# Cyber Platforms and Systems, Tools Virtual Event

## Submission Deadline: 13 July 2020

Defensive Cyber Operations (DCO) is seeking solutions for commercial technologies to foster technological innovation relevant to the Focus Areas enclosed in this Announcement. In this context, innovative means any new technology, process, or business practice, or any new application of an existing technology, process, or business practice that that enhances mission effectiveness for DCO.

This Announcement is considered a competitive process and includes multiple phases for selection. Potential prototype projects will be directly relevant to enhancing the effectiveness of the Army Cyber Mission Forces. This Announcement may result in the award of prototype project(s) as a result of this multi-phased competitive process.

**PLEASE NOTE: DCO currently does not have funding for any of the Focus Areas. Until funding is received only Phase I will be accomplished under this Announcement.**

## CPS TOOLS FOCUS AREAS

DCO seeks industry innovation for solutions, technologies, and/or capabilities to meet multiple Focus Areas (FA) identified.

FA:

1. **Security Orchestration and Automated Response**
2. **Threat Deception**
3. **Forensic Analysis**

Please See Appendix 001 for a detailed list of FA being targeted under this Announcement.

## TIMELINE

### Phase I –White Paper & Functional Test– Due 13 July 2020 NLT 12:00 PM EST

- **White Paper:** Vendors may submit multiple white papers for an individual FA or multiple FA but must submit separate white papers per solution proposed.

Submissions will be reviewed independently against evaluation criteria listed in Appendix 004. See Appendix 002 for White Paper instructions.

- **MANDATORY Functional Test:** Vendors will demonstrate that their solutions will operate on DCO's current standard baseline operating system of Red Hat Enterprise Linux 7 (RHEL7) for the identified FA. The purpose of the functional test is to ensure that the proposed application works in DCO's deployed environment. The Functional Test is **MANDATORY** to verify the application can operate on DCO's platforms. See Appendix 002 for Functional Test Instructions.

**Questions Due – 22 June 2020 NLT 12:00 PM EST:** Interested companies may submit questions regarding specific FAs, preparation of the White Papers, and/or Functional Testing. Responses to questions will be provided through the Vulcan Platform (See below).

> **Note:** All questions should be submitted via Vulcan and the answers will be posted on Vulcan NLT 29 June 2020 4:00 PM EST. All questions regarding the preparation of White Papers should be submitted to the SOSSEC managers (see below).

**Downselect – 3 August 2020:** Companies with favorably evaluated White Papers will receive an invitation for advancement to Phase II. PM DCO may proceed directly to Phase III after a successful Phase I evaluation.

**Phase II – Virtual Interviews –TBD:** The purpose of this phase is to discover, learn and understand more about the proposed solution(s). Phase II invitees will have a standard amount of time to pitch or demonstrate its proposed solution(s) to stakeholders and hold discussions necessary for assessment. Favorably evaluated solutions will advance to Phase III.

**Note**: Phase II is optional, and may not always be conducted, or may not be required for every successful Phase I submission. The Government aims to complete Phase II evaluations and respondent notification within 30 calendar days of the assessment and/or receipt of additional requested information. All favorably evaluated respondents at Phase I will receive Phase II notification, however, only favorably evaluated solutions will enter Phase III. **PM DCO currently does not have funding for any of the Focus Areas. Until funding is received only Phase I will be accomplished under this Announcement. Phase II and III will not occur without funding.**

**Phase III – Price & Project Information– TBD:** the Government intends to request price information from those Companies being favorably considered for a prototype

project award. Companies will collaboratively build project requirements for their specific solutions with the Government team and negotiate agreement terms and conditions for award, to include pricing structure (contract type). The Government reserves the right to correspond with respondents individually to collect price information and answer pricing related questions. Such exchanges may result in multiple price submissions to address Government questions.

**Phase IV – Final Down-Select– TBD:** Awards under this Announcement will be Other Transaction Agreements[1] under 10 U.S.C. 2371b for Prototypes Projects with potential follow-on non-competitive Production Agreements or FAR-based contracts. Multiple awards may be made to pursue dissimilar solutions should they all meet the technical criteria and funds are available.

> Note 1: All potential respondents should be aware that due to unanticipated budget fluctuations, funding in any or all areas may change with little or no notice, impacting the number of prototype award(s).
>
> Note 2: The Government reserves the right to select all, part, or none of the solutions briefs received.

