CHAPTER 11. SPECIAL ITEM NUMBERS 132-45A, 132-45B, 132-45C AND 132-45D

Terms And Conditions Applicable To Highly Adaptive Cybersecurity Services (Hacs) (Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45D)

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 132-51 Information Technology Professional Services may remain under SIN 132-51 unless the labor categories are specific to the Highly Adaptive Cybersecurity Services SINs.**

TERMS AND CONDITIONS

Note: These terms are in addition to those described in Chapter 1, General Information.

During the contract period, International Business Machines Corporation (IBM) and the Government agree that the following terms and conditions will apply to any order for IBM IT Professional Services that is placed by the Government under this Special Item. The term "Government" shall mean all Federal agencies (as defined in Paragraph (b) of 40 USC 472) the Senate, the House of Representatives, the Architect of the Capitol, and the Government of the District of Columbia, all of which are hereinafter referred to as the Government. The materials and services under this Special Item will be available to the Government within the United States, the District of Columbia and Puerto Rico. Such sales will be made to the Government within the United States, the District of Columbia and Puerto Rico. On a case-by-case basis IBM will deliver products and perform Services to overseas U.S. Government locations which are in support of national defense operations (including U.S. Embassies), and to locations which support the national interest of the United States.

DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES

IT 70 Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SIN) Descriptions

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).

132- 45A 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.

132- 45B 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

132- 45C 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.

132- 45D 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

1. SCOPE

a. The labor categories, prices, terms and conditions stated under Special Item Numbers 132-45A, 132- 45B, 132-45C and 132-45D High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.

b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on IT Schedule 70 (e.g. 132-32, 132- 33, 132-8), and may be quoted along with 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 shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

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

2. ORDER

a. Agencies may use written orders, Electronic Data Interchange (EDI) orders, Blanket Purchase Agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.

b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

3. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.

b. The Contractor agrees to render services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner. Since the IBM services performed under this contract are commercial item services, they will be performed in accordance with IBM's standard warranty provision and acceptance criteria.

d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will

apply to all Contractor travel. Contractors cannot use GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor's travel.

4. INSPECTION OF SERVICES

Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS –COMMERCIAL ITEMS (MAY 2015) (ALTERNATE II – JUL 2009) (FAR DEVIATION – JUL 2015) (TAILORED) for Firm-Fixed Price and Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

Since the IBM services performed under this contract are commercial item services, they will be performed in accordance with IBM's standard warranty provision and acceptance criteria.

5. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (MAY 2014) Rights in Data – General, may apply.

The Contractor shall comply with contract clause (52.204-21) to the Federal Acquisition Regulation (FAR) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to the ordering activity's security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.

7. INDEPENDENT CONTRACTOR

All Highly Adaptive Cybersecurity Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

8. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

"Contractor" means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

"Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

9. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for Highly Adaptive Cybersecurity Services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

10. RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

11. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting

Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

ADDITIONAL TERMS FOR IBM SERVICES

STATEMENT OF WORK

A separate Statement of Work will be signed by both IBM and the Government for services provided other than hourly assist services. Upon acceptance by IBM, IBM agrees to provide the Services described in the Statement of Work.

The Statement of Work includes, for example:

A. IBM's responsibilities

B. The Government's responsibilities

C. The specific conditions (Completion Criteria), if any, that IBM is required to meet to fulfill its obligations

D. A performance period for Services and an estimated schedule for planning purposes, and

E. Applicable charges (not including taxes) and any other terms.

F. Resumes shall be provided by IBM upon request.

If a Statement of Work contains an estimated schedule, both IBM and the Government agree to make reasonable efforts to carry out our respective responsibilities according to that Schedule. If the Statement of Work contains Completion Criteria, IBM will inform the Government when each criteria is met. The Government then has 10 days to inform IBM if the Government

believes that IBM has not met the criteria. The project is complete when IBM meets the Completion Criteria.

Changes to Statements of Work

When both IBM and the Government agree to change a Statement of Work, IBM will prepare a written description of the agreed change which must be signed by both IBM and the Government. Any change in the Statement of Work may affect the charges, estimated schedule, or other terms. Depending on the extent and complexity of the requested changes, additional charges may be required for analysis of the changes. Additional work will not commence until funded authorization is received from the Government.

REQUIRED CONSENTS

The Government is responsible for promptly obtaining and providing to IBM all Required Consents necessary for IBM to provide the Services described in a Statement of Work. A Required Consent means any consents or approvals required to give IBM or our subcontractors the right or license to access, use and/or modify (including creating derivative works) the hardware, software, firmware and other products, to enable IBM and our subcontractors to perform the Services set forth in the Statement of Work without infringing the ownership or license rights (including patent and copyright) of the providers or owners of such product. IBM will be relieved of the performance of any obligations that may be affected by your failure to promptly provide any Required Consents to IBM.

CONTROL AND SUPERVISION

IBM and the Government is each responsible for the supervision, direction, control, and compensation of their respective personnel.

The tasks on which assigned personnel assist shall remain the responsibility of the Government. Therefore, IBM does not guarantee that the Government's task will be accomplished under this contract, only that assistance shall be provided. No estimate made by IBM of the assistance to be provided to the Government is guaranteed to any extent or in any way.

