Mississippi State University RFP 16-89
Comprehensive Cybersecurity Assessment Services

Build. Protect. Learn.

Authorized Federal Supply Service (FSS)
Information Technology Category
IT Services / Highly Adaptive Cybersecurity Services (HACS) - Pricelist

General Services Administration (GSA)
Federal Acquisition Service (FAS)
Multiple Award Schedule (MAS)

Contract Number: GS-35F-248GA
Schedule: MAS Refresh 9
MAS Mod: PS-A839
Supplement No. 1 – dated December 23, 2021
Contract Period: February 17, 2022 – February 16, 2027
Special Item Number: 54151HACS
Business Size: Small

BreakPoint Labs
8116 Arlington Boulevard, #255, Falls Church, VA 22042
1-844-HACKME2 (422-5632) ♦ www.breakpoint-labs.com ♦ contracts@breakpoint-labs.com
# Table of Contents

**CUSTOMER INFORMATION** .................................................................................................................. 5

1. **SCHEDULE TITLE** .......................................................................................................................... 5
2. **CONTACT INFORMATION** ......................................................................................................... 5
3. **1A. SPECIAL ITEM NUMBERS (SINS):** ......................................................................................... 5
4. **1B LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN:** ...................................... 5
5. **NOT APPLICABLE** .......................................................................................................................... 5
6. **1.C SERVICES OFFERED:** ............................................................................................................... 5
7. **SEE PRICE LIST** ............................................................................................................................ 5
8. **2. MINIMUM ORDER** ..................................................................................................................... 5
9. **3. MAXIMUM ORDER** ..................................................................................................................... 5
10. **4. GEOGRAPHIC SCOPE OF CONTRACT (DELIVERY AREA) ......................................................... 5
11. **GOVERNMENT PURCHASE CARDS** ........................................................................................... 5
12. **LIABILITY FOR INJURY OF DAMAGE** ............................................................................................ 5
13. **STATISTICAL DATA FOR GOVERNMENT ORDERING OFFICE COMPLETION OF SF-279** .......... 6
14. **5. POINT(s) OF PRODUCTION:** ................................................................................................... 6
15. **NOT APPLICABLE** .......................................................................................................................... 6
16. **6. DISCOUNT FROM LIST PRICES OR STATEMENT OF NET PRICE:** .......................................... 6
17. **7. QUANTITY DISCOUNTS:** .......................................................................................................... 6
18. **NOT APPLICABLE** .......................................................................................................................... 6
19. **8. PROMPT PAYMENT TERMS:** .................................................................................................... 6
20. **NOT APPLICABLE** .......................................................................................................................... 6
21. **9. FOREIGN ITEMS:** ...................................................................................................................... 6
22. **NOT APPLICABLE** .......................................................................................................................... 6
23. **10A. TIME OF DELIVERY:** ............................................................................................................ 6
24. **10B. EXPEDITED DELIVERY:** ...................................................................................................... 6
25. **10C. OVERNIGHT AND 2 DAY DELIVERY:** .................................................................................. 6
26. **10D. URGENT REQUIREMENTS:** ................................................................................................ 6
27. **11. F.O.B POINT(s):** .................................................................................................................... 7
28. **12A. ORDERING ADDRESS(es):** .................................................................................................. 7
29. **12B. ORDERING PROCEDURES:** ................................................................................................. 7
30. **FEDERAL INFORMATION TECHNOLOGY / TELECOMMUNICATIONS STANDARDS REQUIREMENTS** 7
31. **FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS PUBS)** .......... 7
32. **FEDERAL TELECOMMUNICATION STANDARDS (FED-STDs)** .................................................. 8
33. **CONTRACTOR TASKS / SPECIAL REQUIREMENTS (C-FSS-370) (NOV 2003)** ....................... 8
34. **CONTRACT ADMINISTRATION FOR ORDERING ACTIVITIES** .................................................... 9
35. **GSA ADVANTAGE™** ................................................................................................................... 9
36. **PURCHASE OF OPEN MARKET ITEMS** ..................................................................................... 9
37. **BLANKET PURCHASE AGREEMENTS (BPAs)** ............................................................................ 10
38. **CONTRACTOR TEAM ARRANGEMENTS** .................................................................................... 10
39. **INSTALLATION, DEINSTALLATION, REINSTALLATION** ................................................................. 10
40. **PRIME CONTRACTOR ORDERING FROM FEDERAL SUPPLY SCHEDULES** ........................... 10
41. **INSURANCE – WORK ON A GOVERNMENT INSTALLATION (JAN 1997)(FAR 52.228-5)** ............ 11
42. **SOFTWARE INTEROPERABILITY** ............................................................................................... 11
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRICING</td>
<td>28</td>
</tr>
<tr>
<td>BREAKPOINT LABS, LLC. COMMITMENT TO PROMOTE</td>
<td>29</td>
</tr>
<tr>
<td>SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS</td>
<td>29</td>
</tr>
<tr>
<td>BEST VALUE BLANKET PURCHASE AGREEMENT</td>
<td>30</td>
</tr>
<tr>
<td>FEDERAL SUPPLY MULTIPLE AWARD SCHEDULE</td>
<td>30</td>
</tr>
<tr>
<td>(CUSTOMER NAME)</td>
<td>31</td>
</tr>
<tr>
<td>BLANKET PURCHASE AGREEMENT</td>
<td>31</td>
</tr>
</tbody>
</table>
Customer Information

Schedule Title
General Services Administration (GSA) Information Technology (IT) Multiple Award Schedule
Highly Adaptive Cybersecurity Services (HACS)

Contact Information
BreakPoint Labs, LLC.
8116 Arlington Boulevard, #255
Falls Church, VA 22042
Phone: 1-844-422-5632
Fax: 410-505-9229
Website: https://breakpoint-labs.com
Email: contracts@breakpoint-labs.com

