HR001117S0051

Harnessing Autonomy for Countering Cyberadversary Systems (HACCS)

Frequently Asked Questions

As of September 6, 2017

Q35: Please elaborate on the TA4 role of voice of the offense.

A35: During years 1-2, the VOTO team will serve in an advisory capacity. In the latter part of the program, TA4 will act as the integrator and the focal point for transition efforts (continuing through the options).

Q34: Is an interface overlay for TAs 1-3 to TA4 of interest to the program?

A34: Proposals to the individual TAs can include UI work, but that is not a primary focus.

Q33: BAA Page 20: Volume 1: Technical and Management proposal states "the maximum page count for Volume 1 is 30 pages with a required minimum of 10 technical pages (Technical Approach Section). However, in the subsequent Volume 1 breakout by section it only references a "Technical Plan" (v.). Is the "Technical Plan" section the 10 technical pages section referenced on page 20, or, does it also include the Innovative Claims section?

A33: It does include innovative claims.

Q32: Is a publicly known bug in software X considered an n-day, if it has not been explicitly publicly identified as a vulnerability?

A32: Yes.

Q31: Is a publicly unknown vulnerability, in use by an adversary, considered an n-day?

A31: No.

Q30: If a publicly known vulnerability in software X also appears in software Y, but has not been publicly disclosed in software Y, is it still an n-day in software Y?

A30: If it is due to a common component (e.g., a library), then it is an n-day.

Q29: Is a known vulnerability in version A of software X still an n-day in version B of software X, if it has not been publicly disclosed in version B?

A29: If version B > version A, then it is an n-day.

As of August 18, 2017

Q28: Can you please clarify the boundary between TA3 and TA4 roles in generating the agent implementation? Is TA3 generating components that go into a TA4 agent framework or is TA3 generating standalone agents?

A28: TA3 will generate agent implementations sufficiently mature to demonstrate safety and lateral movement capability. TA4 will generate effects and generate or integrate with existing infrastructure(s) for deploying these agent implementations or lessons learned from the TA3 work.

Q27: The BAA says that TA4 will implement the neutralization effects. Could you please clarify what TA3's role is in developing these effects? Is it in terms of defining them and evaluating overall effectiveness/safety/correctness/etc.?

A27: TA3 will generate context for lateral movement, validation for agent implementation, and validation for any rules of operation. TA4 will generate effects. In other words, TA3 generates the effect payload(s) vehicle and TA4 generates the effect payload(s).

Q26: Are organizations supporting TA4 prohibited from supporting other TAs?

A26: The only restriction is that a TA4 prime may not serve as prime elsewhere in the program. Subcontractors to TA4 may serve as a prime or subcontractor to the other TAs.

Q25: What is the expected role of the human operator in the final system? To what extent should the HACCS system interventions be automated?

A25: The final system may have some need for a human in the loop, but, consistent with the BAA, it should be automated to the greatest extent possible.

Q24: Is the framework developed by TA4 intended primarily for testing/evaluation purposes, or is it meant to be a hardened, deployable anti-botnet system?

A24: HACCS is a research and development program. The TA-4 framework should be robust enough for rigorous testing and evaluation.

Q23: On page 11 of the slides, it states that "Characterize x% of the global IP, address space," what does this include? Public IP space only? What are the boundaries/limits?

A23: Public IP space. However, per the BAA, full identification of devices behind each point is desired.

Q22: We were unable to attend the Proposers Day, but are interested in seeing any slides or other information you provided on that day. If you have an email list that you use to send updates, I would appreciate being added to that list.

A22: Links to the Proposers Day slides, along with the FAQ and BAA, will appear on the DARPA opportunities webpage - http://www.darpa.mil/work-with-us/opportunities.

Q21: An extensive test environment will be needed and created for this. Will the government be funding this?

A21: In order to realize time and cost efficiencies, DARPA is looking to leverage existing test environments and facilities.