## HOW CAN YOU PARTICIPATE?

1. Review the Focus Areas in Appendix 001.
2. Review the instructions for submitting White Papers & the Functional Test in Appendix 002.
3. Review the Guidelines for Submissions, Interviews, and Proposals in Appendix 003.
4. Review the Basis of Evaluation in Appendix 004.
5. Submit a White Paper & Functional Test results on the Vulcan Technology Platform at https://vulcan-sof.com/login/ng2/collection/e6b86f3b-3442-4655-bb59-749dfcc878dd.

## QUESTIONS

[1] Other Transaction Agreement (OTA): Legally binding instruments not subject to the requirements of the Federal Acquisition Regulation (FAR) obligating the Government for a purpose IAW 10 USC 2371 and 2371b.

Questions regarding this Announcement should be sent to the SOSSEC managers:

- Ed Aguirre at eaguirre@sossecinc.com
- Eugene Del Coco at edelcoco@sossecinc.com

## DISCLAIMERS

### Follow-On Production

The potential for follow-on production for projects awarded from this announcement will be in accordance with 10.U.S.C. 2371b(f). Upon a determination that the competitively awarded prototype project(s) has been successfully completed, and subject to the availability of funds, the prototype project(s) may result in the award of a follow-on production contract or transaction without the use of competitive procedures.

### Use of Contractor Support

Non-Government advisors may be used in the evaluation of White Papers and proposals and will have signed Non-Disclosure Agreements (NDAs) with the Government. The Government understands that information provided in this Announcement is presented in confidence and may contain trade secret or commercial or financial information and agrees to protect such information from unauthorized disclosure to the maximum extent permitted and as required by law. A respondent's participation in any part of the selection process under this announcement indicates concurrence with the aforementioned use of contractor support personnel.

- Octo Consulting Group
- Northtide Group
- ASI Government Inc. (subcontractor to Northtide Group)
- Steelgate LLC (subcontractor to Perspecta)
- ORock Technologies

## APPENDIX 001- FOCUS AREAS

- **Focus Area 1**
  - **Title:** Security Orchestration and Automated Response (SOAR)
  - **Description:** A solution to enable an automated response to cyber intrusions at the local / NEC, regional (RCC), and Theater level.
  - **Challenges:** Multi-tenancy / data owners, lack of central tools and platforms, no single access to all networks.
  - **Operational Use Scenario:** Upon detection of an incident, the capability should be capable of some or all of the following: incident management, incident response, data enrichment from threat intelligence, and integrate with both DCO and DODIN capabilities.
  - **General Conditions:** Support multi-tenancy (ability for multiple organizations to use and only see their data) and role-based access controls. Live and operate in Army Cyber Command BDP.
  - **Standard/Desired Outcomes:** Configurable and modifiable solution to enable automated response to Cyber Space activities.

**White Paper Requirements**

Interested companies for this focus area shall address the following questions in white paper submissions:

- Describe your SOAR solution. Please detail any distinguishing features, characteristics, or constraints of the solution as it relates to this FA.
- Describe how your solution integrates with security operations.
- Describe your experience in providing SOAR to DoD, Civilian Government Agencies, or the commercial enterprise users.

- **Focus Area 2**
  - **Title:** Threat Deception
  - **Description:** The Threat Deception capability provides Cyber Defenders the ability to capitalize on deception techniques and actions supporting DCO Internal Defense Mission (DCO-IDM). The capability supports hunt and response actions while reducing time from event to response to pace adversaries.
    - Ability to conduct Threat Deception operations in response to advanced persistent threat (APT) within the defended network enclave. Implement a solution to deny, disrupt and degrade AT presence within the defended network perimeter through obfuscation and deception.
  - **Challenges:** Globally integrate operations to address trans-regional, all domain, and multi-functional challenges.
  - **Operational Use Scenario:**
    - deploy with expeditionary forces as well as providing geographically dispersed DCO reach into all friendly contested cyberspace during all operational phases

        - although primarily software, should be able to implement as physical hardware as operationally required
        - afford Cyber Defenders flexibility and creativity to establish operational “playbooks”
    - **General Conditions:**
        - Support military operations at select Bases/Post/Camps/Stations, tactical sites, or other mission partner environments.
        - Entered and be managed in the NIPRNET/SIPRNET and other mission networks
    - **Standard/Desired Outcomes:**
        - Deceive (deny, degrade, disrupt)
        - Impact Adversary (reduce adversary operational effectiveness)
        - Mission Management (automate, augment decision making processes and actions)
        - Support Situational Understanding (integrate and support awareness and understanding)
        - Ease of Use (integrate and support awareness and understanding)
        - Operate at Echelon (effective at network scale)
        - Support multiple operations (efficiently execute multiple concurrent operations)
        - Detection (overwatch devices and triggers)
        - Investigation (automate confidence levels)
        - Support Response Action (enhance containment eradication, increase network security posture)

**White Paper Requirements**

Interested companies for this focus area shall address the following questions in white paper submissions:

- Describe your Threat Deception solution. Please detail any distinguishing features, characteristics, or constraints of the solution as it relates to this FA.
- Describe how your solution will support hunt and response actions while reducing time from event to response to pace adversaries.
- Describe your experience in providing threat deception tools to DoD, Civilian Government Agencies, or the commercial enterprise users.