1a. SPECIAL ITEM NUMBERS (SINs):
<table>
<thead>
<tr>
<th>Special Item Numbers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special Item Number: 54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
</tbody>
</table>

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN:
Not Applicable

1c. SERVICES OFFERED:
See Price List

2. Minimum Order
The maximum dollar of orders to be issued is $500,000.

3. Maximum Order
The minimum dollar of orders to be issued is $100.00.

4. Geographic Scope of Contract (Delivery Area)
The Geographic Scope of Contract is domestic and overseas delivery

Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

Overseas delivery is delivery to points outside of the 48 contiguous states, Washington, DC, Alaska, Hawaii, Puerto Rico, and U.S. Territories

Government Purchase Cards
Government purchase cards are accepted for orders equal to or less than the micro-purchase threshold for oral or written orders under this contract.
Liability for Injury of Damage
The Contractor shall not be liable for any injury to ordering activity personnel or damage to ordering activity property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

Statistical Data for Government Ordering Office Completion of SF-279
Block 9: G. Order/Modification Under Federal Schedule Contract
Block 16: Data Universal Numbering System (DUNS) Number: 079914189
Block 30: Type of Contractor: B. Other Small Business
Block 31: Woman-Owned Small Business: No
Block 37: Contractor's Taxpayer Identification Number (TIN): 47-4581296
Block 40: Veteran Owned Small Business (VOSB): No

5. Point(s) of Production:
Not Applicable

6. Discount from list prices or statement of net price:

<table>
<thead>
<tr>
<th>SIN 54151HACS</th>
<th>Prices shown are NET prices; basic discounts have been deducted.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dollar Volume: 1% for any order greater than $500,000</td>
</tr>
<tr>
<td></td>
<td>Government Education Institutions: Not applicable</td>
</tr>
<tr>
<td></td>
<td>Other: Not applicable</td>
</tr>
</tbody>
</table>

7. Quantity Discounts:
Not applicable

8. Prompt Payment Terms:
Not applicable

9. Foreign Items:
Not Applicable

10a. Time of Delivery:

| SIN 54151HACS | As negotiated between ordering activity and BreakPoint Labs, LLC. |

10b. Expedited Delivery:
Contact Contractor

10c. Overnight and 2 Day Delivery:
Contact Contractor

10d. Urgent Requirements:
When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to
contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

11. F.O.B point(s):

| SIN 54151HACS | Destination |

12a. Ordering Address(es):
BreakPoint Labs, LLC.
8116 Arlington Boulevard, #255
Falls Church, VA 22042
Phone: 1-844-422-5632
Fax: 410-505-9229
Website: https://breakpoint-labs.com
Email: contracts@breakpoint-labs.com

12b. Ordering Procedures:
Ordering activities shall use the ordering procedures of Federal Acquisition Regulation (FAR) 8.405 when placing an order or establishing a BPA for supplies or services. These procedures apply to all schedules.

a. FAR 8.405-1 Ordering procedures for supplies, and services not requiring a statement of work.

b. FAR 8.405-2 Ordering procedures for services requiring a statement of work.

Federal Information Technology / Telecommunications Standards Requirements
Ordering activities acquiring products from this Schedule must comply with the provisions of the Federal Standards Program, as appropriate (reference: NIST Federal Standards Index). Inquiries to determine whether or not specific products listed herein comply with Federal Information Processing Standards (FIPS) or Federal Telecommunication Standards (FED-STDS), which are cited by ordering activities, shall be responded to promptly by the Contractor.

Federal Information Processing Standards Publications (FIPS PUBS)
Information Technology products under this Schedule that do not conform to Federal Information Processing Standards (FIPS) should not be acquired unless a waiver has been granted in accordance with the applicable "FIPS Publication." Federal Information Processing Standards Publications (FIPS PUBS) are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Information concerning their availability and applicability should be obtained from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22161. FIPS PUBS include voluntary standards when these are adopted for Federal use. Individual orders for FIPS PUBS should be referred to the NTIS Sales
Office, and orders for subscription service should be referred to the NTIS Subscription Officer, both at the above address, or telephone number (703) 487-4650.

Federal Telecommunication Standards (FED-STDS)
Telecommunication products under this Schedule that do not conform to Federal Telecommunication Standards (FED-STDS) should not be acquired unless a waiver has been granted in accordance with the applicable "FED-STD." Federal Telecommunication Standards are issued by the U.S. Department of Commerce, NIST, pursuant to National Security Act. Ordering information and information concerning the availability of FED-STDS should be obtained from the GSA, Federal Acquisition Service, Specification Section, 470 East L’Enfant Plaza, Suite 8100, SW, Washington, DC 20407, telephone number (202) 619-8925. Please include a self-addressed mailing label when requesting information by mail. Information concerning their applicability can be obtained by writing or calling the U.S. Department of Commerce, NIST, Gaithersburg, MD 20899, telephone number (301) 975-2833.

Contractor Tasks / Special Requirements (C-FSS-370) (NOV 2003)

a. Security Clearances: The Contractor may be required to obtain/possess varying levels of security clearances in the performance of orders issued under this contract. All costs associated with obtaining/possessing such security clearances should be factored into the price offered under the Multiple Award Schedule.

b. Travel: The Contractor may be required to travel in performance of orders issued under this contract. Allowable travel and per diem charges are governed by Pub.L. 99-234 and FAR Part 31, and are reimbursable by the ordering agency or can be priced as a fixed price item on orders placed under the Multiple Award Schedule. Travel in performance of a task order will only be reimbursable to the extent authorized by the ordering agency. The Industrial Funding Fee does NOT apply to travel and per diem charges.

c. Certifications, Licenses and Accreditations: As a commercial practice, the Contractor may be required to obtain/possess any variety of certifications, licenses and accreditations for specific FSC/service code classifications offered. All costs associated with obtaining/possessing such certifications, licenses and accreditations should be factored into the price offered under the Multiple Award Schedule program.

