Initial announcement

FUNDING OPPORTUNITY NUMBER: BAA 11-01-RIKA

CFDA Number: 12.800

I. FUNDING OPPORTUNITY DESCRIPTION:

This BAA is a contracting tool directly responsive to Air Force Research Laboratory (AFRL) Integrated Cyber Defense attributes.

This BAA seeks to procure proactive cyberspace defensive capabilities for anticipating and avoiding threats through understanding the cyber situation, predicting adversarial actions, assessing potential impacts, and for implementing deterrence and effects-based defensive methodologies. It also supports work to detect and defeat threats and protect information systems by engagement and influence through defensive mechanisms employing such methods as adversary denial and deception. Also included are areas to adaptively maintain, organize, and automatically regenerate and reconstitute resources to ensure continued mission operations.

The Air Force Research Laboratory, Information

Directorate is soliciting white papers for Cyber Mission focus areas and Computer Network Defense & Support. The following section provides a description of focus areas within Integrated Cyber Defense and a general description of the Computer Network Defense (CND) & Support Technology base.

NOTE: The POC for each focus area is provided for QUESTIONS ONLY. See Section IV Paragraph 6 for submission details.

FY 11 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 of our networks. If we control the dynamics of our systems and networks, any deviation from these known dynamics can also provide an opportunity for increased discrimination of attacker activity and unexpected system states. AFRL will pursue Science & Technology for defensive cyber maneuver and agility to disrupt adversary cyberspace operations, including adversary 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. We wish to disrupt our adversaries and not ourselves. The security of such mechanisms is also paramount, so that their power is not co-opted by attackers against us for their own purposes.

Objective: The objective is to avoid attacks by making it harder for a determined adversary to succeed by increasing agility, diversity, and redundancy, to disrupt attack planning and execution.

Questions regarding this focus area can be directed to:
Walt Tirenin (315) 330-1871 Walt.Tirenin@rl.af.mil

For FY12, we are specifically seeking white papers in the two areas of "Polymorphic Enclaves" and "Polymorphic Machines" as described below.

FY 12 SPECIFIC FOCUS AREA: POLYMORPHIC ENCLAVES

Background:

The current static nature of our systems and networks allows attackers to continually gather intelligence, and perform planning needed, to execute cyber attacks at will. Intelligence collection can occur from both outside and inside our networks; therefore agility must be incorporated

comprehensively across our networks to address these threats. Network intelligence gathered by an attacker remains valid for as long as the network remains static. In order to help defend and shield our networks from attack, we must break the underlying assumption of their static nature.

Objective: We seek to create a rapidly-shifting network architecture with automated agility and diversity mechanisms, to continually, dynamically, and unpredictably modify or morph the network into secure operational modes both before and during attacks. If a successful attack should occur, the network must not only survive the attack, but also ensure minimal disruption of the services provided by the network by "mutating" or shifting into a form that can prevent further or future attacks. These capabilities must, however, maintain the transparency and utility of the network and its services to authorized users, while creating uncertainty and complexity for the attacker. Potential agility techniques may include asymmetric routing; MAC, IP, and Port hopping; service migration; OS "fingerprint" spoofing; and possibly protocol mutations. These techniques must be employed in combination with a system-level architecture that ties these mechanisms together, to ensure optimal effectiveness and proper management.

Questions regarding this focus area can be directed to:
Walt Tirenin (315) 330-1871 Walt.Tirenin@rl.af.mil

FY 12 SPECIFIC FOCUS AREA: POLYMORPHIC MACHINES

Background:

Large-scale adoption of homogeneous computing environments, such as the Federal Desktop Core Configuration (FDCC), creates significant risk of wide-spread and rapidly-executed disabling attacks. Standardized machine configurations like the FDCC are widely adopted in government and industry. They have been shown to reduce maintenance costs and some vulnerabilities by simplifying and standardizing configuration, and thus reducing the incidence of attacks due to human errors. Unfortunately, a single attack exploit for the standardized configuration can be used to compromise all systems with that configuration. To counter this threat, we can leverage for example, virtualization extensions found in modern commodity processors to provide low overhead diversification of code. We can also apply metamorphic transformations on code, a technique that has been effectively used by malware authors, to create semantically equivalent but behaviorally different variants of programs.

