Online access to contract ordering information, terms and conditions, up to date pricing, and the option to create an electronic delivery order are available through GSA Advantage!, a menu driven database system. The internet address for GSA Advantage! is: GSAAdvantage.gov.

### General Purpose Commercial Information Technology Equipment, Software and Services (MASS Schedule)

<table>
<thead>
<tr>
<th>FPDS Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D301</td>
<td>IT and Telecom – Facility Operation and Maintenance</td>
</tr>
<tr>
<td>D302</td>
<td>IT and Telecom Systems Development</td>
</tr>
<tr>
<td>D303</td>
<td>IT and Telecom – Data Entry</td>
</tr>
<tr>
<td>D305</td>
<td>IT and Telecom – Teleprocessing, Timeshare and Cloud Computing</td>
</tr>
<tr>
<td>D306</td>
<td>IT and Telecom – Systems Analysis</td>
</tr>
<tr>
<td>D307</td>
<td>IT and Telcom – IT Strategy and Architecture</td>
</tr>
<tr>
<td>D308</td>
<td>Programming</td>
</tr>
<tr>
<td>D310</td>
<td>IT and Telecom Cyber Security and Data Backup</td>
</tr>
<tr>
<td>D311</td>
<td>IT and Telecom Data Conversion</td>
</tr>
<tr>
<td>D312</td>
<td>IT and Telecom Optical Scanning</td>
</tr>
<tr>
<td>D313</td>
<td>IT and Telecom Computer Aided Design/Computer Aided Manufacturing</td>
</tr>
<tr>
<td>D316</td>
<td>IT and Telecom Telecommunications Network Management</td>
</tr>
<tr>
<td>D317</td>
<td>IT and Telecom Web-based subscription</td>
</tr>
<tr>
<td>D319</td>
<td>IT and Telcom Annual Software Maintenance Service Plans</td>
</tr>
<tr>
<td>D320</td>
<td>IT and Telecom Annual Hardware Maintenance Service Plans</td>
</tr>
<tr>
<td>D322</td>
<td>IT and Telecom – Internet</td>
</tr>
<tr>
<td>D324</td>
<td>IT and Telecom – Business Continuity</td>
</tr>
<tr>
<td>D399</td>
<td>IT and Telecom Other Information Technology Services, Not Elsewhere Classified</td>
</tr>
</tbody>
</table>

**Note 1:** All non-professional labor categories must be incidental to and used solely to support hardware, software and/or professional services, and cannot be purchased separately.

**Note 2:** Offerors and Agencies are advised that the Group 70 – Information Technology Schedule is not to be used as a means to procure services that properly fall under the Brooks Act. These services include, but are not limited to, architectural, engineering, mapping, cartographic production, remote sensing, geographic information systems, and related services. FAR 36.6 distinguishes between mapping services of an A/E nature and mapping services that are not connected nor incidental to the traditionally accepted A/E Services.

**Note 3:** This solicitation is not intended to solicit for the reselling of IT Professional Services, except for the provision of implementation, maintenance, integration, or training services in direct support of a product. Under such circumstances the services must be performance by the publisher or manufacturer or one of their authorized agents.

For more information on ordering from Federal Supply Schedules go to the GSA Schedules page at GSA.gov.

**GS-35F-0621T**

**Contract Period:** August 31, 2022 – August 30, 2027

Veris Group, LLC dba Coalfire Federal  
PO BOX 220985 Chantilly, VA 20153  
703-935-5749  
[www.coalfirefederal.com](http://www.coalfirefederal.com)  
Large Business
# TABLE OF CONTENTS

## SECTION 1.0 INFORMATION FOR ORDERING ACTIVITIES (ALL SINS)  
### 1.1 CUSTOMER INFORMATION ...
### 1.2 MAXIMUM ORDER ...
### 1.3 MINIMUM ORDER ...
### 1.4 GEOGRAPHIC COVERAGE ...
### 1.5 POINT(S) OF PRODUCTION ...
### 1.6 DISCOUNTS FROM LIST PRICE(S) ...
### 1.7 QUANTITY DISCOUNTS ...
### 1.8 PROMPT PAYMENT TERMS ...
### 1.9 FOREIGN ITEMS ...
### 1.10 DELIVERY ...
### 1.11 F.O.B POINT(S) ...
### 1.12 ORDERING INFORMATION ...
### 1.13 PAYMENT ADDRESS(ES) ...
### 1.14 WARRANTY PROVISION ...
### 1.15 EXPORT PACKING CHARGES ...
### 1.16 RENTAL, MAINTENANCE, AND REPAIR ...
### 1.17 INSTALLATION ...
### 1.18 REPAIR PARTS ...
### 1.19 SERVICE AND DISTRIBUTION POINTS ...
### 1.20 PARTICIPATING DEALERS ...
### 1.21 PREVENTIVE MAINTENANCE ...
### 1.22 SPECIAL ATTRIBUTES ...
### 1.23 UNIQUE ENTITY IDENTIFIER (UEI) NUMBER ...
### 1.24 SYSTEM FOR AWARD MANAGEMENT (SAM) ...