d. Insurance: As a commercial practice, the Contractor may be required to obtain/possess insurance coverage for specific FSC/service code classifications offered. All costs associated with obtaining/possessing such insurance should be factored into the price offered under the Multiple Award Schedule program.

e. Personnel: The Contractor may be required to provide key personnel, resumes or skill category descriptions in the performance of orders issued under this contract. Ordering activities may require agency approval of additions or replacements to key personnel.

f. Organizational Conflicts of Interest: Where there may be an organizational conflict of interest as determined by the ordering agency, the Contractor’s participation in such order may be restricted in accordance with FAR Part 9.5.

g. Documentation/Standards: The Contractor may be requested to provide products or services in accordance with rules, regulations, OMB orders, standards and documentation as specified by the agency’s order.

h. Data/Deliverable Requirements: Any required data/deliverables at the ordering level will be as specified or negotiated in the agency’s order.
i. **Government-Furnished Property:** As specified by the agency’s order, the Government may provide property, equipment, materials or resources as necessary.

j. **Availability of Funds:** Many Government agencies’ operating funds are appropriated for a specific fiscal year. Funds may not be presently available for any orders placed under the contract or any option year. The Government’s obligation on orders placed under this contract is contingent upon the availability of appropriated funds from which payment for ordering purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are available to the ordering Contracting Officer.

k. **Overtime:** For professional services, the labor rates in the Schedule should not vary by virtue of the Contractor having worked overtime. For services applicable to the Service Contract Act (as identified in the Schedule), the labor rates in the Schedule will vary as governed by labor laws (usually assessed a time and a half of the labor rate).

**Contract Administration for Ordering Activities**

Any ordering activity, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212-4, paragraphs (1) Termination for the ordering activity’s convenience, and (m) Termination for Cause (See 52.212-4).

**GSA Advantage!™**

GSA Advantage!™ is an on-line, interactive electronic information and ordering system that provides on-line access to vendors' schedule prices with ordering information, which may be found at [https://www.gsaadvantage.gov](https://www.gsaadvantage.gov).

**Purchase of Open Market Items**

NOTE: Open Market Items are also known as incidental items, noncontract items, non-Schedule items, and items not on a Federal Supply Schedule contract. Ordering Activities procuring open market items must follow FAR 8.402(f).

For administrative convenience, an ordering activity contracting officer may add items not on the Federal Supply Multiple Award Schedule (MAS) -- referred to as open market items -- to a Federal Supply Schedule blanket purchase agreement (BPA) or an individual task or delivery order, only if-

1. All applicable acquisition regulations pertaining to the purchase of the items not on the Federal Supply Schedule have been followed (e.g., publicizing (Part 5), competition requirements (Part 6), acquisition of commercial items (Part 12), contracting methods (Parts 13, 14, and 15), and small business programs (Part 19));
2. The ordering activity contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;
3. The items are clearly labeled on the order as items not on the Federal Supply Schedule; and
4. All clauses applicable to items not on the Federal Supply Schedule are included in the order.
Blanket Purchase Agreements (BPAs)
The use of BPAs under any schedule contract to fill repetitive needs for supplies or services is allowable. BPAs may be established with one or more schedule contractors. The number of BPAs to be established is within the discretion of the ordering activity establishing the BPA and should be based on a strategy that is expected to maximize the effectiveness of the BPA(s). Ordering activities shall follow FAR 8.405-3 when creating and implementing BPA(s).

Contractor Team Arrangements
Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74, Industrial Funding Fee and Sales Reporting, i.e., each contractor (team member) must report sales and remit the IFF for all products and services provided under its individual contract.

Installation, Deinstallation, Reinstallation
The Davis-Bacon Act (40 U.S.C. 276a-276a-7) provides that contracts in excess of $2,000 to which the United States or the District of Columbia is a party for construction, alteration, or repair (including painting and decorating) of public buildings or public works with the United States, shall contain a clause that no laborer or mechanic employed directly upon the site of the work shall receive less than the prevailing wage rates as determined by the Secretary of Labor. The requirements of the Davis-Bacon Act do not apply if the construction work is incidental to the furnishing of supplies, equipment, or services. For example, the requirements do not apply to simple installation or alteration of a public building or public work that is incidental to furnishing supplies or equipment under a supply contract. However, if the construction, alteration or repair is segregable and exceeds $2,000, then the requirements of the Davis-Bacon Act applies.

The ordering activity issuing the task order against this contract will be responsible for proper administration and enforcement of the Federal labor standards covered by the Davis-Bacon Act. The proper Davis-Bacon wage determination will be issued by the ordering activity at the time a request for quotations is made for applicable construction classified installation, deinstallation, and reinstallation services under SIN 132-8 or 132-9.

Prime Contractor Ordering From Federal Supply Schedules
Prime Contractors (on cost reimbursement contracts) placing orders under Federal Supply Schedules, on behalf of an ordering activity, shall follow the terms of the applicable schedule and authorization and include with each order –

a. A copy of the authorization from the ordering activity with whom the contractor has the prime contract (unless a copy was previously furnished to the Federal Supply Schedule contractor); and

b. The following statement:

This order is placed under written authorization from ______ dated ______. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern.
Insurance – Work on a Government Installation (JAN 1997)(FAR 52.228-5)
   a. The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Schedule or elsewhere in the contract.
   b. Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Government's interest shall not be effective—
      (1) For such period as the laws of the State in which this contract is to be performed prescribe; or
      (2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.
   c. The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance, and shall make copies available to the Contracting Officer upon request.

Software Interoperability
Offerors are encouraged to identify within their software items any component interfaces that support open standard interoperability. An item’s interface may be identified as interoperable on the basis of participation in a Government agency-sponsored program or in an independent organization program. Interfaces may be identified by reference to an interface registered in the component registry located at http://www.core.gov.