❖ **Focus Area 3**

- **Title:** Forensic Analysis
- **Description:** Conduct detailed forensics examination of images to identify hostile/malicious code, possible entry points/attack vectors, and pertinent information. Analyze anomalous/malicious software from Army intrusions to produce whitepapers for distribution within DoD. Conduct reverse-engineering of suspicious code in order to support forensics and/or malware analysis.

- Forensic analysis involves the examination of artifacts created by suspicious or malicious activity on a computer system. This can include information that is relatively easy to identify, such as Internet histories, or more obscure data points such as the recovery of deleted data. Malware analysis is segregated further into static and dynamic analysis. Dynamic analysis is the process of executing malware in a controlled environment and analyzing its effects on the system. This includes monitoring the memory space used by the malware to discern operating capabilities, and observance of malware interaction with the file system. Network connections are also monitored to identify any network traffic generated during execution. Most malware analysis cases involve a combination of both dynamic and static analysis. Dynamic analysis is used to produce a general understanding of how malware operates, and static analysis is then used to reinforce and expound upon the observations made during dynamic analysis. Static analysis is conducted by disassembling the executable file into its most basic assembly programming.
- **Challenges:** Constant evolution of media makes the forensic imaging occasionally difficult requiring new adapters with write blocking capabilities. Encrypted media presents its own challenge, because without the proper key the ability to analyze an image is impossible. This analysis requires a reverse engineer to trace each of the programs functions, and identify the data being moved among memory registers. Static analysis can be used to divide how a command and control node might communicate with a piece of malware, and provides the greatest level of understanding regarding functionality. It is also, however, the most time and labor intensive and some malware have built-in anti-forensics mechanisms that make dynamic analysis impossible.
- **Operational Use Scenario:** The capability needs to enable global, regional, and local cyberspace defenders the ability to conduct efficient and forensically sound data collection and examination. The capability must also function either remotely or locally and integrate with a sandbox-like, virtual environment that allows for real-time analysis and automated dynamic malware analysis for initial quick response reporting.
- **General Conditions:** Globally support the Department of the Army.
- **Standard/Desired Outcomes:**
    - Deceive (deny, degrade, disrupt)
    - Impact Adversary (reduce adversary operational effectiveness)
    - Mission Management (Support decision making processes and actions)
    - Support Situational Understanding (integrate and support awareness and understanding)
    - Ease of Use (integrate and support awareness and understanding)
    - Operate at Echelon (effective at network scale)
    - Support multiple operations (efficiently execute multiple concurrent operations)

- Detection (Supply pertinent information to strengthen Defensive Cyber Operations)
- Investigation (quick and concise)
- Support Response Action (enhance DCO by increasing network security posture)

**White Paper Requirements**

Interested companies for this focus area shall address the following questions in white paper submissions:

- Describe your Forensic Analysis solution. Please detail any distinguishing features, characteristics, or constraints of the solution as it relates to this FA.
- Describe how your solution integrates with incident response.
- Describe your experience in providing Forensic Analysis solutions to DoD, Civilian Government Agencies, or the commercial enterprise users.

## APPENDIX 002 – WHITE PAPER & FUNCTIONAL TEST INSTRUCTIONS (PHASE I)

### White Paper

1. Format

    a. Executive Summary: A brief description of your organization and core competencies.

    b. White Paper Requirements: Describe the unique aspects of your solution and/or technology as it relates to the FA by answering the questions listed in Appendix 001 for the respective FA.

    c. Value Proposition Summary: It is the Company's responsibility to demonstrate why it is offering the best solution and what value-add this solution will bring to PM DCO. This is the respondent's chance to convince the Government as to why it should invest in a prototype. Respondents are reminded this is not a sales pitch and should stay on message to demonstrating why the proposed solution will address the FA.

2. Should be written in clear, concise, layman style statements.

3. Limited to THREE PAGES MAXIMUM. (Cover Page not included)

    - Font size should be no smaller than 12 pt.