Objective: We seek a variety of different methods and mechanisms, integrated and applied in a manner that is controlled by the transformation and diversification process, and yet appears to an attacker to be a continuously and randomly shifting target space. These capabilities must, however, maintain the transparency and utility of the systems to authorized users, while creating uncertainty and complexity for the attacker.

Questions regarding this focus area can be directed to:
Sergey Panasyuk (315) 330-4721

Sergey.Panasyuk@rl.af.mil

FY 11 & FY12 SPECIFIC FOCUS AREA:
INCORRUPTIBLE DATA CODES /
EXECUTABLES

Background:

The Department of Defense (DoD) requires trustworthy data and software executables for successful performance of assigned missions.

Objective: Deliver self-contained, verifiably incorruptible/trustworthy data and executables with protection while at rest, under execution, or in transit upon and within any environment/system relevant to the warfighter. This includes both our own systems and systems that we do not own or directly control.

Research Concentration Areas: The "Incorruptible Data Codes / Executables" focus area is interested in the research challenges identified below. However, different approaches and concepts deemed to have significant potential to achieve the stated objectives will be considered.

• Development and technical evaluation and refinement of watermarking algorithms and protocols for the purpose of information provenance, pedigree, and assurance:

• Addressing all forms of data and multimedia formats; to include but not limited to: images, audio, video, formatted and raw data types

• Protocols with provable security which incorporate other accepted security mechanisms (timestamping, hashing, key exchange, etc.)

• Particular emphasis on:
Interaction of watermarked data with watermarked/secured code which has Anti-Tamper and Protection guarantees

• Watermarking algorithms and protocols which provide multiple aspects (provenance, pedigree, assurance) while working in conjunction with data for specific application (sensing, etc)

• Software-only data and executable protections

• Hardware-assisted data and executable protections

• Measuring and verifying incorruptibility/trust

Questions regarding this focus area can be directed to:
Chad Heitzenrater (315) 330-2575
Chad.Heitzenrater@rl.af.mil

FY11 & FY12 FOCUS AREA: ASSURED EXECUTION

Background:

The current focus of computer security is at the operating system (e.g. role-based users), applications (e.g. anti-virus programs), and the network (e.g. firewalls). Focus needs to be shifted to the operating system at the hardware and virtualized hardware layers. Innovative technology

developments are sought to defend computers and computer networks, and assure dynamic mission objectives.

Objective: The vision of this program is "A trusted execution environment within each device (e.g. computer, network router) that is a platform for conducting cyber defensive operations that uses "out of band" communication, and remains trusted should the host be compromised." The two areas of high interest are 1) Virtualization and 2) Root of Trust.

Virtualization: The combination of complex applications running on complex operating systems presents a very large footprint to attack. Additionally, DoD has very little control over modern shrink-wrapped software applications and operating systems. Current cost concerns prohibit DoD from developing, building, and maintaining their own applications, operating systems, and hardware. Virtualization technologies offer ways to defeat cyber attacks prior to engagement. Key concepts include but are not limited to: A secure environment that encapsulates and protects the operating systems, device drivers, and applications; secure, segregated, inaccessible areas for critical code; and secure communications for critical code processes.

Root of Trust: The integrity of computers and computer networks is dependent on the integrity of the host hardware and host root account. This area of research investigates modeled hardware root of trust that imparts immunity from an adversary with root access to the underlying host. Innovative ways to achieve a secure root of trust on a host are

sought. Also sought are ways to achieve a network root of trust.

Questions regarding this focus area can be directed to: Joe Carozzoni (315) 330-7796 Joe.Carozzoni@rl.af.mil

FY 11 & FY12 SPECIFIC FOCUS AREA: FIGHT THROUGH & SURVIVE WITH MISSION ASSURANCE

Background:

The DoD has a critical need for information systems that adapt and/or gracefully degrade when unexpected events occur. These systems are subjected to constant change such as overload, component failure, cyber attacks, evolving operational requirements, and/or a dynamic operational environment. A system should adapt to these changes by reconfiguring its resources to provide a different, though acceptable, level of service and security to assure mission essential functions. Without adaptation many important activities receive fewer resources than needed while less important activities waste resources by receiving more resources than necessary. Most existing systems either do not adapt or have ad hoc hardwired mechanisms to accommodate only a small, predefined, set of changes. There are no standard methodologies or common tools to assist application developers in managing this sort of dynamic adaptation.