Advance Payments
A payment under this contract to provide a service or deliver an article for the United States Government may not be more than the value of the service already provided or the article already delivered. Advance or pre-payment is not authorized or allowed under this contract. (31 U.S.C. 3324).

13. Payment Address(es):
BreakPoint Labs, LLC.
8116 Arlington Boulevard, #255
Falls Church, VA 22042
Phone: 1-844-422-5632
Fax: 410-505-9229
Website: https://breakpoint-labs.com
Email: finance@breakpoint-labs.com

14. Warranty Provision:
   a. For the purpose of this contract, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:
      (1) Time of delivery/installation quotations for individual orders;
      (2) Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional
characteristics and capabilities of a product/equipment/service/software package submitted in response to requirements which result in orders under this schedule contract.

(3) Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the Contractor.

b. The above is not intended to encompass items not currently covered by the GSA Schedule contract.

15. Export Packing Charges:
Not Applicable

16. Terms and Conditions of Rental, Maintenance, and Repair:
Not Applicable

17. Terms and Conditions of Installation:
Not Applicable

18a. Terms and Conditions of Repair Parts:
Not Applicable

18b. Terms and Conditions for Any Other Services:

19. List of Service and Distribution Points:
Not Applicable

20. List of Participating Dealers:
Not Applicable

21. Preventive Maintenance:
Not Applicable

22a. Special Attributes:
Not Applicable

22b. Section 508 Compliance:
If applicable, Section 508 compliance information on the supplies and services in this contract are available in Electronic and Information Technology (EIT) at the following: https://breakpoint-labs.com

The EIT standard can be found at: www.Section508.gov.

23. Data Universal Number System (DUNS) number:
079914189
24. Notification Regarding Registration in System for Award Management (SAM) database:
Contractor has registered in the Systems for Award Management.

Commercial and Government Entity (CAGE) Code
7FZP3

Special Notice to Agencies: Small Business Participation
SBA strongly supports the participation of small business concerns in the Federal Acquisition Service. To enhance Small Business Participation SBA policy allows agencies to include in their procurement base and goals, the dollar value of orders expected to be placed against the Federal Supply Schedules, and to report accomplishments against these goals.

For orders exceeding the micropurchase threshold, FAR 8.404 requires agencies to consider the catalogs/pricelists of at least three schedule contractors or consider reasonably available information by using the GSA Advantage!™ on-line shopping service (www.gsaadvantage.gov). The catalogs/pricelists, GSA Advantage!™ and the Federal Acquisition Service Home Page (www.gsa.gov/fas) contain information on a broad array of products and services offered by small business concerns.

This information should be used as a tool to assist ordering activities in meeting or exceeding established small business goals. It should also be used as a tool to assist in including small, small disadvantaged, and women-owned small businesses among those considered when selecting pricelists for a best value determination.

For orders exceeding the micropurchase threshold, customers are to give preference to small business concerns when two or more items at the same delivered price will satisfy their requirement.

Overseas Activities
The terms and conditions of this contract shall apply to all orders for installation, maintenance and repair of equipment in areas listed in the pricelist outside the 48 contiguous states and the District of Columbia, except as indicated below:

None.

Upon request of the Contractor, the ordering activity may provide the Contractor with logistics support, as available, in accordance with all applicable ordering activity regulations. Such ordering activity support will be provided on a reimbursable basis, and will only be provided to the Contractor's technical personnel whose services are exclusively required for the fulfillment of the terms and conditions of this contract.

Central Contractor Registration (CCR) Database
BreakPoint Labs, LLC. has registered with the CCR Database.

Trade Agreements Act of 1979, as Amended
All items are U.S. made end products, designated country end products, Caribbean Basin country end products, Canadian end products, or Mexican end products as defined in the Trade Agreements Act of 1979, as amended.
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-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
- OMB Memorandum M-19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 2017 Report to the President on Federal IT Modernization
- 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 800-44 - 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 800-137 - 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.

Scope
a. The labor categories, prices, terms and conditions stated under Special Item Number 54151HACS High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Multiple Award Schedule.
b. Services under this SIN are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on the IT Multiple Award Schedule (e.g. 33411, 811212, 518210C), 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.

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.

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.
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.
Information Technology (IT) Multiple Award Schedule
Highly Adaptive Cybersecurity Services (HACS)

**Inspection of Services**

**Responsibilities of the Contractor**
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.

**Independent Contractor**

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.

**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.

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

Description of Highly Adaptive Cybersecurity Services and Pricing
a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Number 54151HACS for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.

The following is an example of the manner in which the description of a commercial job title should be presented (see SCP FSS 004)

EXAMPLE

Commercial Job Title: Computer Network Defense Analysis

Description: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Professionals involved in this specialty perform the following tasks:

• Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities
• Provide daily summary reports of network events and activity relevant to Computer Network Defense practices
• Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise.

Knowledge, Skills and Abilities: Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed

Minimum Experience: 5 Years

Minimum Education Requirements: a bachelor's of science degree with a concentration in computer science, cybersecurity services, management information systems (MIS), engineering or information science is essential.
Highly Desirable: Offensive Security Certified Professional (OSCP) or commercial Cybersecurity advanced certification(s).

**Special Item Number 54151HACS – Penetration Testing – Subject to Cooperative Purchasing**

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. Related Job Titles include but are not limited to: Blue Team Technician, Penetration Tester, Red Team Technician, and Ethical Hacker.

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).

**Special Item Number 54151HACS – Incident Response – Subject to Cooperative Purchasing**

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.

Related Job Titles include: but are not limited to: Incident Response Analyst, Computer Crime Investigator, and Intrusion Analyst.

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.

**Special Item Number 54151HACS – Cyber Hunt – Subject to Cooperative Purchasing**

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.

Related Job Titles include but are not limited to: Computer Crime Investigator, Incident Handler, Incident Responder, Incident Response Analyst, Incident Response Coordinator and Intrusion Analyst.

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.

