BROAD AGENCY ANNOUNCEMENT
USAFA-PASCC-BAA-2016
Project on Advanced Systems and Concepts
for
Countering Weapons of Mass Destruction

TWO-STEP CALL ANNOUNCEMENT

FEDERAL AGENCY NAME: United States Air Force Academy (USAFA) in support of the Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction

BROAD AGENCY ANNOUNCEMENT TITLE: Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC)

BROAD AGENCY ANNOUNCEMENT NUMBER: USAFA-PASCC-BAA-2016

BROAD AGENCY ANNOUNCEMENT TYPE: Amendment 0003 to Initial announcement

CATALOG OF FEDERAL DOMESTIC ASSISTANCE (CFDA) NUMBER: 12.800

CALL ANNOUNCEMENT TITLE/NUMBER: USAFA-PASCC-BAA-2016 CALL 0004

TECHNICAL POINT OF CONTACT: The technical point of contact for this CALL as outlined in the baseline BAA is:

Dr. James M. Smith, Director
USAF Institute for National Security Studies
USAFA, CO
Email: James.Smith@usafa.edu
Phone: 719-333-2717

CONTRACTING POINT OF CONTACT: The contracting point of contact for this CALL as outlined in the baseline BAA is:

Ms. Erica Wilson, 10 CONS/PKC
USAFA, CO
PASCC Contracting Email: 10CONS.PASCC@us.af.mil
Phone: 719-333-8048

BACKGROUND: The USAFA is seeking unclassified research white papers and proposals (if requested) that do not contain proprietary information. If proprietary information is submitted it is the offerors responsibility to mark the relevant portions of their proposal as specified in the latest amendment of USAFA-PASCC-BAA-2016. The United States Air Force's Institute for National Security Studies (INSS), in partnership with PASCC, invites white papers and proposals (if requested) for studies in many broad areas related to countering the threat posed by weapons of mass destruction (WMD).

The Defense Threat Reduction Agency (DTRA) has requested that USAF INSS/PASCC issue a call for papers soliciting white papers outlining studies in response to the following directions.

With this call for papers, USAF INSS announces to academia, research institutions, and non-profit organizations it is soliciting white paper for studies that will help enable the DoD and the USG to prepare for and combat WMD and improvised threats. The white papers should propose rigorous, innovative projects that:

1. Facilitate critical engagement between U.S. and foreign subject-matter experts (SMEs) on key WMD, CWMD, or nuclear deterrence issues;

2. Address current and emerging challenges facing CCMDs and DoD; or

3. Expand knowledge or develop new concepts relevant to the national security missions and requirements of DoD and the Armed Services.

PASCC does not fund:

- Development of technologies or scientific capabilities;
- Studies about traditional cybersecurity or traditional counterterrorism;
- Construction projects;
- Proposals from Federal Agencies, Federally Funded Research & Development Centers (FFRDCs), including Department of Energy National Laboratories, or USG schools of higher education, military laboratories, or warfare centers. This includes subcontracting/sub-recipient efforts.

PROBLEM STATEMENT

Both state and non-state adversaries have indicated a growing willingness to employ a wide-range of offensive cyber tools for achieving a varied set of political and military ends. These operations in the virtual world have demonstrated both (1) critical vulnerabilities in essential U.S. and allied military and civilian infrastructure, and (2) an accompanying potential for damage and loss equaling, if not exceeding, that attainable by kinetic force.

WMD connotes a traditional threat that includes nuclear, biological, chemical, and radiological weapons, and (in some applications) enhanced high explosive weapons. This definition does not include recent advancements in non-kinetic weapons of mass effect and disruption. This expanded spectrum includes such emerging threats as dazzling and blinding weapons, ultra-sonics, directed energy weapons, and offensive cyber warfare.

Broadly defined, offensive cyber weapons are deployed in the connected virtual world (the internet, the world-wide web) and can manifest widespread effects in both virtual and physical domains, to include but not limited to:

- Corruption and destruction of critical infrastructure system controls and safeguards (power, water, transportation);
- Compromise, theft and abuse of sensitive “big data” collections (financial or healthcare records);
- Covert introduction of systemic adjustments or erroneous data to compromise the reliability and accuracy of critical and widely relied upon military and civilian systems such as GPS, frequency coordination, and time measurement networks; and
- Disinformation tactics, utilizing social media to spread (generally) plausible but false rumors and innuendo designed to strain alliances, divide polities, and undercut public confidence in institutional integrity and social cohesion.

