SOURCES SOUGHT ANNOUNCEMENT

The Defense Information Systems Agency (DISA) is seeking sources for the development and sustainment of the next generation platform supporting SharkSeer.

CONTRACTING OFFICE ADDRESS:
DISA/Defense Information Technology Contracting Organization (DITCO)/PL8331
2300 East Drive, Bldg. 3600
Scott Air Force Base, IL 62225-5406

INTRODUCTION:

This is a SOURCES SOUGHT TECHNICAL DESCRIPTION to determine the availability and technical capability of large and small businesses (including the following subsets: Small Disadvantaged Businesses, HUBZone firms, Certified 8(a), Service-Disabled Veteran-Owned Small Businesses and Woman Owned Small Business) to provide the required products and/or services for the SharkSeer program.

SharkSeer is currently a program funded and maintained by the National Security Agency (NSA) whose objective is to identify and mitigate Advanced Persistent Threats (APTs) and Zero Day malware resident of Department of Defense (DoD) Information Network (DoDIN) Internet Access Points (IAPs) in near-real time with commercial technology, utilizing auto orchestration. DISA has been tasked by the United States (U.S.) Congress to migrate the program from NSA to its enterprise, and to support development, engineering, sustainment efforts for SharkSeer henceforth.

DISA's Perimeter Defense division (ID51) is seeking information from potential sources to provide the engineering and sustainment services necessary to migrate the NSA SharkSeer program to DISA, and to develop and sustain the next generation of SharkSeer (2.0). The DISA version will build on the success of the SharkSeer component of the Cyber Network Defense (CND) Tools program to make it more efficient, condensed, and simplified than the original release, and significantly improve the mechanisms for zero-day network defense (ZND), information sharing, and collaboration of cyber threat intelligence data within the DoD.

Contractors shall follow a Security Development and Operations model in conjunction with agile framework methodologies to ensure that best practices for secure development are a part of the overall development and integration processes. The environment shall be designed to provide ease-of-use for the engineers, administrators, and analysts. Contractor employees assigned to SharkSeer shall demonstrate expertise in such functionalities as:

- Security Incident Event Management (SIEM) products (including Splunk)
- Commercial off-the-shelf (COTS) and Government off-the-self (GOTS) Security Orchestration Automation and Response (SOAR)
- Cross Domain Solutions (CDS, including CloudShield/NetDefender)
- Systems administration (including Linux and Windows)
- Virtualization technologies (including VMWare and NetApp)
- Malware analytics (including FireEye and McAfee)
- Networking (including Juniper and Cisco routing, switching, and firewalls)
- Automation and orchestration (including Ansible and Salt)
- Custom programming/scripting (including Java and Python)
- Load-balancing technologies
- Service Now integration
- Cloud technologies
- Understanding of engineering and systems integration in general. (The awardee's employees are required to become familiar with and conversant in engineering and systems integration within DISA within sixty [60] days of contract award.)

Information Assurance (IA) and cybersecurity expectations include expertise in DISA Security Technical Implementation Guides (STIGs), DISA Information Assurance Vulnerability Alerts (IAVA) processes, Nessus scanning, security architecture, cybersecurity engineering, and DISA Risk Management Framework (RMF) standards.

DISCLAIMER:

THIS SOURCES SOUGHT IS FOR INFORMATIONAL PURPOSES ONLY. THIS IS NOT A REQUEST FOR PROPOSAL. IT DOES NOT CONSTITUTE A SOLICITATION AND SHALL NOT BE CONSTRUED AS A COMMITMENT BY THE GOVERNMENT. RESPONSES IN ANY FORM ARE NOT OFFERS AND THE GOVERNMENT IS UNDER NO OBLIGATION TO AWARD A CONTRACT AS A RESULT OF THIS ANNOUNCEMENT. NO FUNDS ARE AVAILABLE TO PAY FOR PREPARATION OF RESPONSES TO THIS ANNOUNCEMENT. ANY INFORMATION SUBMITTED BY RESPONDENTS TO THIS TECHNICAL DESCRIPTION IS STRICTLY VOLUNTARY.