Special Item Number 54151HACS – Risk and Vulnerability Assessments (RVA) – Subject to Cooperative Purchasing
Risk and vulnerability assessments 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. At a minimum offerors who would like to be considered for this SIN must offer the following services: Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), and Database Assessment.

Related Job Titles include but are not limited to: Risk/Vulnerability Analyst, Vulnerability Manager, Ethical Hacker, Computer Network Defense (CND) Auditor, Compliance Manager, and Information Security Engineer.

At a minimum, offerors who would like to be considered for this SIN must offer the following services:
• 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.

Special Item Number 54151HACS – High Value Asset Assessments (HVA) – Subject to Cooperative Purchasing
High Value Asset Assessments – include **Risk and Vulnerability Assessment (RVA)** which assesses 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. **Security Architecture Review (SAR)** evaluates a subset of the agency’s HVA security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how an HVA’s individual security components integrate and operate, including how data is protected during operations. **Systems Security Engineering (SSE)** identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle. SSE focuses on, but is not limited to the following security areas: perimeter security, network security, endpoint security, application security, physical security, and data security.

Related Job Titles include but are not limited to: Risk/Vulnerability Analyst, Vulnerability Manager, Ethical Hacker, Computer Network Defense (CND) Auditor, Compliance Manager, and Information Security Engineer.

At a minimum, the following services are offered:
- **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.
### Labor Category Descriptions

#### Cybersecurity Subject Matter Expert

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>Functional Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Generally recognized as a leader in the industry in their area of expertise; sought out by others in the area of expertise for advice and guidance.</td>
</tr>
<tr>
<td></td>
<td>- Provides expert support, analysis, strategy. Policy, research, and advice into exceptionally complex problems, and processes relating to cybersecurity or other functional area.</td>
</tr>
<tr>
<td></td>
<td>- Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives. Expertise is in Cybersecurity or other functional area.</td>
</tr>
<tr>
<td></td>
<td>- Performs highly specialized and technical tasks associated with the most current and cutting-edge technologies including research and development.</td>
</tr>
<tr>
<td></td>
<td>- May serve as a technical consultant to a project or a number projects dealing with area of cybersecurity or other related technical fields.</td>
</tr>
<tr>
<td></td>
<td>- Coordinates with Customers/Government personnel to ensure the problems have been properly defined and the solutions satisfy customer needs.</td>
</tr>
</tbody>
</table>

#### Minimum Qualifications and Experience

<table>
<thead>
<tr>
<th>Level</th>
<th>Education</th>
<th>Experience (Years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level III</td>
<td>PhD or Equivalent</td>
<td>15+</td>
</tr>
<tr>
<td>Level II</td>
<td>Masters or Equivalent</td>
<td>8-12</td>
</tr>
<tr>
<td>Level I</td>
<td>Bachelors or Equivalent</td>
<td>2-5</td>
</tr>
</tbody>
</table>

#### Cybersecurity Technical Expert

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>Functional Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Performs or reviews technical security assessments of computing environments to identify points of vulnerability, non-compliance with established IA standards and regulations and recommend mitigation strategies.</td>
</tr>
<tr>
<td></td>
<td>- Validates and verifies system security requirements definitions and analyses and establishes system security designs.</td>
</tr>
<tr>
<td></td>
<td>- Designs, develops, implements and/or integrates IA and security systems and system components including those for networking, computing, and enclave environments to include those with multiple enclaves and with differing data protection/classification requirements.</td>
</tr>
<tr>
<td></td>
<td>- Builds cybersecurity into systems deployed to operational environments.</td>
</tr>
<tr>
<td></td>
<td>- Assists architects and systems developers in the identification and implementation of appropriate information security functionality to ensure uniform application security policy and enterprise solutions.</td>
</tr>
<tr>
<td></td>
<td>- Supports the design and implementation of security architectures.</td>
</tr>
</tbody>
</table>
- May provide or support cybersecurity assessments, defensive and offensive cyber operations (DCO), cybersecurity training and research and development (R&D)
- Contributes to the security planning, assessment, risk analysis, risk management, RMF, certification and awareness activities for system and networking operations
- Performs system installation, configuration maintenance, account maintenance, signature maintenance, patch management, and troubleshooting of operational IA and DCO systems
- Applies system security engineering expertise in one or more of the following to: system security design process; engineering life cycle; information domain; cross domain solutions; identification; authentication; and authorization; system integration; risk management; intrusion detection; contingency planning; incident handling; configuration control; change management; auditing; certification and accreditation process; principles of cybersecurity (confidentiality, integrity, non-repudiation, availability, and access control; and security testing)
- Tests, implements, deploys, maintains, and administers the infrastructure systems which are required to effectively manage the cyber, IA, and CND networks and systems (e.g., routers, firewalls, intrusion detection/prevention systems)
- Participates / leads research and development efforts into offensive and defensive cyber operations
- May conduct research and development regarding intrusion detection, threat analysis, or other areas of emerging technology

### Minimum Qualifications and Experience

<table>
<thead>
<tr>
<th>Level</th>
<th>Education</th>
<th>Experience (Years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level III</td>
<td>Masters or Equivalent</td>
<td>15+</td>
</tr>
<tr>
<td>Level II</td>
<td>Bachelors or Equivalent</td>
<td>8-12</td>
</tr>
<tr>
<td>Level I</td>
<td>Bachelors or Equivalent</td>
<td>2-5</td>
</tr>
</tbody>
</table>

### Labor Category

**Cybersecurity Technical Analyst**

- Identifies and manages network and system vulnerabilities and security events
- Receives, acknowledges, disseminates, tracks, reports and updates vulnerability management (VM) alerts, vulnerability assessments, red/blue team events, security incidents and events
- Provides inspection services across the enterprise on behalf of the organization’s manager
- Supports or performs global inspection services to ensure compliance to applicable mandates and/or standards
- 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
- Identifies and reports detected events through persistent monitoring and analysis of I&W and AS&W indicators, dissemination and reporting (daily/weekly) of cyber related activity
- Supports and/or performs inspections of enclave services
- Tests, implements, deploys, maintains, and administers the infrastructure systems which are required to effectively manage the DCO provider network and resources (i.e., routers, firewalls, intrusion detection/prevention systems, and other DCO tools as deployed within customers' enterprise)
- Analyzes requirements, designs and develops software to support cyber functions
- Conducts / participates in risk assessments during the certification and accreditation process
- Provides security certification test and evaluation of assets, vulnerability management and response, security assessments, and customer support

Minimum Qualifications and Experience
Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.