Objective: The vision for this focus area is "survive with mission assurance". This focus area is

concerned with runtime assessment and management of resources/assets to ensure mission essential functions and conveying trustworthiness.

Research Concentration Areas: The "Fight Through & Survive with Mission Assurance" focus area explores the research challenges below, but other approaches that achieve the stated objectives will be considered:

(1) Cyber Defense Metrics - Identify low-level observable properties and measurable quantities that contribute to the mission based assessment.

(2) Mission Aware Adaptive Tradeoffs - Integration of QoS (Functionality) and QoIA (Security) management. There is a need to understand tradeoff policy and de-confliction of QoS and QoIA based on the mission. There is a need to develop fine-grained tunable IA mechanisms and controls.

(3) Survivability Architecture- Compose a survivability architecture that supports and enforces service delivery and information assurance requirements based on mission priorities.
Funding for this focus area is not available in FY12.

Questions regarding this focus area can be directed to:
Pat Hurley (315) 330-3624 Patrick.Hurley@rl.af.mil

FY 11 & 12 SPECIFIC FOCUS AREA:
SELF-REGENERATIVE INCORRUPTIBLE

ENTERPRISE THAT DYNAMICALLY RECOVERS WITH IMMUNITY

Background:

Existing approaches to information system security and survivability consist of preventing, detecting and containing unintentional errors and/or cyber attacks. The problem with this approach is that regardless of how well systems are protected or how well they tolerate errors and/or attacks; they will eventually fail over time unless they have the ability to self-regenerate. Once a successful cyber attack is discovered the adversary can quickly use the same attack over and over again to cause the same negative effect on our mission. Existing systems are currently taken offline and out of the fight for hours to days to be repaired and there is no guarantee that the repair is immune to the attack or variants of the attack. What are needed are information systems that are able to dynamically recover with immunity in mission time without human intervention in response to unforeseen errors and/or previously unknown cyber attacks.

Objective: The vision for this focus area is "recover with immunity". This focus area is concerned with recovering with immunity from errors and/or cyber attacks to ensure mission critical systems stay in the fight.

Research Concentration Areas: The "Self Regenerative, Incorruptible Enterprise" focus area explores the research challenges below, but other approaches that achieve the stated objectives will be considered:

(1) Persistent applications (data & state) - The goal of this technology area is to make applications hard to corrupt, disable or remove (like malware). When an attack is successful these applications find a way to keep performing the mission.

(2) Machine Generated Reconstitution - The goal of this technology area is to automatically machine-generate repairs to recover with immunity from errors/cyber attacks.

(3) Reconstitution of Data and State - The goal of this technology area is mission continuation by automatically repairing corrupted data & state to remove residue from errors/cyber attacks.

(4) Understanding Synthetic Diversity or other technology used to recover with immunity - There is a need to better understand the use of synthetic diversity or other technology used to ensure complete attack space coverage and/or understand the effectiveness against various classes of cyber attack.

Funding for the Self-Regenerative Incorruptible Enterprise focus area in FY12 will focus on persistent applications (data & state).

Questions regarding this focus area can be directed to:
Pat Hurley (315) 330-3624 Patrick.Hurley@rl.af.mil

FY 11 & FY12 FOCUS AREA: CYBER MISSION

ASSURANCE

Background:

This focus is on novel approaches to assure critical Air Force mission essential functions (MEF) in a contested cyber environment. Mission assurance seeks to codify a top-down approach for mapping MEF dependence on cyberspace across the information lifecycle (information generation, processing, storage, transmission, consumption and destruction), identifying cyber vulnerabilities, developing metrics to assess the risk from cyber vulnerabilities on MEF, and developing strategies to mitigate the vulnerabilities. We view mission assurance in the context of preventing and avoiding threats by deterring potential threats through increased costs and reduced benefits.

We seek a scientific basis for mission assurance, including the development of mathematical models to represent MEF dependence on cyber, an exploration of the fractal nature of mission mapping, and the development of metrics for the cost of vulnerability mitigation in proportion to the increased cost to potential threats. These will in turn enable the development of more rigorous approaches to situational understanding as well as command and control.