## SECTION 2.0 TERMS AND CONDITIONS (ALL SINS)  
### 2.1 LIABILITY FOR INJURY OR DAMAGE ...
### 2.2 FEDERAL IT / TELECOMMUNICATION STANDARDS REQUIREMENTS ...
### 2.3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS ...
### 2.4 FEDERAL TELECOMMUNICATIONS STANDARDS (FED-STDs) ...
### 2.5 CONTRACTOR TASKS / SPECIAL REQUIREMENTS (C-FSS-370) (NOV 2003) ...
### 2.6 CONTRACT ADMINISTRATION FOR ORDERING ACTIVITIES ...
### 2.7 PURCHASE OF OPEN MARKET ITEMS ...
2.8 OVERSEAS ACTIVITIES .................................................................11
2.9 BLANKET PURCHASE AGREEMENTS (BPA) ........................................11
2.10 CONTRACTOR TEAM ARRANGEMENTS ...........................................11
2.11 PRIME CONTRACTOR ORDERING FROM FEDERAL SUPPLY SCHEDULES ...11
2.12 INSURANCE-WORK ON GOVERNMENT INSTALLATION (JAN 1997) ..............11
2.13 SOFTWARE INTEROPERABILITY ..........................................................12
2.14 ADVANCE PAYMENTS .........................................................................12

SECTION 3.0 TERMS AND CONDITIONS INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S) 13

3.1 SCOPE ............................................................................................13
3.2 PERFORMANCE INCENTIVES ..........................................................13
3.3 ORDER ..........................................................................................13
3.4 PERFORMANCE OF SERVICES .........................................................13
3.5 STOP-WORK ORDER (FAR 52.242-15)(AUG 1989) .................................14
3.6 INSPECTION OF SERVICES ..............................................................14
3.7 RESPONSIBILITIES OF THE CONTRACTOR ........................................14
3.8 RESPONSIBILITIES OF THE ORDERING ACTIVITY ..............................14
3.9 INDEPENDENT CONTRACTOR ..........................................................14
3.10 ORGANIZATIONAL CONFLICT OF INTEREST ....................................15
3.11 INVOICES ....................................................................................15
3.12 PAYMENTS ..................................................................................15
3.13 RESUMES ....................................................................................15
3.14 INCIDENTAL SUPPORT COSTS .........................................................15
3.15 APPROVAL OF SUBCONTRACTS .......................................................15
3.16 DESCRIPTION OF IT SERVICES AND PRICING .................................16
3.17 SIN 54151S COMMERCIAL LABOR CATEGORY DESCRIPTIONS ...............16
3.18 SIN 54151S LABOR CATEGORY QUALIFICATION EQUIVALENCIES .............21

SECTION 4.0 TERMS AND CONDITIONS (HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (SINS 54151HACS) 22

4.1 SCOPE ............................................................................................22
4.2 ORDER ..........................................................................................24
4.3 PERFORMANCE OF SERVICES .........................................................24
4.4 INSPECTION OF SERVICES ..............................................................25
4.5 RESPONSIBILITIES OF THE CONTRACTOR ........................................25
4.6 RESPONSIBILITIES OF THE ORDERING ACTIVITY ....................................................... 25
4.7 INDEPENDENT CONTRACTOR ....................................................................................... 25
4.8 ORGANIZATIONAL CONFLICTS OF INTEREST ......................................................... 25
4.9 INVOICES ......................................................................................................................... 25
4.10 RESUMES ..................................................................................................................... 26
4.11 APPROVAL OF SUBCONTRACTS .............................................................................. 26
4.12 DESCRIPTION OF HACS SERVICES AND PRICING ............................................. 26
4.13 SIN 54151HACS LABOR CATEGORY DESCRIPTIONS ........................................... 27

