BAA-18-R-STCD

# WHITE PAPER CALL 007

## Autonomous Defensive Cyber Operations (ADCO)

10 June 2019

This call for White Papers (WP) is being issued under Broad Agency Announcement (BAA), BAA-18-R-STCD, which was published on FedBizOpps.gov on 20 June 2018, and last updated on 18 April 2019. Respondents must refer to the solicitation document entitled BAA-18-R-STCD_ 20180620 BAA Final Rev6 (18April19), and it must be read in conjunction with this call for WP's. All instructions set forth in the BAA-18-R-STCD solicitation document apply to this call.

The Space and Terrestrial Communications Directorate (S&TCD) is issuing this call for WP's in association with Topic #S1825. To be eligible for consideration and possible contract award, the technology or methodology shall be either basic research, applied research, advanced technology development not for a specific system/hardware, or demonstration and validation.

**ADDITIONAL INFORMATION:**

Problem Statement:

Cyber defenders react at human speed. Current techniques are manual, time-consuming, and impose an unacceptable burden of knowledge on the defender. Current techniques lack designs that take the limitations of a human analyst into consideration. Cyber defenders lack the time and resources to protect against autonomous cyberspace tactics, techniques, and procedures designs, such as those that employ machine learning (ML), and artificial intelligence (AI) to orchestrate increasingly sophisticated attacks against autonomous systems at speeds and frequencies well beyond the abilities of human analysts. ML and AI technologies are needed to act as a force multiplier to help expedite and ease the cyber defender's essential tasks, how they use and understanding defensive cyber tools, how they answer the Commander's cyber questions, and how they understand which cyber threats to mitigate and how.
Cyber threats are continuously evolving and as such, future cyber attackers will leverage autonomous designs in their orchestrated, sophisticated cyber-attacks and increase the speed at which the attacks are executed beyond what today's traditional human cyber attackers are capable of doing. Implementing machine learning into the tactical network and cyber tools creates an opportunity to achieve overmatch and have the upper hand against dynamic and evolving cyber attackers. As the observe, orient, decide, and act loop implemented by cyber defenders is required to shrink to deal with autonomous cyber-attacks it will be necessary to proactively identify zero day

vulnerabilities, known vulnerabilities, and misconfigurations in tactical networks, systems, and applications before attackers can exploit them.

Despite the benefits of autonomous design, autonomous decision making engines have a unique attack surface when methods and algorithms such as those used in AI and ML have been incorporated in their decision making process. Attacks can: target vulnerabilities in the autonomous software, target how the autonomous software's decisions engines make their decisions and create situations where the wrong decision is made, and target information going into and out of the autonomous software. Thus a need exists to secure and assess the validity of autonomous decision making engines.

Information Sought:
S&TCD is interested in receiving WPs on the above topic from companies that have a successful track record developing ML and AI implementations for the purpose of enterprise and/or tactical ADCO although the main focus is tactical and as far down into the network as feasibly possible. The identified technology solution(s) should be at technology readiness level (TRL) 3 or higher but not over TRL 6 to be considered. The end state of the identified solution should be a demonstration/proof of concept system at TRL 6 that can be tested and verified in United States Army specific tactical information technology environments and then transitioned and integrated with an Army Program of Record's systems and applications.

White papers can introduce the incorporation of commercial standards/technologies, however, they should demonstrate the development of novel and innovative techniques. S&TCD's expectation is that the focus of any effort conducted under this BAA topic will be to address the core goal of developing an integrated ADCO system for use in the tactical environment. Proposers are encouraged to submit WPs even if they will only address one area in Topic #S1825 as not a requirement to address all areas.
It is essential that any identified solutions are based around designs that have a clear path to be matured and commercialized to meet other important system goals including, but not limited to: affordability; network scalability; network bandwidth usage; risk management framework (*i.e.* information assurance) authorizations; network management; cognizant of size, weight, power, and cost constraints of disconnected intermittent and limited (DIL) tactical Army networks; cognizant of how different autonomous cyber defenses will integrate with each other, with non-autonomous cyber tools, and with Army applications and systems; cognizant of the system processing load and impact autonomy creates; adaptability to executing upon a broad array of hardware platforms and operating systems that are not created for nor were expected to operate autonomous software upon; ability to operate on varying amounts of data from very small messages in small amounts to very large messages in large amounts; and ability to work in a non-Internet connected environment. Existing commercial products that are unable to support the constraints of DIL tactical Army networks as is will be considered if the proposer is able to make the case that the product is at a TRL 5 or below when applied to tactical Army networks.

**AWARD INFORMATION:**

1. ANTICIPATED AWARD DATE: January 2020

2. FUNDING: Under this call, the Government intends to award up to four (4) contract(s) with a period of performance of a 12-month base with up to four (4) 12 month options. The option years are not guaranteed and are based on funding availability. The anticipated funding for this call is up to $25M for the total contract ceiling, however, the Government reserves the right to award smaller or larger contracts or assistance instruments.

| **Fiscal Year (FY)** | FY20 | FY21 | FY22 | FY23 | FY24 | |
|---|---|---|---|---|---|---|
| **Anticipated Funding** | $5,019 | $7,157 | $4,606 | $4,380 | $3,241 | $24,403 |

NOTE: This funding profile is an **estimate only** and not a contractual obligation for funding. All funding is subject to change due to Government discretion and availability. Potential respondents should be aware that due to unanticipated budget fluctuations funding in any or all areas may change with little or no notice. Awards under this call are expected to range from $3M to $25M with a range between $3M-$7M per year. The Government reserves the right to select all, part, or none of the WP's received, subject to the availability of funds.

3. BAA TYPE: This is a call for WP's only, and will be governed by the "two-step" process described in General Information of the BAA-18-R-STCD. **Respondents that submit a proposal without first submitting a WP may not be eligible for award.**

4. SUBMISSION INSTRUCTIONS: This call should not exceed 10 pages in length (single sided, single spaced, with 12-size font). The 10 page limitation does not include the Rough-Order-of-Magnitude or the Cover Page. Refer to baseline BAA-18-R-STCD Section III for all other instructions on WP preparation, submission, and evaluation.

5. QUESTIONS DUE DATE AND TIME: Technical questions are due no later than **24 June 2019 3:00 pm EST** via email to the Technical Point of Contact (TPOC) with a carbon copy (Cc) to the Contracting Officer (KO), Contract Specialist (KS), and Acquisition Management Team (AMT) Mailbox, as listed below. Questions and answers will be posted to FBO.

   Government will publish questions and answers received by industry to FBO, via a revision to this Data Call, per ADDENDUM 001, Technical Questions and Clarifications, herein.

6. WHITE PAPER DUE DATE AND TIME: WP's are due no later than **15 July, 2019 3:00 pm EST** via email to the TPOC with a Cc to the KO, KS, and AMT Mailbox, as listed below.

TPOC: frank.c.geck.civ@mail.mil
AMT: usarmy.apg.ccdc-c5isr.mbx.stcd-amt@mail.mil
KO: Brian Holman, brian.j.holman2.civ@mail.mil
KS: Andrew Pilone, andrew.m.pilone.civ@mail.mil

If the submission will be classified, respondents should contact the TPOC and KO for instruction on how to submit the WP, via appropriate methods/channels. The KO shall be informed, in writing, that a classified WP has been submitted, its title and to whom it was submitted to.

Contractual questions may be directed to the KO and/or KS at any time.