Research into cloud computing technologies could provide potential solutions to the mission assurance research area by increasing the availability and redundancy of continuous or contingency operations. We invite novel techniques for secure data storage, processing and communication practices within a cloud

architecture. We seek solutions that utilize the dynamic characteristics of cloud computing technology to prevent and avoid threats. Under the establishment of an internal center of excellence in cloud computing, there is a need for further research within AFRL and the DoD community. The center of excellence should provide opportunities for this research through collaboration and related internships.

Objectives:

• Create a scientific basis for mission assurance.

• Provide novel techniques for secure data storage, processing and communication practices within a cloud architecture.

• Construct appropriate research opportunities within the DoD community.

• Support other S&T initiatives in the areas of situational understanding and command and control

Questions regarding this focus area can be directed to: Dr. Sarah Muccio (315) 330-4016 Sarah.Muccio@rl.af.mil or Mr. Brian Kropa (315) 330-1544 Brian.Kropa@rl.af.mil

The scope of this BAA is not limited to the aforementioned focus areas.

Other applicable areas of technology include, but are not limited to, Rapid/Live Forensics, Botnet Detection & Mitigation, Attack Attribution, Insider

Threat Detection & Mitigation, Range Development, and Cyber Modeling, Simulation, Metrics, and Measurements. The work could include 'Abnormality ID and Remediation' and might also include 'Cyber Economic Incentives' which would entail a look at the concept of 'Amortization of R & D' (that is, a look at quantification of how long to pay back R & D resources used for an operational improvement before the R & D/Ops improvement becomes obsolete). Also, Data Mining application under Visualization Support would be applicable.

II. AWARD INFORMATION:

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: FY 11 - $4M; FY 12 - $12M; FY 13- $12M; FY 14 - $12M; FY 15 - $9M. Individual awards will not normally exceed 36 months with dollar amounts ranging between $100K and $1M per year. There is also the potential to make awards up to any dollar value. Awards of efforts as a result of this announcement will be in the form of contracts, grants, cooperative agreements, or other transactions depending upon the nature of the proposed work.

III. ELIGIBILITY INFORMATION:

1. ELIGIBLE APPLICANTS: All potential applicants are eligible. All foreign allied participation is excluded at the prime contractor level.

2. COST SHARING OR MATCHING: Cost sharing is not a requirement.

3. CCR Registration: Unless exempted by 2 CFR 25.110 all offerors must:

(a) Be registered in the Central Contractor Registration (CCR) prior to submitting an application or proposal;

(b) Maintain an active CCR registration with current information at all times during which it has an active Federal award or an application or proposal under consideration by an agency; and

(c) Provide its DUNS number in each application or proposal it submits to the agency.

4. Executive Compensation and First-Tier Sub-contract/Sub-recipient 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 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#2:1.1.1.4.1.2.1.1

IV. APPLICATION AND SUBMISSION INFORMATION:

1. APPLICATION PACKAGE: THIS ANNOUNCEMENT CONSTITUTES THE ONLY

SOLICITATION. WE ARE SOLICITING WHITE PAPERS ONLY. DO NOT SUBMIT A FORMAL PROPOSAL AT THIS TIME. 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.

For additional information, a copy of the AFRL/Rome Research Sites "Broad Agency Announcement (BAA): A Guide for Industry," April 2007, may be accessed at: http://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/Reference%2DNumber%2DBAAGUIDE/listing.html

2. CONTENT AND FORM OF SUBMISSION:

Offerors are required to submit 4 copies of a 4-5 page white paper AND 1 electronic copy on a CD summarizing their proposed approach/solution. All whitepaper/proposals shall be submitted in Microsoft Word or PDF format, double spaced, and have a font no smaller than 12 pitch with any figures, tables and charts easily legible. The purpose of the white paper is to preclude unwarranted effort on the part of an offeror whose proposed work is not of interest to the Government. The white paper will be formatted as follows:

• Section A: Title, Period of Performance, Estimated Cost, Name/Address of Company, Technical and Contracting Points of Contact (phone, fax and email), and target technology area (e.g., Rapid Forensics) - (this section is NOT included in the page count);

• Section B: Task Objective

• Section C: Innovative Claims (How will this effort enhance or replace the state-of-the-art?);

• Section D: Technical Approach (Why is this approach superior to alternatives or current practice?);

• Section E: Biggest Technical Challenge (What are the major technical challenges in the approach? How will those challenges be mitigated?);

• Section F: Schedule and Proposed Deliverables.

