Factor 5 Oral Technical Evaluation Criteria

Addendum to SCP-FSS-004 SPECIFIC PROPOSAL INSTRUCTIONS FOR SCHEDULE 70

132- 45A Penetration Testing

Expected tasks within the scope of this SIN include but are not limited to:

- Conducting and/or supporting authorized penetration testing on enterprise network assets
- Analyzing site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives
- Assisting with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes)

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

132- 45B Incident Response

Expected tasks within the scope of this SIN include but are not limited to:

- Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
- Perform command and control functions in response to incidents
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation

Minimum Knowledge Areas:

- 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

132- 45C Cyber Hunt

Expected tasks within the scope of this SIN include but are not limited to:

- Collecting intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise

- Coordinating with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
- Correlating incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation

Minimum Knowledge Areas:

- 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

132- 45D Risk and Vulnerability Assessments (RVA)

Expected tasks within the scope of this SIN include but are not limited to the following.

- Network Mapping - consists of identifying assets on an agreed upon IP address space or network range(s).
- Vulnerability Scanning - comprehensively identifies IT vulnerabilities associated with agency systems that are potentially exploitable by attackers.
- Phishing Assessment - includes activities to evaluate the level of awareness of the agency workforce with regard to digital form of social engineering that uses authentic looking, but bogus, emails request information from users or direct them to a fake Website that requests information. Phishing assessments can include scanning, testing, or both and can be conducted as a one- time event or as part of a larger campaign to be conducted over several months.
- Wireless Assessment - includes wireless access point (WAP) detection, penetration testing or both and is performed while onsite at a customer's facility.
- Web Application Assessment - includes scanning, testing or both of outward facing web applications for defects in Web service implementation may lead to exploitable vulnerabilities. Provide report on how to implement Web services securely and that traditional network security tools and techniques are used to limit access to the Web Service to only those networks and systems that should have legitimate access.
- Operating System Security Assessment (OSSA) - assesses the configuration of select host operating systems (OS) against standardized configuration baselines.
- Database Assessment - assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities.

Minimum Knowledge Areas:

- 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
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)
- 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 network access, identity and access management (e.g., public key infrastructure, PKI)
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth)
- Knowledge of IA principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- Skill in assessing the robustness of security systems and designs
- Skill in the use of social engineering techniques
- Skill in applying host/network access controls (e.g., access control list)
- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
- Skill in using network analysis tools to identify vulnerabilities
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data
- Conducting required reviews as appropriate within environment (e.g., Technical Surveillance Countermeasure Reviews (TSCM), TEMPEST countermeasure reviews)
- Perform technical (evaluation of technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (i.e., local computing environment, network and infrastructure, enclave boundary, and supporting infrastructure)
- Maintaining knowledge of applicable Computer Network Defense policies, regulations, and compliance documents specifically related to Computer Network Defense auditing

Oral Technical Evaluation Procedure

Pre-scenario Questions:

1. **Services Provided**
    - **a.** Which cybersecurity services do you offer?
2. **Logistics**
    - **a.** How quickly can you deploy resources for an engagement (Pentest/IR/Hunt/RVA)?
    - **b.** What is your average team makeup for each type of engagement?
    - **c.** Do you have resources to deploy nation-wide?

After addressing the aforementioned questions, the offeror will be evaluated on their knowledge of the proposed services. The oral technical evaluation will require the offeror to respond to a specific scenario

and general questions to assess the offeror's expertise. The questions and evaluation topics for each SIN are as follows:

1. **SIN 132-45 A - Penetration Test Evaluation Overview -** the following questions and topics will be discussed during the Penetration Test SIN evaluation.
    - **a.** What activities do you carry out during the Pre-Engagement, Testing/Assessment, and Post-Engagement phases?
    - **b.** Provide us with a background of your organization's Penetration Testing capabilities.
    - **c.** What processes and methods are used to conduct reconnaissance activities?
    - **d.** What specific tools, techniques, and procedures (TTPs) do you utilize to discover and enumerate vulnerabilities for potential exploitation?
    - **e.** What are some specific tools, techniques, and procedures (TTPs) used to exploit identified vulnerabilities?
    - **f.** 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?
2. **SIN 132-45 B - Incident Response Evaluation Overview -** the following questions and topics will be discussed during the Incident Response SIN evaluation.
    - **a.** What activities do you carry out during the Pre-Deployment phase, Incident Identification, Intrusion Detection, and Analysis phase, and the Post-Incident phase?
    - **b.** Provide us with a background of your organization's Incident Response Service capabilities:
    - **c.** What malware analysis and reverse engineering capabilities do you have?
    - **d.** What are the specific processes and methods used to conduct preparation activities?
    - **e.** What are the specific tools and procedures used by the vendor to detect and analyze potential incidents?
    - **f.** What are some specific techniques and procedures used to contain and remediate incidents?
    - **g.** What post-incident support processes or procedures would be put in place?
3. **SIN 132-45 C - Cyber Hunt Evaluation Overview -** the following questions and topics will be discussed during the Cyber Hunt SIN evaluation.

    - **a.** What activities do you carry out during the various phases of your Cyber Hunt missions?
    - **b.** Provide us with a background of your organization's Cyber Hunt Service capabilities.
    - **c.** What are the specific processes and methods used for hypothesis generation/creation?
    - **d.** What are the specific tools, techniques, and procedures (TTPs) used by the vendor to test hypotheses?
    - **e.** What are some specific techniques and procedures used to identify malicious patterns of behavior?
    - **f.** Describe how the Analytic Automation processes or procedures will be put in place.

4. **SIN 132-45 D - Risk and Vulnerability Assessment Evaluation Overview -** the following questions and topics will be discussed during the Penetration Test SIN evaluation.

a. What activities do you carry out during the Pre-Engagement, Testing/Assessment, and Post-Engagement phases?
b. Provide us with a background of your organization's Risk and Vulnerability Assessment capabilities.
c. Describe the scope and general level of effort (LOE) for each type of service provided.
d. What is your process for conducting RVA testing activities?
e. Describe the tools utilized during the testing/assessment phase.
f. What is your process for conducting RVA post assessment testing activities?

Oral Technical Evaluation Criteria

The offeror's responses to the government's questions during the oral technical evaluation session shall be used to determine whether the Offeror has the requisite experience and expertise to perform tasks expected to be performed within the scope of these SINs. Each oral technical proposal will be evaluated and rated on an acceptable/unacceptable basis. The rating definitions provided below will be used for the evaluation of the offeror's responses to questions during the oral evaluation.

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