CHAPTER 11. SPECIAL ITEM NUMBERS 54151HACS

Terms And Conditions Applicable To Highly Adaptive Cybersecurity Services (Hacs) (Special Item Numbers 54151HACS

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- **Federal Acquisition Regulation (FAR) Part 52.204-21**
- **OMB Memorandum M-06-19** - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- **OMB Memorandum M -07-16** - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- **OMB Memorandum M-16-03** - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- **OMB Memorandum M-16-04** – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- **The Cybersecurity National Action Plan (CNAP)**
- **NIST SP 800-14** - Generally Accepted Principles and Practices for Securing Information Technology Systems
- **NIST SP 800-27A** - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- **NIST SP 800-30** - Guide for Conducting Risk Assessments
- **NIST SP 800-35** - Guide to Information Technology Security Services
- **NIST SP 800-37** - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- **NIST SP 800-39** - Managing Information Security Risk: Organization, Mission, and Information System View
- **NIST SP 800-44** - Guidelines on Securing Public Web Servers
- **NIST SP 800-48** - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- **NIST SP 800-53** – Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-61** - Computer Security Incident Handling Guide
- **NIST SP 800-64** - Security Considerations in the System Development Life Cycle

- **NIST SP 800-82** - Guide to Industrial Control Systems (ICS) Security
- **NIST SP 800-86** - Guide to Integrating Forensic Techniques into Incident Response
- **NIST SP 800-115** - Technical Guide to Information Security Testing and Assessment
- **NIST SP 800-128** - Guide for Security-Focused Configuration Management of Information Systems
- **NIST SP 800-137** - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- **NIST SP 800-153** - Guidelines for Securing Wireless Local Area Networks (WLANs)
- **NIST SP 800-171** - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

******NOTE: All non-professional labor categories must be incidental to, and used solely to support Highly Adaptive Cybersecurity Services, and cannot be purchased separately.**

******NOTE: All labor categories under the Special Item Number 54151S**

Information Technology Professional Services may remain under SIN 54151S unless the labor categories are specific to the Highly Adaptive Cybersecurity Services SINs.

1. SCOPE

a. The labor categories, prices, terms and conditions stated under this Offering apply exclusively to High Adaptive Cybersecurity Services within the scope of this MAS Information Technology Schedule.

b. Services under these SINs are limited to Cybersecurity Services only. Software and hardware products may be ordered under different Special Item Numbers under this Schedule and may be quoted in addition to Services to provide a total solution.

c. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.

d. Highly Adaptive Cybersecurity Services provided under these SINs comply with Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

e. IBM shall provide services at the Contractor's facility and/or at the ordering activity location, as mutually agreed to by IBM and Client.

TERMS AND CONDITIONS

IBM's CyberSecurity Services are governed by the terms of the Client Relationship Agreement for Services (CRA for Services) and any Attachment or Statement of Work provided at the transaction level. In the event of conflict, the Attachment or Statement or Work prevails over the terms of the CRA.

DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES

Highly Adaptive Cybersecurity Services (HACS) consist of Proactive, Reactive, and Remediation Services. These services include Penetration Testing, Incident Response, Cyber Hunt, and Risk and Vulnerability Assessments (RVA).

IBM's Offerings Include:

Penetration Testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

Tasks 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)

Knowledge Areas include but are not limited to:

- 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.

Incident Response services help organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.

Tasks 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.

Knowledge Areas include but are not limited to:

- 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

Cyber Hunt activities are responses to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunt activities start with the premise that threat actors known to target some organizations in a specific industry, or specific systems, are likely to also target other organizations in the same industry or with the same systems. Use information and threat intelligence specifically focused on the proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities.

Tasks 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

Knowledge Areas include but are not limited to:

- 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.

Risk and Vulnerability Assessments (RVA) conduct assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. RVA services include but are not limited to: Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA),and Database Assessment.

Tasks include but are not limited to:

- 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.

Knowledge Areas include but are not limited to:

- 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