CONTRACTS/PROGRAM BACKGROUND:

The current NSA suite of SharkSeer contracts (a total of seven) ends on December 31, 2019, but NSA will issue follow-on contracts for SharkSeer Operations and Maintenance (O&M) support in January 2020, and hold those contracts in place until all seven SharkSeer functional boundaries have been migrated successfully from NSA to DISA. DISA will gradually assume responsibility for each of these boundaries as soon as the SharkSeer 2.0 contract is fully staffed, and will continue to do so through the completion of that process, projected for FY21.

Incumbent Information	Award Type	CAGE/Bus Size
Contract Number: H98230-12-D-0126 Program: Vulnerability Analysis Operations (VAO) II Task Order Number: Task Order 9 Contract Type: Cost Plus Fixed Fee Incumbent: **Parsons Corporation**	Competitive award	9R677 L
Contract Number: H98230-15-C-0564 Program: BIGGERBOAT Task Order Number: Task Order 22 Contract Type: Firm Fixed Price Incumbent: **LookingGlass Cyber Solution, Inc.**	Non-competitive award	4MHX9 L
Contract Number: H98230-13-C-1123 Program: Enterprise Information Technology Operations (EITO) Delivery and Task Order Numbers: DO105/TTO 1&2 Contract Type: CPAE/LOE Incumbent: **ITSM Alliance**	Competitive award	6KEJ9 S
Contract Number: H98230-15-D-0004 (EPM) Program: Enterprise Program Management (EPM) Task Order Number: DO105/TTO 1&2 Contract Type: Firm Fixed Price Incumbent: **CACI**	Competitive award	3JFA6 L
Contract Number: H98230-15-C-0127 Program: FireEye Task Order Number: DO105/TTO 1&2 Contract Type: LOE Incumbent: **FireEye**	Competitive award	5QHL3 L
Contract Number: H98230-14-C-1169 Program: McAfee Task Order Number: DO105/TTO 1&2 Contract Type: LOE Incumbent: **McAfee, LLC**	Non-competitive award	9Y089 L
Contract Number: H98230-14-C-1169 (SPLUNK) Program: Splunk Task Order Number: DO105/TTO 1&2 Contract Type: LOE Incumbent: **ClearShark, LLC**	Competitive award	1VH01 L (541519)

This is a new acquisition, the objective of which is to migrate, consolidate, and update the current NSA version of SharkSeer to reduce vulnerabilities, and to develop a more efficient, condensed, and simplified cybersecurity tool, in compliance with both the John S. McCain National Defense Authorization Act for Fiscal Year 2019 and direction from the DoD as to this realignment.

ANTICIPATED PERIOD OF PERFORMANCE: SharkSeer 2.0 will consist of a base period of 12-months, and four 12-month option periods.

ANTICIPATED PLACE OF PERFORMANCE: Fort George G. Meade, Maryland

REQUIRED CAPABILITIES

Interested contractors shall submit their capabilities to perform each of the areas outlined below.

1. Optimize existing SIEM and Security Orchestration Automation and Response (SOAR) solutions to simplify and increase the efficiency DoD ZND capabilities, while maintaining a forward-thinking focus to establish the next generation of SharkSeer.
    a. Describe your experience in implementing, maintaining, and consolidating SIEM and SOAR solutions (including Splunk as well as other COTS and GOTS based technologies) to provide auto-tasking capabilities.
    b. Describe the complexity and size of Splunk environments you have deployed and maintained, including the number of Splunk systems, amount of storage, and number of alerts generated.
2. Develop and sustain malware analytic and ZND solutions for the prevention of malicious activity originating in compromised DoD) networks.
    a. Describe your experience and expertise in McAfee Advanced Threat Defense (ATD), McAfee Network Security Platform (NSP), FireEye Network Security Services (NX, VX, and CMS), sandbox capabilities, and any other perimeter defense capabilities in which your firm and the employees you would dedicate to this program may have been involved.
3. Develop and deliver defensive cyberspace operations information-sharing and collaboration-specific capabilities to enable near real-time response actions, with a clear path to real-time event data collection, aggregation, analysis, normalization, monitoring, and storage, as well as automated reporting of security incidents, utilizing COTS, GOTS, and cloud-based platforms.
    a. Describe your experience in providing critical architectural and platform development to support these activities.
    b. Describe your experience interfacing with other agencies and departments to provide information sharing and collaboration capabilities.
4. Design, deploy, and sustain COTS and GOTS cross-domain solutions (CDS) within the DoD.
    a. Describe your experience and expertise in Lookingglass CDS technologies including Cloudshield-4000, Cloudshield-4000E, Scoutshield, and Netdefender.

    b. Describe your experience in other COTS and GOTS based CDS technologies.