The Russian Federation, the People's Republic of China, the Democratic People's Republic of Korea, Iran, and a number of violent extremist organizations have all embraced and employed some or all of these elements of offensive cyberspace operations against the United States and its partners and allies over the past decade. These operations are becoming increasingly sophisticated in nature, and steadily more integrated into adversary military doctrine, strategies, plans, and operations that already incorporate and integrate conventional and unconventional weapons, to include WMD. These developments necessitate an assessment of the potential nexus between offensive cyber operations and WMD and the implications of this interrelationship for the Countering WMD (CWMD) mission, which is one of DTRA's missions.

RESEARCH QUESTIONS

This analysis should include:

a. Defining, scoping, and exploring the Cyberwarfare/WMD nexus

- How adversaries may employ offensive cyber operations to improve the effectiveness, survivability, or lethality of their WMD arsenals;
- How adversaries may employ offensive cyber operations to degrade U.S. and allies defenses against WMD;
- How adversaries may employ offensive cyber operations to degrade U.S. deterrence strategies or posture, or improve their own deterrence strategies or posture;
- How adversaries may employ offensive cyber operations as a substitute for "traditional" WMD.

b. Assessing implications for CWMD Mission

- Given (a), how does the current DoD/DTRA understanding and execution of the CWMD mission address this nexus? Are there possible seams and gaps?
- If seams and gaps exist, what types of investments should be considered with regard to research and development toward new capabilities (offensive or defensive)?
- If seams and gaps exist, what types of changes should be considered with regard to CWMD strategy or policy? With regard to WMD deterrence strategy or policy?
- Should the definition of the CWMD mission be expanded to include weapons of mass disruption and effect?
- How can DTRA support CCMDs in countering adversaries' integration of offensive cyber operations and WMD in their doctrines, strategies, plans, and operations?

PROPOSED APPROACH

A proactive, collaborative, integrated approach maximizing innovation is needed to minimize the risks and unanticipated consequences of the current and future cyber threat.

A new perspective is needed to address this problem, and it should include independent organizations not anchored to traditional WMD definitional and doctrinal concepts. DTRA seeks a performer to bring together a group of private industry, Government, and academia entities in a threatcasting/futures workshop- exercise to help fuel that innovative environment, facilitating the deconstruction of the cyber-threat intersection with WMD into manageable component issues capable of allowing development of a potential way forward.

Baseline Reference Materials:

Virtual War and Weapons of Mass Deception: Stefan Banach (4/19/18) should provide the baseline reference for the proposed study topic. A publication of the United States Military Academy Modern War Institute; Banach argues that evolving cyberwar capabilities are the Next Revolution in Military Affairs, and we are ill prepared to address that prospect. Link: https://mwi.usma.edu/virtual-war-weapons-mass-deception/

The 2014 NDU Study Link:
http://ndupress.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccationalPaper-10.pdf

An outline of the threatcasting approach:
http://threatcasting.com/wp-content/uploads/2017/09/ThreatcastingWest2017.pdf

End Products:

- One Threatcasting exercise to examine implications of addressing cyberwarfare within the expanded WMD paradigm (to include SOCOM and CYBERCOM)
- Final Report not to exceed 30 pages.
- Power Point Summarizing Brief not to exceed 10 pages
- One Concept Paper on the Cyberwar-WMD nexus (NTE 3 pages)

REQUIREMENT DESCRIPTION: The USAFA is soliciting white papers for research under **Section j – Research Areas of the Broad Agency Announcement USAFA-PASCC-BAA-2016 Amendment 0003.**

THIS WILL BE A TWO-STEP CALL ANNOUNCEMENT:

FIRST STEP: WHITE PAPERS

WHITE PAPER FORMAT: White papers submitted in response to this CALL should conform to the requirements found in the latest amendment of USAFA-PASCC-BAA-2016, to include a brief technical description, a short resume of the principle investigator and a rough order of magnitude of cost.