PERSONNEL

Each party will assign personnel that are qualified to perform the tasks required of such party under this Agreement and is responsible for the supervision, direction, control, and compensation of its personnel. Subject to the foregoing, each party may determine the assignment of its personnel and its contractors.

IBM may engage subcontractors to provide or assist in providing Services, in which case IBM remains responsible for the fulfillment of its obligations under this Agreement and for the performance of the Services.

Government Resources

If Government is making available to IBM any facilities, software, hardware or other resources in connection with IBM’s performance of Services, Government agrees to obtain any licenses or approvals related to these resources that may be necessary for IBM to perform the Services and develop project Materials. IBM will be relieved of its obligations that are adversely affected by Government’s failure to promptly obtain such licenses or approvals. Government agrees to reimburse IBM for any reasonable costs and other amounts that IBM may incur from Customer’s failure to obtain these licenses or approvals.

Unless otherwise agreed in an Attachment or Transaction Document, Government is responsible for i) any data and the content of any database Government makes available to IBM in connection with a Service under this Agreement, ii) the selection and implementation of procedures and controls regarding access, security, encryption, use, and transmission of data, and iii) backup and recovery of the database and any stored data. IBM's responsibilities regarding such data or databases, including any confidentiality and security obligations, are governed by the Attachments and Transaction Documents applicable to the particular Services transaction.

MATERIALS OWNERSHIP AND LICENSE

An Attachment or Transaction Document will specify Materials to be delivered to the Government and identify them as "Type I Materials," "Type II Materials," or otherwise as both parties agree. If not specified, Materials will be considered Type II Materials.

The Government will own the copyright in Materials created as part of a Service that are identified as "Type I Materials" and each such Material will constitute a "work made for hire" to the extent permissible under U.S. copyright law. If any such Materials are not works made for hire under applicable law, IBM assigns the ownership of copyrights in such Materials to the Government. The Government grants IBM an irrevocable, nonexclusive, worldwide, paid-up license to use, execute, reproduce, display, perform, sublicense, distribute, and prepare derivative works based on, Type I Materials.

IBM or its suppliers will own the copyright in Materials created as part of a Services transaction that are identified as Type II Materials. IBM grants the Government an irrevocable, nonexclusive, worldwide, paid-up license to use, execute, reproduce, display, perform, and distribute (for the specific Government Contract, unless otherwise agreed to by IBM) copies of Type II Materials.

IBM or its suppliers retains ownership of the copyright in any of IBM's or its suppliers' works that pre-exist or were developed outside of the Government Agreement and any modifications or enhancements of such works that may be made under the Government's Agreement. To the extent they are embedded in any Materials, such works are licensed in accordance with their separate licenses provided to the Government, if any, or otherwise as Type II Materials.

Each party agrees to reproduce the copyright notice and any other legend of ownership on any copies made under the licenses granted in this section.

ACCEPTANCE

A. For items having Completion Criteria (in the statement of work), when IBM meets the Completion Criteria.

B. For hourly service, upon completion of the service hours.

WARRANTY FOR IBM SERVICES

IBM warrants that it performs each IBM Service using reasonable care and skill and according to its current description (including any completion criteria) contained in this Agreement, Attachment, or a Transaction Document. Government agrees to provide timely written notice of any failure to comply with this warranty so that IBM can take corrective action.

EXTENT OF WARRANTY/ITEMS NOT COVERED BY WARRANTY

If a Machine is subject to federal or state consumer warranty laws, IBM's statement of limited warranty included with the Machine applies is place of these Machine warranties.

The warranties stated herein will not apply to the extent there has been misuse, accident, modification, unsuitable physical or operating environment, operation in other than the Specified Operating Environment, improper maintenance by the Government, or failure caused by a product for which IBM is not responsible. With respect to Machines, the warranty is voided by removal or alteration of Machine or parts identification labels.

THESE WARRANTIES ARE YOUR EXCLUSIVE WARRANTIES AND REPLACE ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

IBM does not warrant uninterrupted or error-free operation of a Product or Service or warrant that all defects will be corrected.

Unless IBM specifies otherwise, it provides Materials, non-IBM Products, and non-IBM Services WITHOUT WARRANTIES OF ANY KIND. However non-IBM manufacturers, developers, suppliers, or publishers may provide their own warranties to you. Warranties, if any, for Other IBM Programs (IBM Programs licensed under a separate IBM license agreement, e.g., IBM International Program Licensing Agreement) and Non-IBM Programs (Programs licensed under a separate third party License agreement) may be found in their license agreements.

European Union General Data Protection Regulation (GDPR)

The European Union passed the General Data Protection Regulation (EU/2016/679) (GDPR), effective 25 May 2018. The GDPR is designed to ensure a consistent level of protection of the rights and freedoms of natural persons with regard to the processing of their data and to establish one set of data protection rules for Personal Data. IBM is committed to GDPR readiness.

Regarding GDPR, you represent as follows:

a. Either you do not require IBM to process Personal Data within the meaning of GDPR (e.g., because no processing of Personal Data occurs in the European Union (EU); no monitoring of Personal behavior takes place in EU; or your activities are otherwise exempt from GDPR); and you will communicate to IBM in writing, without undue delay, any anticipated change affecting this representation, or

b. You agree to IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and applicable DPA Exhibit, which apply and supplement the contract. Please contact your IBM representative for the applicable Data Processing Exhibit.