SECTION 5.0 USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION
PROCUREMENT PROGRAMS 32

5.1 PREAMBLE ..................................................................................................................... 32
5.2 COMMITMENT .............................................................................................................. 32

SECTION 6.0 BLANKET PURCHASE AGREEMENT 33

SECTION 7.0 ORDER-LEVEL MATERIALS 37
SECTION 1.0 INFORMATION FOR ORDERING ACTIVITIES (ALL SINS)

1.1 CUSTOMER INFORMATION
1.a Table of Awarded Special Item Number(s)

<table>
<thead>
<tr>
<th>SINS</th>
<th>Description</th>
<th>Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES</td>
<td>See Section 3.16</td>
</tr>
<tr>
<td>54151HACS</td>
<td>HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)</td>
<td>See Section 4.12</td>
</tr>
<tr>
<td>70-500</td>
<td>ORDER-LEVEL MATERIALS (OLMS)</td>
<td>Priced at the Order Level</td>
</tr>
</tbody>
</table>

1.b Lowest Price Model Number and Unit Price
Not Applicable

1.c Commercial Job Titles and Descriptions
SIN 54151S: Information Technology (IT) Professional Services, see Section 3.16
SIN 54151HACS: Highly Adaptive Cybersecurity Services (HACS), see Section 4.12

1.2 MAXIMUM ORDER
The Maximum Order value is $500,000. All Dollar Amounts are Exclusive of any Discount for Prompt Payment

1.3 MINIMUM ORDER
The minimum dollar value of orders to be issued is $100

1.4 GEOGRAPHIC COVERAGE

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.

Offerors are requested to check one of the following boxes:

[X] The Geographic Scope of Contract will be domestic and overseas delivery.
[ ] The Geographic Scope of Contract will be overseas delivery only.
[ ] The Geographic Scope of Contract will be domestic delivery only.

1.5 POINT(S) OF PRODUCTION
Not Applicable

1.6 DISCOUNTS FROM LIST PRICE(S)
SIN 54151S: See Section 3.16
SIN 54151HACS: See Section 4.12
SIN 70-500: To be determined by individual order

1.7 QUANTITY DISCOUNTS
None

1.8 PROMPT PAYMENT TERMS
Prompt Payment: 0.5% - 10 days from receipt of invoice or date of acceptance, whichever is later.
Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.
1.9 FOREIGN ITEMS
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.

1.10 DELIVERY
10.a Time of Delivery

<table>
<thead>
<tr>
<th>SPECIAL ITEM NUMBER</th>
<th>DELIVERY TIME (Days ARO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>As per client request</td>
</tr>
<tr>
<td>54151HACS</td>
<td>As per client request</td>
</tr>
<tr>
<td>70-500</td>
<td>To be determined by individual order</td>
</tr>
</tbody>
</table>

10.b Expedited Delivery
Items available for expedited delivery are noted in this price list when applicable.

10.c Overnight and 2-day Delivery
As per client request.

10.d 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.

1.11 F.O.B POINT(S)
Destination

1.12 ORDERING INFORMATION
12.a Ordering Address(es)
Corporate Headquarters
Veris Group, LLC dba Coalfire Federal
PO BOX 220985
Chantilly, VA 20153
Tel: 703-935-5749| Fax: 703-880-7590
www.coalfirefederal.com

The following telephone number(s) can be used by ordering activities to obtain technical and/or ordering assistance:

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Telephone No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>William Malone</td>
<td>Executive Vice President</td>
<td>571-392-5071</td>
</tr>
<tr>
<td>Andrew Dunlop</td>
<td>Vice President</td>
<td>703-402-4397</td>
</tr>
<tr>
<td>Lisa Kennedy</td>
<td>Director Federal Contracts</td>
<td>703-935-5749</td>
</tr>
</tbody>
</table>

12.b Ordering Procedures
Ordering activities shall use the ordering procedures of Federal Acquisition Regulation (FAR) 8.405 when placing an order or establishing a Blanket Purchase Agreement (BPA) for supplies or services. These procedures apply to all schedules.
FAR 8.405-1 Ordering procedures for supplies, and services not requiring a statement of work.
FAR 8.405-2 Ordering procedures for services requiring a statement of work.
1.13 PAYMENT ADDRESS(ES)
Veris Group, LLC dba Coalfire Federal
PO BOX 220985
Chantilly, VA 20153
Tel: 571 384 2328| Fax: 703-880-7590
www.coalfirefederal.com

