Highly Adaptive Cybersecurity Services Webinar

8/24/2016

Speakers

Giovanni Onwuchekwa
Branch Chief, Programs and Analysis
IT Schedule 70

Jill Thomas
Division Director, IT Schedule 70 Contract Operations
IT Schedule 70

Julius White
Program Lead, Information Assurance and Security Branch
Security Services Division

Background

- In support of Cybersecurity National Action Plan (CNAP) and Cybersecurity Implementation Plan (CSIP)
- Establish a contract solution for specific cybersecurity services.
- Two Request For Information (RFI) published.
- Held two industry days in Washington D.C. and San Francisco, CA.

Highly Adaptive Cybersecurity Services (HACS)

- 132-45A: Penetration Testing
- 132-45B: Incident Response
- 132-45C: Cyber Hunt
- 132-45D: Risk and Vulnerability Assessment (RVA)

Evaluation Process

SIN #	Services	Primary Evaluation Methodology
132- 45A	Incident Response	• Oral vendor interview - Incident response scenario. • Project Experience
132- 45B	Penetration Testing	• Oral vendor interview - Attack network scenario. • Project Experience
132- 45C	Cyber Hunt	• Oral vendor interview - Cyber hunt scenario. • Project Experience
132- 45D	Risk and Vulnerability Assessment (RVA)	• Oral vendor interview on RVA capabilities and processes. • Project Experience

Oral Technical Evaluation Procedure

- Identify up to five key personnel to attend.
- Evaluation consists of SIN-specific scenarios & questions.
- Expect to spend no more than 40 minutes per SIN.
- Total evaluation session may take up to three (3) hours, depending on the number of SINs.
- Offerors may attend virtually.
- Recording devices are not allowed.

Scenario-based Oral Technical Evaluation

SIN 132-45A Penetration Test Minimum Knowledge Areas	SIN 132-45B Incident Response Minimum Knowledge Areas	SIN 132-45C Cyber Hunt Minimum Knowledge Areas	SIN 132-45D Risk and Vulnerability Assessment Minimum Knowledge Areas
● Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit, etc.) ● Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.) ● Ability to identify systemic security issues based on the analysis of vulnerability and configuration data	●Knowledge of incident categories, incident responses, and timelines for responses ● Knowledge of incident response and handling methodologies ● Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies	● Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored]) ● Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.) ● Knowledge of incident categories, incident responses, and timelines for responses	● Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP) and Internet Protocol (IP), Open System Interconnection Model (OSI), Information Technology Infrastructure Library, v3 (ITIL)) ● Knowledge of system and application security threats and vulnerabilities ● Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services

Scenario-based Oral Technical Evaluation

SIN 132-45A Penetration Test Evaluation Overview	SIN 132-45B Incident Response Evaluation Overview	SIN 132-45C Cyber Hunt Evaluation Overview	SIN 132-45D Risk and Vulnerability Assessment Evaluation Overview
a. What processes and methods are used to conduct reconnaissance activities? b. What specific tools, techniques, and procedures (TTPs) do you utilize to discover and enumerate vulnerabilities for potential exploitation? c. What are some specific tools, techniques, and procedures (TTPs) used to exploit identified vulnerabilities? d. After gaining access to systems and/or data, describe TTPs used for "pivoting" in order to establish a new source of attack on the newly compromised target?	a. What are the specific processes and methods used to conduct preparation activities? b. What are the specific tools and procedures used by the vendor to detect and analyze potential incidents? c. What are some specific techniques and procedures used to contain and remediate incidents? d. What post-incident support processes or procedures would be put in place?	a. What are the specific processes and methods used for hypothesis generation/creation? b. What are the specific tools, techniques, and procedures (TTPs) used by the vendor to test hypotheses? c. What are some specific techniques and procedures used to identify malicious patterns of behavior? d. Describe how the Analytic Automation processes or procedures will be put in place.	a. What is your process for conducting RVA testing activities? b. How would your team develop an understanding of a company's mission, its operating environment, discover its cybersecurity needs and define a robust RVA plan? c. What is your process for conducting RVA post assessment testing activities?

Oral Technical Evaluation Criteria

TECHNICAL RATINGS	
Rating	**Definition**
Acceptable	The proposal clearly meets the minimum requirements of the solicitation.
Unacceptable	The proposal does not clearly meet the minimum requirements of the solicitation.

- Offerors who do not pass the evaluation will be ineligible to re-submit proposals for 6 months.

Project Experience

- Submit narrative for 3 projects within the scope of each SIN proposed.
- Not to exceed to 4 pages per project.
  - Detailed description work performed and results
  - Methodology, tools, and/or processes utilized
  - Demonstration of compliance with any applicable laws, regs, standards, etc.
  - Demonstration of required specific experience and/or special qualifications detailed under the proposed SIN.

Next Steps

- SIN will be established on September 1, 2016
- There will be no limit on the number of awardees
- Dedicated tiger team to support offers/modifications
- All other updates will be on GSA Interact - IT Schedule 70 Group

Questions?

Key References

- **GSA Interact**
  - **Schedule 70 Group - https://interact.gsa.gov/group/it-schedule-70**
- **New vendors**
  - **GSA S70 Road Map - http://www.gsa.gov/portal/category/100406**
- **Existing S70 contract holders**
  - **eMod process - http://eoffer.gsa.gov/eoffer_docs/eMod_process.htm**