<table>
<thead>
<tr>
<th>Level</th>
<th>Education</th>
<th>Experience (Years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level III</td>
<td>Masters or Equivalent</td>
<td>15+</td>
</tr>
<tr>
<td>Level II</td>
<td>Bachelors or Equivalent</td>
<td>8-12</td>
</tr>
<tr>
<td>Level I</td>
<td>Bachelors or Equivalent</td>
<td>2-5</td>
</tr>
</tbody>
</table>

Labor Category: Incident Responder
Functional Responsibilities
- 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
- Creates and disseminates AS&W to enterprise and DCO community
- Conducts cyber incident trend analysis and malware analysis
- Tests, implements, deploys, maintains, and administers the infrastructure systems which are required to effectively manage the DCO provider network and resources (i.e., routers, firewalls, intrusion detection/prevention systems, and other DCO tools as deployed within customers' enterprise)
- May participate in risk assessment during the Certification and Accreditation process

Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.
## Information Technology (IT) Multiple Award Schedule

### Highly Adaptive Cybersecurity Services (HACS)

### Contract Number: GS-35F-248GA

<table>
<thead>
<tr>
<th>Minimum Qualifications and Experience</th>
<th>Level</th>
<th>Education</th>
<th>Experience (Years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level III</td>
<td>Masters or Equivalent</td>
<td>15+</td>
<td></td>
</tr>
<tr>
<td>Level II</td>
<td>Bachelors or Equivalent</td>
<td>8-12</td>
<td></td>
</tr>
<tr>
<td>Level I</td>
<td>Bachelors or Equivalent</td>
<td>2-5</td>
<td></td>
</tr>
</tbody>
</table>

### Labor Category: Penetration Tester

<table>
<thead>
<tr>
<th>Functional Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Conducts and/or supporting authorized penetration testing on enterprise network assets</td>
</tr>
<tr>
<td>- Emulates adversarial cyber activities to identify weaknesses, enumerate vulnerabilities, and assess the overall security posture of customer networks and information systems</td>
</tr>
<tr>
<td>- Analyzing site/enterprise DCO policies and configurations and evaluate compliance with regulations and enterprise directives</td>
</tr>
<tr>
<td>- Assisting with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes)</td>
</tr>
<tr>
<td>- Assesses threats to the environment via penetration testing, risk assessments and other assessments</td>
</tr>
<tr>
<td>- Provides inputs on the adequacy of security designs and architectures</td>
</tr>
<tr>
<td>- Supports cybersecurity assessments, defensive and offensive operations</td>
</tr>
<tr>
<td>- Provides support to security certification test and evaluation of assets, vulnerability management and response, security assessments, and provides customer support and guidance</td>
</tr>
</tbody>
</table>

### Minimum Qualifications and Experience

Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.

<table>
<thead>
<tr>
<th>Level</th>
<th>Education</th>
<th>Experience (Years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level III</td>
<td>Masters or Equivalent</td>
<td>15+</td>
</tr>
<tr>
<td>Level II</td>
<td>Bachelors or Equivalent</td>
<td>8-12</td>
</tr>
<tr>
<td>Level I</td>
<td>Bachelors or Equivalent</td>
<td>2-5</td>
</tr>
</tbody>
</table>

### Labor Category: Cybersecurity Software Developer

<table>
<thead>
<tr>
<th>Functional Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Develops, maintains, and enhances complex and diverse software systems (e.g., processing-intensive analytics, novel algorithm development, manipulation of extremely large data sets, real-time systems, and business management information systems) based on documented requirements</td>
</tr>
<tr>
<td>- Provides specific input to the software components of system design to include hardware/software trade-offs, software reuse, use of COTS/GOTS in place of new development, and requirements analysis and synthesis from system level to individual software components</td>
</tr>
<tr>
<td>- Designs, implements, and integrates software applications or performs software engineering tasks</td>
</tr>
</tbody>
</table>
- Utilizes software engineering and design methodologies appropriate to the development, integration, and production environment
- Ensures efficient delivery of software engineering capabilities using industry standards and repeatable processes
- Mitigates risks, controls costs and schedule variance, and effectively manages large scale, integrated software projects
- Reviews and tests software components for adherence to the design requirements and documents test results
- Supports software and web architecture development, requirements analysis, process execution and evaluation, selection and evaluation of COTS/GOTS tools, and integration (with both new and legacy systems)
- Interacts with customers and development team to gather and define requirements
- Analyzes and studies customer requirements to determine the most effective software and web technologies to satisfy their needs
- Designs, creates, tests, and maintains software and web based applications and content solutions to satisfy customer requirements
- Provides software process management and configuration management throughout the software / web development lifecycle