1.14 WARRANTY PROVISION
14.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.

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

1.15 EXPORT PACKING CHARGES
Not Applicable

1.16 RENTAL, MAINTENANCE, AND REPAIR
Not Applicable

1.17 INSTALLATION
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 33411.

1.18 REPAIR PARTS
18.a Repair Part: Not Applicable

18.b Terms and Conditions applicable to other services: Not Applicable
1.19  SERVICE AND DISTRIBUTION POINTS
Not Applicable

1.20  PARTICIPATING DEALERS
Not Applicable

1.21  PREVENTIVE MAINTENANCE
Not Applicable

1.22  SPECIAL ATTRIBUTES
22.a  Environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants) are not applicable.

22.b  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: www.coalfirefederal.com. The EIT standard can be found at: www.Section508.gov/.

1.23  UNIQUE ENTITY IDENTIFIER (UEI) NUMBER
Unique Entity Identifier (UEI) number: P2BGLMB7JN52

1.24  SYSTEM FOR AWARD MANAGEMENT (SAM)
Coalfire Federal has registered in the System for Award Management Database.
Type of Contractor – Large Business
Woman-Owned Small Business – No
Contractor's Taxpayer Identification Number (TIN): 20-2300601
Veteran Owned Small Business (VOSB): No
CAGE Code: 36BY6
SECTION 2.0 TERMS AND CONDITIONS (ALL SINS)

2.1 LIABILITY FOR INJURY OR 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.

2.2 FEDERAL IT / TELECOMMUNICATION 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.

2.3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS
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.

2.4 FEDERAL TELECOMMUNICATIONS 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, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Ordering information and information concerning the availability of FED-STDs should be obtained from the GSA, Federal Supply 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, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone number (301) 975-2833.

2.5 CONTRACTOR TASKS / SPECIAL REQUIREMENTS (C-FSS-370) (NOV 2003)

2.5.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.

2.5.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. The Industrial Funding Fee does NOT apply to travel and per diem charges.

NOTE: Refer to FAR Part 31.205-46 Travel Costs, for allowable costs that pertain to official company business travel in regard to this contract.

2.5.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.

2.5.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.

2.5.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.

2.5.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.

2.5.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.

2.5.h Data/Deliverable Requirements: Any required data/deliverables at the ordering level will be as specified or negotiated in the agency’s order.

2.5.i Government-Furnished Property: As specified by the agency’s order, the Government may provide property, equipment, materials or resources as necessary.

2.5.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.

2.5.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).

2.6 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 (l) Termination for the ordering activity’s convenience, and (m) Termination for Cause.

2.7 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. ODCs (Other Direct Costs) are not part of this contract and should be treated as open market purchases. 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.

2.8 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:

2.9 BLANKET PURCHASE AGREEMENTS (BPA)
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).

2.10 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.

2.11 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 –

2.11.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

2.11.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.

2.12 INSURANCE-WORK ON GOVERNMENT INSTALLATION (JAN 1997)
2.12.a In accordance with FAR 52.228-5, 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.

2.12.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.

2.12.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.

2.13 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.

2.14 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).
SECTION 3.0 TERMS AND CONDITIONS INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S)

3.1 SCOPE
3.1a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT/IAM Professional Services within the scope of this Information Technology Schedule.

3.1b. 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.

3.2 PERFORMANCE INCENTIVES
3.2a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract in accordance with this contract.

3.2b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.

3.2c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity’s mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3.3 ORDER
3.3a. Agencies may use written orders, 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.

3.3b. 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.

3.4 PERFORMANCE OF SERVICES
3.4a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

3.4b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

3.4c. 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.

3.4d. Any Contractor travel required in the performance of IT/IAM 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.
3.5 STOP-WORK ORDER (FAR 52.242-15)(AUG 1989)

3.5a The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

3.5b If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

3.5c If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

3.5d If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

3.6 INSPECTION OF SERVICES


3.7 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 (Deviation – Dec 2007) Rights in Data – General, may apply.

3.8 RESPONSIBILITIES OF THE ORDERING ACTIVITY
Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT/IAM Professional Services.

3.9 INDEPENDENT CONTRACTOR
All IT/EC 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.
3.10 ORGANIZATIONAL CONFLICT OF INTEREST

3.10.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.

3.10b. 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.

3.11 INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for IT/EC 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.