5. Provide Information Technology (IT) engineering and systems integration support including software engineering (in Python and Java), systems engineering and administration (including Linux and Windows), and network engineering (including Juniper routing and switching, Cisco firewalls, and load balancing technologies).
    a. Describe your experience and expertise in engineering, deploying and maintaining multivendor environments involving each domain of IT including software engineering, systems engineering, and network engineering.
    b. Describe the size and complexity of the networks and systems your company and the personnel who will be dedicated to this task order as full-time equivalent have deployed and managed as well as the size of the communities you have serviced.

6. Improve the overall security posture of the SharkSeer program.
    a. Describe your experience and expertise in implementing DISA STIGs and DISA IAVA processes, performing Nessus scanning, optimizing and maintaining security architecture, cybersecurity engineering, and adhering to DISA RMF standards.

SPECIAL REQUIREMENTS

All contractor personnel shall be U.S. citizens and possess at least a full SECRET security clearance upon commencement of work; however, access to classified data/information up to and including TOP SECRET with SCI may be required. Contractor facilities shall be cleared to the level of SECRET at time of request for proposals. Please provide your security clearance level with your response.

Minimum required certification standards include the 8570 requirements, under section “DoD 8570.01-M Requirements”. All contractors shall meet Information Assurance Technical (IAT) Level II certification by holding and maintaining Security+ Continuing Education (CE).

IAT Level III certification is required for two Information Assurance and Cybersecurity roles and all Subject Matter Expert (SME) Roles. IAT Level III certifications can include Certified Information Systems Security Professional or CompTIA Advanced Security Practitioner CE.

Further specialized vendor certifications and/or experience are required for SME roles including such expertise as the following: (Please note that skill in automation and orchestration technologies including Ansible or salt technology is mandatory for all SMEs.)

- A SME in McAfee technologies will be required to have at minimum six (6) years of relevant experience in malware analytics and ZND technologies including the McAfee products ATD and NSP.
- SME in FireEye technologies will be required to have at minimum six (6) years of relevant experience in malware analytics and ZND technologies including FireEye products NX, VX, and CMS.
- A SME in BRO, YARA, and SURICATA rules will be required to support, maintain, and deploy each of these systems.
- A SME in Splunk will be required to hold and maintain Splunk Enterprise Certified Architect certification as well as have at minimum three years of experience in engineering Splunk solutions. The SME may also hold and maintain Splunk Enterprise Certified Admin certification as well as have at minimum five (5) years of experience in engineering Splunk solutions.
- A SME in engineering solutions for Linux will be required to hold and maintain Red Hat Certified Engineer certification as well as have at minimum eight (8) years of relevant experience.
- A SME in engineering infrastructure solutions for Windows will be required to hold and maintain Microsoft Certified Solutions Expert Core Infrastructure: IT Pro & Developer certification. The Microsoft SME shall also have at minimum eight (8) years of relevant experience.
- SMEs in VMware and virtualization technologies will be required to hold and maintain one of three VMware Design Expert Certifications, including Data Center Virtualization, Network Virtualization, and Desktop and Mobility. Additionally, the virtualization SME shall have at minimum five (5) years of relevant experience. VMware Professional Certifications may be substituted for any of the three expert level certifications in the same tracks, if the virtualization SME has an additional three (3) years of relevant experience. If the virtualization SME has a certification in only one track, the SME is required to understand technologies in the other tracks. The virtualization SME shall have experience deploying and maintaining vSphere, NSX, and Horizon. The virtualization SME also shall understand how to deploy and maintain NetApp.
- SMEs in software engineering will be required to have at minimum a bachelor’s degree in Computer Science, Computer Engineering, or Software Engineering as well as eight (8) years of relevant experience programming in Python and Java. Preferably, the SME may also have a master’s degree in Computer Science, Computer Engineering, or Software Engineering with five (5) years of relevant experience programming in Python and Java.
- SMEs in software engineering shall have in-depth experience with Linux operating systems. The SME shall also be capable of learning other programming languages as necessary.
- SMEs in developing solutions to shall include auto tasking SIEM products utilizing SOAR solutions.