<table>
<thead>
<tr>
<th>Minimum Qualifications and Experience</th>
<th>Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
<td><strong>Education</strong></td>
</tr>
<tr>
<td>Level III</td>
<td>Masters or Equivalent</td>
</tr>
<tr>
<td>Level II</td>
<td>Bachelors or Equivalent</td>
</tr>
<tr>
<td>Level I</td>
<td>Bachelors or Equivalent</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>Cybersecurity Systems Engineer</th>
</tr>
</thead>
</table>
| **Functional Responsibilities** | - Analyzes user’s requirements, concept of operations documents, and high level system architectures to develop network requirements specifications
- Guides users in formulating requirements, advises alternative approaches, and conducts feasibility studies
- Provides technical leadership for the integration of network requirements, design, and technology
- Incorporates new network plans, designs and systems into ongoing operations
- Develops network architecture and network design documentation
- Guides network development and implementation planning through assessment or preparation of network engineering management plans and network integration and test plans
- Designs and performs integration of new technologies into local and wide area networks
- Provides advanced troubleshooting and problem resolution of complex network problems |
- Manages the transition and migration of networks and development of network addressing schemes
- Performs administration duties for networking hardware including routers, switches, hubs, gateways, access points, network interface cards, networking cables, network bridges, modems, ISDN adapters, firewalls and other related network hardware
- Analyzes system requirements and leads design and development activities
- Interacts with the customer/Government regarding Systems Engineering technical considerations and for associated problems, issues or conflicts
- Supports the development of cross functional or large-scale automated information systems to include enterprise architectures
- Provides comprehensive definition of all aspects of system development from analysis of mission needs to verification of system performance
- Performs evaluation of system alternatives and assessment of risks and costs

Minimum Qualifications and Experience
Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.

<table>
<thead>
<tr>
<th>Level</th>
<th>Education</th>
<th>Experience (Years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level III</td>
<td>Masters or Equivalent</td>
<td>12+</td>
</tr>
<tr>
<td>Level II</td>
<td>Bachelors or Equivalent</td>
<td>5-8</td>
</tr>
<tr>
<td>Level I</td>
<td>Bachelors or Equivalent</td>
<td>1-2</td>
</tr>
</tbody>
</table>

Labor Category
Program / Project Manager

Functional Responsibilities
- Responsible for the successful cost, schedule, performance and quality of the contract
- Serves as the main point of contact for the Contracting Officer (CO), the Contracting Officer’s Representative (COR), the Government Program Manager, and the Contractor’s senior management
- Ensures proper performance of tasks necessary to ensure the most efficient and effective execution of the contract
- Utilizes expert communication skills needed to direct the skilled technical resources and report on the technical progress, issues, and problem areas, as well as write and review technical documents
- Plans, executes, and finalizes projects that meet or exceed customer objectives
- Develops the overall project plan and manages project operations
- Manages the project stakeholders, project team, project risk, project schedule, project budget, and project conflicts
- Ensures team members know and execute their respective roles and the roles of the other team members
- Ensures proper relationships are established between customers, teaming partners, and vendors to facilitate the delivery of information technology services
Minimum Qualifications and Experience

Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.

<table>
<thead>
<tr>
<th>Level</th>
<th>Education</th>
<th>Experience (Years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level III</td>
<td>Masters or Equivalent</td>
<td>12+</td>
</tr>
<tr>
<td>Level II</td>
<td>Bachelors or Equivalent</td>
<td>5-8</td>
</tr>
<tr>
<td>Level I</td>
<td>Bachelors or Equivalent</td>
<td>1-2</td>
</tr>
</tbody>
</table>

Labor Category: Program / Project Analyst

Functional Responsibilities
- Responsible for designing, developing, and maintaining detailed resource-loaded schedules for implementation, developmental and operational systems
- Works with developmental and operational teams to develop detailed schedules and assists in keeping these schedules current
- Develops and or modifies project schedules and or the integration of multiple project schedules into an overall Master Program Schedule
- Maintains the overall Master Program /Project Schedule
- Links project schedules with the overarching program, Investment Portfolio, functional area and/or other Integrated Master Plans (IMPs)
- Provides hands-on development of layered schedules and IMPs that address how an acquisition project is progressing and how that project contributes to overarching requirements and objectives
- Maintains status on linkages and dependencies with related projects

Minimum Qualifications and Experience

Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.

<table>
<thead>
<tr>
<th>Level</th>
<th>Education</th>
<th>Experience (Years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level III</td>
<td>Masters or Equivalent</td>
<td>12+</td>
</tr>
<tr>
<td>Level II</td>
<td>Bachelors or Equivalent</td>
<td>5-8</td>
</tr>
<tr>
<td>Level I</td>
<td>Bachelors or Equivalent</td>
<td>1-2</td>
</tr>
</tbody>
</table>

Equivalencies

BreakPoint Labs Equivalencies

<table>
<thead>
<tr>
<th>Degree</th>
<th>Equivalent Qualifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhD</td>
<td>Masters + 5 years experience</td>
</tr>
<tr>
<td></td>
<td>Bachelors + 10 years experience</td>
</tr>
<tr>
<td>Masters</td>
<td>Bachelors + 5 years experience</td>
</tr>
<tr>
<td>Bachelors</td>
<td>Associate + 5 years experience</td>
</tr>
<tr>
<td>Associates</td>
<td>HS or equivalent + 5 years experience</td>
</tr>
<tr>
<td>HS</td>
<td>GED or equivalent</td>
</tr>
</tbody>
</table>
Pricing