3.12 PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time and materials orders, the Payments under Time and Materials and Labor Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) applies to time and materials orders placed under this contract. For labor hour orders, the Payment under Time and Materials and Labor Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) applies to labor hour orders placed under this contract.

3.13 RESUMES

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

3.14 INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

3.15 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.
3.16 DESCRIPTION OF IT SERVICES AND PRICING
The following pages contain the description of categories of IT/IAM Professional services offered along with the corresponding prices.

Table 1: 3.17 SIN 54151S IT Services Government Site Hourly Rates

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Labor Category</th>
<th>08/31/22</th>
<th>08/30/23</th>
<th>08/31/23</th>
<th>08/30/24</th>
<th>08/31/24</th>
<th>08/30/25</th>
<th>08/31/25</th>
<th>08/30/26</th>
<th>08/31/26</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Program Manager</td>
<td>$135.32</td>
<td>$138.57</td>
<td>$141.89</td>
<td>$145.30</td>
<td>$148.79</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Senior Systems Analyst</td>
<td>$113.21</td>
<td>$115.93</td>
<td>$118.71</td>
<td>$121.56</td>
<td>$124.48</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Information Security Specialist</td>
<td>$129.87</td>
<td>$132.98</td>
<td>$136.18</td>
<td>$139.44</td>
<td>$142.79</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Data Security Analyst Int</td>
<td>$130.36</td>
<td>$133.48</td>
<td>$136.69</td>
<td>$139.97</td>
<td>$143.33</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Data Security Analyst Senior</td>
<td>$133.92</td>
<td>$137.13</td>
<td>$140.42</td>
<td>$143.79</td>
<td>$147.24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Security Engineer</td>
<td>$139.58</td>
<td>$142.93</td>
<td>$146.36</td>
<td>$149.87</td>
<td>$153.47</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Analyst I</td>
<td>$76.83</td>
<td>$78.68</td>
<td>$80.57</td>
<td>$82.50</td>
<td>$84.48</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Analyst II</td>
<td>$100.05</td>
<td>$102.46</td>
<td>$104.91</td>
<td>$107.43</td>
<td>$110.01</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Security Analyst I</td>
<td>$122.52</td>
<td>$125.46</td>
<td>$128.47</td>
<td>$131.55</td>
<td>$134.71</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Security Analyst II</td>
<td>$138.67</td>
<td>$142.00</td>
<td>$145.41</td>
<td>$148.90</td>
<td>$152.47</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Consultant I</td>
<td>$162.10</td>
<td>$165.99</td>
<td>$169.98</td>
<td>$174.06</td>
<td>$178.23</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Consultant II</td>
<td>$153.58</td>
<td>$157.27</td>
<td>$161.04</td>
<td>$164.91</td>
<td>$168.87</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Consultant III</td>
<td>$177.87</td>
<td>$182.14</td>
<td>$186.51</td>
<td>$190.99</td>
<td>$195.57</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Consultant IV</td>
<td>$217.33</td>
<td>$222.55</td>
<td>$227.89</td>
<td>$233.36</td>
<td>$238.96</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Project Manager I</td>
<td>$133.06</td>
<td>$136.25</td>
<td>$139.52</td>
<td>$142.87</td>
<td>$146.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Subject Matter Expert</td>
<td>$277.93</td>
<td>$284.60</td>
<td>$291.43</td>
<td>$298.43</td>
<td>$305.59</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Coalfire Federal applies a fixed escalation rate of 2.4% based on the Bureau of Labor Statistics Employment Cost Index (ECI), Table 5: Compensation – Not Seasonally Adjusted – Employment Cost Index for Total Compensation, for Private Industry Workers, by Occupational Group and Industry.

Note: The rates listed above include the Industrial Funding Fee (IFF).

3.16.a Basic Discount Terms = .75% So 37.31% Rounded 1% to 37%.

3.17 SIN 54151S COMMERCIAL LABOR CATEGORY DESCRIPTIONS

3.17.1 PROGRAM MANAGER

Minimum Technical Qualifications/Experience: Overall eight years of experience in the IT industry, out of which at least five years must be in the field of Program Management, Project Management of IT projects, and/or Client Account and Relationship Management.