Q20: One of the biggest hurdles to fingerprinting a "hack" is knowing where it originated. A lot of times effective botnets & hacks mask their locations and intents. With rules of engagement in mind, and noting your requirement to "insert an agent" into the gray network – are you suggesting that to have true cyber defense, you in actuality have to be authorized to execute offensive cyber?

A20: The program is developing technologies that address a specific type of threat and concept of operations. Doctrine, operational authorities, and the relevant legal framework for use of any such technologies are beyond the technical scope of the effort.

Q19: Detecting known or zero-day?

A19: To the extent that the question refers to vulnerabilities, the program is looking to generate exploits only for known vulnerabilities, also referred to as n-day vulnerabilities.

Q18: How are the success factors measured?

A18: The success of individual components will be evaluated as delineated in the BAA.

Q17: What is the outcome of the program?

A17: The outcome of the program (if successful) will be technology that transitions to operational partners with the appropriate legal authorities to use them.

Q16: Clarify relationship of "target" network owner and "GRAY" network owner.

A16: For the purposes of this effort, there is no meaningful difference.

Q15: Does the scope of grey networks include critical infrastructure (electrical grid, manufacturing)?

A15: Yes. The identification of critical infrastructure is of interest; whether and how to act in these networks or computing devices is determined by the rules of operation that would be specified by the operators of the system .

Q14: How will the 5% of IP with 80% accuracy be validated? (Phase 1 evaluation)

A14: Strong proposals will have a thorough and convincing evaluation plan. DARPA will pursue validation using complimentary data sources.

Q13: What kind of data we can expect to have from DARPA?

A13: The proposer should discuss the type(s) and amount of data required to support their technical approach.

Q12: Can we build vulnerabilities related to any device (IoT, Android)?

A12: Generation of n-day exploits based on known vulnerabilities is in scope for any type Internet-connected device.

Q11: What is the budget for the program?

A11: Budget information will not be disclosed.

Q10: Are FFRDC's eligible?

A10: Yes. But please note that FFRDCs are subject to applicable direct competition limitations and cannot propose to this BAA in any capacity unless they meet the following conditions: (1) FFRDCs must clearly demonstrate that the proposed work is not otherwise available from the private sector. (2) FFRDCs must provide a letter on official letterhead from their sponsoring organization citing the specific authority establishing their eligibility to propose to Government solicitations and compete with industry, and their compliance with the associated FFRDC sponsor agreement's terms and conditions. This information is required for FFRDCs proposing to be awardees or subawardees.

Q9: For TA2, if an agent obtains access, can or should it remain persistent to mitigate future bots?

A9: Persistence may be part of the rules of operation. However, any persistence is expected to be of limited time duration.

Q8: TA2: Is it fine looking for zero–days or just restricted to n-days?

A8: Just n-days.

Q7: Who controls intellectual property?

A7: DARPA desires, at a minimum, Government Purpose Rights (GPR) for any technology developed under this program.

Q6: Are you open to a large scale virtualized environment to support enabling parameterized experiment runs as part of the TA4 framework?

A6: DARPA does not seek to fund the creation of such an environment; however, if one already exists, its use may be viewed as a strength of the proposal.

Q5: Will the 'botnet' environments be static or dynamic – that is, will the botnet spread during an experimental run?

A5: The botnet environment will be dynamic; the botnet will spread during an experimental run.

Q4: Are you seeking robust measures of effectiveness integrated as part of the TA4 framework against the stated metrics?

A4: Yes.

Q3: Are any impacts to infected networks allowed? (e.g., cutting off access of non-botnet comms; e.g., denying access to DNS)

A3: It is preferred that side effects be minimized. Understanding and quantifying any unavoidable side effects is required when minimization is impossible.

Q2: Is precision of agents an important metric? Or are "kitchen sink" approaches to neutralization in scope?

A2: Yes, precision of agent effects is an important aspect of safety and reliability.

Q1: Do we care how "stealthy" the agents are when they are deployed? Is this incorporated into "correctness of agent implementation"? Or into the rules of operation?

A1: Stealth of the agents is not a concern of the program.