Effective 1 November 2019

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Subject Matter Expert III</td>
<td>$262.09</td>
</tr>
<tr>
<td>Cybersecurity Subject Matter Expert II</td>
<td>$155.75</td>
</tr>
<tr>
<td>Cybersecurity Subject Matter Expert I</td>
<td>$123.78</td>
</tr>
<tr>
<td>Cybersecurity Technical Expert III</td>
<td>$206.31</td>
</tr>
<tr>
<td>Cybersecurity Technical Expert II</td>
<td>$149.90</td>
</tr>
<tr>
<td>Cybersecurity Technical Expert I</td>
<td>$104.68</td>
</tr>
<tr>
<td>Cybersecurity Technical Analyst III</td>
<td>$188.85</td>
</tr>
<tr>
<td>Cybersecurity Technical Analyst II</td>
<td>$140.05</td>
</tr>
<tr>
<td>Cybersecurity Technical Analyst I</td>
<td>$104.50</td>
</tr>
<tr>
<td>Incident Responder III</td>
<td>$183.18</td>
</tr>
<tr>
<td>Incident Responder II</td>
<td>$135.84</td>
</tr>
<tr>
<td>Incident Responder I</td>
<td>$101.10</td>
</tr>
<tr>
<td>Penetration Tester III</td>
<td>$186.01</td>
</tr>
<tr>
<td>Penetration Tester II</td>
<td>$137.95</td>
</tr>
<tr>
<td>Penetration Tester I</td>
<td>$103.54</td>
</tr>
<tr>
<td>Cybersecurity Software Developer III</td>
<td>$202.73</td>
</tr>
<tr>
<td>Cybersecurity Software Developer II</td>
<td>$154.14</td>
</tr>
<tr>
<td>Cybersecurity Software Developer I</td>
<td>$122.66</td>
</tr>
<tr>
<td>Cybersecurity Systems Engineer III</td>
<td>$166.51</td>
</tr>
<tr>
<td>Cybersecurity Systems Engineer II</td>
<td>$131.74</td>
</tr>
<tr>
<td>Cybersecurity Systems Engineer I</td>
<td>$83.02</td>
</tr>
<tr>
<td>Program / Project Manager III</td>
<td>$202.73</td>
</tr>
<tr>
<td>Program / Project Manager II</td>
<td>$159.73</td>
</tr>
<tr>
<td>Program / Project Manager I</td>
<td>$90.49</td>
</tr>
<tr>
<td>Program / Project Analyst III</td>
<td>$132.45</td>
</tr>
<tr>
<td>Program / Project Analyst II</td>
<td>$94.27</td>
</tr>
<tr>
<td>Program / Project Analyst I</td>
<td>$65.45</td>
</tr>
</tbody>
</table>
BreakPoint Labs, LLC. Commitment to Promote Small Business Participation Procurement Programs

PREAMBLE

BreakPoint Labs, LLC. provides commercial products and services to ordering activities. We are committed to promoting participation of small, small disadvantaged and women-owned small businesses in our contracts. We pledge to provide opportunities to the small business community through reselling opportunities, mentor-protégé programs, joint ventures, teaming arrangements, and subcontracting.

COMMITMENT

To actively seek and partner with small businesses.

To identify, qualify, mentor and develop small, small disadvantaged and women-owned small businesses by purchasing from these businesses whenever practical.

To develop and promote company policy initiatives that demonstrate our support for awarding contracts and subcontracts to small business concerns.

To undertake significant efforts to determine the potential of small, small disadvantaged and women-owned small business to supply products and services to our company.

To insure procurement opportunities are designed to permit the maximum possible participation of small, small disadvantaged, and women-owned small businesses.

To attend business opportunity workshops, minority business enterprise seminars, trade fairs, procurement conferences, etc., to identify and increase small businesses with whom to partner.

To publicize in our marketing publications our interest in meeting small businesses that may be interested in subcontracting opportunities.

We signify our commitment to work in partnership with small, small disadvantaged and women-owned small businesses to promote and increase their participation in ordering activity contracts. To accelerate potential opportunities please contact BreakPoint Labs, LLC., William Glodek at 1-844-422-5632 or email contracts@breakpoint-labs.com.
Best Value Blanket Purchase Agreement
Federal Supply Multiple Award Schedule

(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act (ordering activity) and (Contractor) enter into a cooperative agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Multiple Award Schedule Contract(s) _______.

Federal Supply Multiple Award Schedule contract BPAs eliminate contracting and open market costs such as: search for sources; the development of technical documents, solicitations and the evaluation of offers. Teaming Arrangements are permitted with Federal Supply Multiple Award Schedule Contractors in accordance with Federal Acquisition Regulation (FAR) 9.6.

This BPA will further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive, individual purchases from the schedule contract. The end result is to create a purchasing mechanism for the ordering activity that works better and costs less.

Signatures

<table>
<thead>
<tr>
<th>Ordering Activity</th>
<th>Date</th>
<th>Contractor</th>
<th>Date</th>
</tr>
</thead>
</table>

Pursuant to GSA Federal Supply Multiple Award Schedule Contract Number(s), Blanket Purchase Agreements, the Contractor agrees to the following terms of a Blanket Purchase Agreement (BPA) EXCLUSIVELY WITH (ordering activity):

(1) The following contract items can be ordered under this BPA. All orders placed against this BPA are subject to the terms and conditions of the contract, except as noted below:

<table>
<thead>
<tr>
<th>Model Number / Part Number</th>
<th>*Special BPA Discount/Price</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(2) Delivery:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Delivery Schedules / Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(3) The ordering activity estimates, but does not guarantee, that the volume of purchases through this agreement will be ________________.

(4) This BPA does not obligate any funds.

(5) This BPA expires on __________ or at the end of the contract period, whichever is earlier.

(6) The following office(s) is hereby authorized to place orders under this BPA:

<table>
<thead>
<tr>
<th>Office</th>
<th>Point of Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(7) Orders will be placed against this BPA via Electronic Data Interchange (EDI), FAX, or paper.

(8) Unless otherwise agreed to, all deliveries under this BPA must be accompanied by delivery tickets or sales slips that must contain the following information as a minimum:

(a) Name of Contractor;
(b) Contract Number;
(c) BPA Number;
(d) Model Number or National Stock Number (NSN);
(e) Purchase Order Number;
(f) Date of Purchase;
(g) Quantity, Unit Price, and Extension of Each Item (unit prices and extensions need not be shown when incompatible with the use of automated systems; provided, that the invoice is itemized to show the information); and
(h) Date of Shipment.
(9) The requirements of a proper invoice are specified in the Federal Supply Multiple Award Schedule contract. Invoices will be submitted to the address specified within the purchase order transmission issued against this BPA.

(10) The terms and conditions included in this BPA apply to all purchases made pursuant to it. In the event of an inconsistency between the provisions of this BPA and the Contractor’s invoice, the provisions of this BPA will take precedence.