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). All white papers/proposals shall be double spaced with a font no smaller than 12 pitch. 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 11-01-RIKA with their submission. All responses to this announcement must be addressed to W. John Maxey (Technical POC), as discussed in paragraph seven of this section.

3. SUBMISSION DATES AND TIMES: It is recommended that white papers be received by the following dates to maximize the possibility of award: FY11 should be submitted by 15 March 2011; FY12 by 1 December 2011; FY13 by 1 December 2012; FY14 by 1 December 2013; and

FY15 by 1 Dec 2014. White papers will be accepted anytime during the period that this BAA remains open, but it is less likely that funding will be available in each respective fiscal year after the dates cited. FORMAL PROPOSALS ARE NOT BEING REQUESTED AT THIS TIME. This BAA is open and effective until 2pm EST on 28 Sep 2015 unless cancelled at an earlier date.

4. FUNDING RESTRICTIONS: 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).

5. CLASSIFICATION GUIDANCE FOR WHITEPAPER 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 proposer 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. Proposers 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.

6. 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/isp/odaa/nispom06.html

7. OTHER SUBMISSION REQUIREMENTS: DO NOT send white papers to the Contracting Officer. All unclassified responses to this announcement will be sent via U.S. Postal Service registered mail and addressed to AFRL/RIGA, 525 Brooks Road, Rome NY 13441-4505, and reference BAA-11-01-RIKA. Electronic submission is not authorized unless expressly permitted by the technical POC listed in Section VII. Questions can be directed to the technical POC listed in Section VII.

CLASSIFIED SUBMISSIONS MUST BE SENT TO AFRL/RIGA SEPARATELY FROM UNCLASSIFIED PAPERS AS PER THE INSTRUCTIONS BELOW. 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-11-01-RIKA
AFRL/RIGA
525 Brooks Road
Rome NY 13441-4505

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 mission assurance objectives;

(3) The extent to which the offeror demonstrates relevant technology and domain knowledge, which may include testing of prototype capabilities and assessment against Information Assurance requirements; and

(4) The 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, or 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.

VI. AWARD ADMINISTRATION INFORMATION:

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.

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 no earlier than 45 days after proposal submission.

2. ADMINISTRATIVE AND NATIONAL POLICY REQUIREMENTS:

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 proposer 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. After reviewing incoming proposals, if a determination is made that contract award may result in access to classified information a DD Form 254 will be issued upon contract award. Proposers that intend to include classified information or data in their 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.

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. Data subject to export control constraints may be involved and only firms holding certification under the US/Canada Joint Certification Program (JCP) (www.dlis.dla.mil/jcp) are allowed access to such data.

3. REPORTING: Once a proposal has been selected for award, offerors will be required to submit their reporting requirement through one of our web-based, reporting systems known as JIFFY or TFIMS. Prior to award, the offeror will be notified which reporting system they are to use, and will be given complete instructions regarding its use. Please note that use of the JIFFY or TFIMS application requires customers outside of the .mil domain to purchase an approved External Certificate Authority certificate to facilitate a secured log on process. It is necessary to obtain an

ECA certificate BEFORE obtaining a JIFFY or TFIMS user account. Additional information on obtaining an ECA is available at: http://iase.disa.mil/pki/eca/index.html

VII. AGENCY CONTACTS:

Questions of a technical nature shall be directed to the cognizant technical point of contact, as specified below:

TPOC Name: W. John Maxey
Telephone: (315) 330-3617
Email: William.Maxey@rl.af.mil

Questions of a contractual/business nature shall be directed to the cognizant contracting officer, as specified below:

Lynn White
Telephone (315) 330-4996
Email: Lynn.White@rl.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 2010) 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) 904-7024; Comm: (937) 904-4407

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

Contracting Office Address:
AFRL/Information Directorate
26 Electronic Parkway
Rome, New York 13441-4514

Primary Point of Contact.:
Lynn G. White,
Contracting Officer
Lynn.White@rl.af.mil
Phone: (315) 330-4996
Fax: (315) 330-8120

Return To Opportunities List
Watch This Opportunity

For Help: Federal Service Desk Accessibility