- SMEs in Cisco firewall and network security technologies shall hold and maintain CCIE Security certification as well as have at minimum four (4) years of relevant experience. CCNP Security certification may be substituted for vendor certification requirements if the SME has an additional four years of relevant network engineering experience in Cisco firewall and network security technologies. The SME in Cisco firewall and network security technologies shall also be capable of designing and managing network security infrastructure involving other vendor firewall and network security solutions.
- SMEs in Juniper routing and switching technologies shall hold and maintain Juniper Networks Certified Expert Enterprise Routing and Switching (JNCIE-ENT) or JNCIE-SP certification as well as have at minimum four (4) years of relevant experience in engineering solutions for enterprise networks. JNCIP-ENT or JNCIP-SP may be substituted for certification requirements if the SME has an additional four (4) years of relevant network engineering experience in Juniper technologies.

Additionally, the SME in Juniper routing and switching technologies shall also have relevant experience in load balancing technologies to include software programs as Juniper, Gigamon, and F5. SMEs in Windows, Linux, virtualization, and Splunk are required to cross-train to understand how to deploy and maintain each technology.

SMEs in Cisco firewall technologies and Juniper routing and switching technologies are required to cross-train, to understand how to deploy, and to maintain each technology. SMEs in McAfee and FireEye ZNE are required to cross-train, to understand how to deploy, and to maintain each technology.

SOURCES SOUGHT:

The anticipated North American Industry Classification System Code (NAICS) for this requirement is 541519, with the corresponding size standard of $30.0M.

To assist DISA in making a determination regarding the level of participation by small business in any subsequent procurement that may result from this Sources Sought, you are also encouraged to provide information regarding your plans to use joint venturing (JV) or partnering to meet each of the requirement areas contained herein. This includes responses from qualified and capable Small Businesses, Small Disadvantaged Businesses, Historically Under-utilized Business Zones, Service Disabled-Veteran Owned Small Businesses, Women-owned Small Businesses, and 8(a) companies. Provide information as to how you envision combining your company's areas of expertise with those of any proposed JV/partner to meet the specific requirements contained in this announcement.

In order to make a determination for a small business set-aside, two or more qualified and capable small businesses must submit responses that demonstrate their qualifications.

Responses shall demonstrate the company's ability to perform in accordance with the Limitations on Subcontracting clause (Federal Acquisition Regulation 52.219-14).

SUBMISSION DETAILS:

Responses must include:

1) Business name and address;
2) Name of company representative and their business title;
3) Type of Small Business;
4) Cage Code;

Contract vehicles that would be available to the Government for the procurement of the product and service, including DISA's SETI and ENCORE III; the General Service Administration (GSA)'s Professional Services Schedule, GSA IT Schedule-70, VETS-2 small business, and Alliant-2 small business; the National Institutes of Health Chief Information Officer-Solutions and Partner 3 (NIH CIO-SP3) small business; NASA Solutions for Enterprise-Wide Procurement (SEWP); Federal Supply Schedules (FSS); or any other relevant Government Agency contract vehicle. (This information is for market research only and does not preclude your company from responding to this notice.)

Contractors who wish to respond to this should send responses via email NLT October 4, 2019 by 4:00 PM Eastern Standard Time (EST) to disa.meade.bd.mbx.bdl2@mail.mil and nicole.a.thomas17.civ@mail.mil. Interested businesses should submit a brief capabilities statement package (no more than five pages) demonstrating ability to perform the services listed in the Required Capabilities section.

Proprietary information and trade secrets, if any, shall be clearly marked on all materials. All information received that is marked Proprietary will be handled accordingly. Please be advised that all submissions become Government property and will not be returned. All government and contractor personal reviewing sources sought responses will have a signed non-disclosure agreement and understand their responsibility for proper use and protection from unauthorized disclosure of proprietary information as described 41 USC 423. The Government shall not be held liable for any damages incurred if proprietary information is not properly identified.