WHITE PAPER DUE DATE AND TIME: The due date for white papers submitted in response to this CALL is no later than 4:00 PM Local Time on **23 January 2019**. ***White papers received after the due date and time shall be governed by the provisions of FAR 52.215-1(c)(3).***

WHITE PAPERS AND ALL QUESTIONS ARE TO BE E-MAILED TO:
10 CONS/PKC
Attn: Erica Wilson
Email: 10CONS.PASCC@us.af.mil

***Please note: It is the responsibility of the submitting organization to ensure white papers have been received by the USAF Academy. If you do not receive a confirmation email within 48 hours of submitting your white paper, it is your responsibility to contact the contracting office to ensure receipt. Failure to do so may result in a late white paper. White papers not received on time will NOT be processed.**

WHITE PAPERS EVALUATED AND SELECTED: White papers will be evaluated and full proposals requested in accordance with the latest amendment of USAFA-PASCC-BAA-2016. Only white papers that meet agency needs will be funded. Further, be advised as funds are limited, otherwise meritorious white papers may not be funded. Offerors whose white papers are not of interest to the Government will be notified via letter that the effort proposed is not of interest to the Government.

SECOND STEP: PROPOSALS

INTENT TO PROPOSE: Should potential offerors receive a formal request for proposal, they are requested to advise the Grants Officer point of contact (by e-mail) if they intend to submit a proposal. Such notification is merely a courtesy and is not a commitment by the offeror to submit a proposal.

PROPOSAL INSTRUCTIONS: Offerors are requested to follow the instructions within the baseline BAA, USAFA-PASCC-BAA-2016 Amendment 0003 on how to submit a proposal. All proposals must be submitted through Grants.gov, https://www.grants.gov and must include all the required forms specified within the baseline BAA.

REGISTRATION REQUIREMENTS: Prospective Awardees shall be registered in the System for Award Management (SAM) database prior to award, during performance, and through final payment of any award resulting from this announcement. Offerors may obtain information on registration and annual confirmation requirements via the Internet at www.sam.gov or by calling 1-866-606-8220.

ANTICIPATED FUNDING: The total anticipated funding for all awards made as a result of this CALL is $30,000.00. All funding is subject to change due to Government discretion and availability, as well as technical needs.

ANTICIPATED TYPE OF CONTRACTS/INSTRUMENTS: The Government anticipates awarding the instrument best suited to the nature of research proposed including a grant, cooperative agreement, or procurement contract. Potential offerors are reminded that in accordance with 32 CFR 22.205 and 2 CFR 200.400, a fee or profit may not be paid to the recipient of a cooperative agreement or grant.

PERIOD OF PERFORMANCE: The anticipated period of performance for awards resulting from this CALL is generally 12 months per award, depending on the proposed effort.

PROPOSAL DUE DATE AND TIME: The due date for proposals will be no less than 30 days after a formal request for proposal has been sent to the submitter of the selected white paper(s). The formal request for proposal will establish the due date. **Proposals received after the due date and time shall be governed by the provisions of FAR 52.215-1(c)(3).**

ANTICIPATED NUMBER OF AWARDS: The Government reserves the right to make multiple awards, single awards, or no awards pursuant to this CALL.

ANTICIPATED AWARD DATE: The Government anticipates issuing awards subject to this CALL in the March 2019 timeframe; however, timelines depend on quantity and merit of white papers/proposals received.

CALL AMENDMENTS: Offerors should monitor Grants.gov (http://www.grants.gov) for any additional notices to this CALL that may permit extensions to the white paper submission date or otherwise modify this announcement.

APPLICABILITY OF BASELINE BAA: All requirements of USAFA-PASCC-BAA-2016 Amendment 0003 apply unless specifically amended and addressed in this CALL. For complete information regarding USAFA-PASCC-BAA-2016, refer to the initial opened-ended BAA as amended. It contains information applicable to all calls issued under the BAA and provides information on the overall program, proposal preparation and submission requirements, proposal review and evaluation criteria, award administration, agency contacts, etc. Direct questions may be addressed to the points of contact identified above.