4. Cover Page: Vendors must provide the following background information with their white paper submissions.

    - Name of Company
    - Company Address
    - Company POC (name, email, phone)
    - Company URL
    - Where is your organization based? (US Based Company/Internationally Based Company)
    - Does your Company identify as: Large/Small Business or not a commercial endeavor
    - Does your Company identify as: traditional or non-traditional[2] contractor

[2] Non-traditional Defense contractor (NDC): An entity that is not currently performing and has not performed, for at least the one-year period preceding the solicitation of sources by DoD for the procurement or transaction, any contract or subcontract for the DoD that is subject to full coverage under the cost accounting standards prescribed pursuant to section 1502 of title 41 and the regulations implementing such section (see 10 U.S.C. 2302(9)).

- What Focus Area does your White Paper Address?
- SOSSEC Member (yes/no)

5. All White Papers uploaded to Vulcan must adhere to the following naming convention.

**CO-20-0007_Company Name_Focus Area_Solution Title**

**Functional Test**

1. Please read the Registration & Quick Start guide at https://docs.druid.orocktech.com/

2. Send an email to **Russell Houck, russell.l.houck.ctr@mail.mil** to register in DCO's centralized continuous integration pipeline, which is the DCO Resource for Updates Innovation and Development Updating (DRUID).

3. Functional testing in DRUID includes vendor developed unit testing and an automated compliance scan. After completion of either activity, please provide the results with your white paper submission.

## APPENDIX 003 – GUIDELINES FOR WHITE PAPERS, INTERVIEWS, AND PROPOSALS

1) 10 USC 2371b requires competitive procedures be used to the maximum extent practical. This Announcement serves as a competitive opportunity for interested parties to present solutions and be evaluated for selection of a prototype project and is considered to satisfy the reasonable effort to obtain competition in accordance with 10 USC 2371b (b)(2).

2) The Government will not reimburse interested respondents for costs of preparing and submitting white papers, pricing information, or any other activity during the competitive selection process.

3) Unnecessarily elaborate brochures or marketing materials are not desired.

4) Use of a diagram(s) or figure(s) to depict the essence of the proposed solution is strongly encouraged.

5) Multiple white papers addressing different FAs may be submitted by the same organization; however, each solution brief may only address one solution based on the stated FA.

6) All information in white papers must be unclassified **and non-proprietary.** Submission of a white paper under this Announcement indicates confirmation that the submission provided is unclassified and does not contain proprietary information.

7) The period of performance for any white paper or proposal submitted under this Announcement should generally be no greater than 24 months.

8) White Papers may be considered by the Government for a prototype award up to one (1) year after submission for same or similar requirements.

9) The Government will be using the Vulcan Technology Platform to collect, receive, share, and assess white papers. Vendors interested in responding to this announcement will need to register to obtain access to Vulcan at the following website: www.Vulcan-SOF.com.

10) Only SOSSEC members in good standing are eligible for awards under this Announcement. All non-SOSSEC members who submit under this announcement must become SOSSEC members prior to award. Project award(s) as a result of this Announcement will be in the form of Project Agreement (PA) between SOSSEC, Inc. and the selected SOSSEC Consortium Member (referred to as the Project Agreement Holder (PAH)) that incorporates the terms of any teaming agreement

with the OT Lead, SOSSEC, Inc. (including flow-down articles from the OTA, [may be provided at respondents request]). OTA Articles to be included in any Project Award document (PA) between SOSSEC, Inc. and the selected SOSSEC Consortium member are not subject to revision/modification or deletion.

# APPENDIX 004 – BASIS FOR EVALUATION

The Government will be assessing the following during each Phase of the selection process. The Government may use some or all of the identified criteria in any phase of selection process.

## A. Phase I - White Papers & Functional Test

The Government will use the below criteria when evaluating solution briefs:

- Interoperability with DCO environment
- Innovation
- Tools that successfully complete the Functional test will be highly considered for Phase II

Please be advised white papers that do not address FA questions in Appendix 001 will not be favorably considered for Phase II

## B. Phase II – Virtual Interviews

Virtual Interviews should provide more details on the technical feasibility of the proposed solution. Interviews will be assessed on against the following criteria:

- Operational Impact to the end user
- Data Rights and Intellectual Property Assertions
- Infrastructure Impacts and Performance Characteristics
- Tools that successfully complete the Functional test will be highly considered for Phase III

## C. Phase III – Price Information

The primary purpose of this Phase is to collect information in order to make a final down-select decision in Phase IV. Requests for pricing will include preparation instructions for Prototype Proposals. During this Phase, invited companies will collaboratively develop prototype project requirements with the Government teams for their specific projects and negotiate Terms and Conditions into their Agreements.

## D. Phase IV – Final Down-Select

Prototype project awards will be determined using the following criteria:

- Price Reasonableness
- Schedule

- Data Rights/Intellectual Property
- Innovation
- Availability of Funding