Functional Responsibility: Program Manager is the central point of contact with the Contracting Officer, Contracting Officer’s Representative and Task Managers. Responsible for coordinating the management of all work performed on this contract, including subcontractors, team members, and vendors. Keeps in constant touch with the project managers regarding the status of various task order projects, the issues facing the project teams and effectively and regularly updates the client representatives. Also facilitates the information, which the team requires from the client to effectively implement various Task Order Projects and if necessary, escalates the burning issues to the client representatives and contract officer.
**Minimum Education:** Bachelor’s degree in relevant IT or business management field or equivalent industry qualification and three or more years of additional experience. Master’s Degree in IT systems, MIS, Computer Science, or master’s degree in Business Administration is desirable.

### 3.17.2 SENIOR SYSTEMS ANALYST

**Minimum Technical Qualifications/Experience:** Overall three years of experience in analyzing information systems, and business processes of organizations, mentoring other System Analysts, coordinating and supporting the development, enhancement, and maintenance of products and services applicable to multiple lines of a customer's business using information technology.

**Functional Responsibility:** Coordinates and supports the development, enhancement, and maintenance of products and services applicable to multiple lines of a customer's business using information technology. Also responsible for technically analyzing the business processes, and/or Information Systems of organizations. This includes the analysis of the architecture of the system, what hardware, operating system and software the organization uses, what is the role of each hardware and software element, what databases the organization runs and on what platforms, is the data being used reliable, which processes run on which platform/hardware, in what programming languages have the business logic been written. Anticipates and identifies user problems and needs. Recommends business solutions based on customer requirements and industry trends. Leads, plans, schedules, and controls complex projects and activities with customers, support groups, and vendors on concurrent projects. Applies extensive knowledge of the customer's business and industry to develop project specifications. Advises on methods to improve business processes and remove non-value-added activities. Coordinates and participates in proposals, feasibility studies, implementations, and new business development. Leads the training of customers and peers and builds relationships with multiple customer levels. Performs Quality Assurance on systems and processes.

**Minimum Education:** Bachelor’s degree, or equivalent, in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors’ Degree in disciplines other than those listed above will also be considered if and only if they have at least four years of experience in analyzing the business processes and Information Systems of organizations.

### 3.17.3 INFORMATION SECURITY SPECIALIST

**Minimum Technical Qualifications/Experience:** Overall four years of experience in conducting security assessments of networks and information systems; and implementing, integrating and maintaining the Information Security of organizations.

**Functional Responsibility:** Analyzes and defines security requirement for computer systems which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solutions. Establishes and satisfies complex system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements.

**Minimum Education:** Bachelor’s degree, or equivalent, in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors’ Degree in disciplines other than those listed above will also be considered if and only if they have at least five years of experience in analyzing, designing, implementing, integrating and maintaining the Information Security of organizations.
3.17.4 DATA SECURITY ANALYST (SENIOR)

**Minimum Technical Qualifications/Experience:** At least three years of experience in defining data security requirements for high-level applications and systems, evaluation of approved security product capabilities, and developing solutions to multilevel security (MLS) problems.

**Functional Responsibility:** Analyzes and defines data requirements for MLS issues. Designs, develops, engineers, and implements solutions to MLS requirements. Responsible for the implementation and development of the MLS. Gathers and organizes technical information about an organization’s mission goals and needs, existing security products, and ongoing programs in the MLS arena. Performs risk analyses, which include risk assessment. Provides daily supervision of, and direction to, staff.

**Minimum Education:** Bachelor’s degree, or equivalent, in Computer Sciences, Information Systems, Business, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors’ Degree in disciplines other than those listed above will also be considered if and only if they have at least three years of experience in defining, implementing and maintaining the Information Security of organizations.

3.17.5 DATA SECURITY ANALYST (INTERMEDIATE)

**Minimum Technical Qualifications/Experience:** At least two years of specialized experience in defining data security requirements for high-level applications and systems, evaluation of approved security product capabilities, and developing solutions to multilevel security (MLS) problems.

**Functional Responsibility:** Analyzes and defines data security requirements for MLS issues. Designs, develops, engineers, and implements solutions to MLS requirements. Gathers and organizes technical information about an organization’s mission goals and needs, existing security products, and ongoing programs in the MLS arena. Performs risk analyses, which include risk assessment.

**Minimum Education:** Bachelor’s degree, or equivalent, in Computer Sciences, Information Systems, Business, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors’ Degree or equivalent experience in disciplines other than those listed above will also be considered if and only if they have at least two years of experience in defining, implementing and maintaining the Information Security of organizations.

3.17.6 SECURITY ENGINEER

**Minimum Technical Qualifications/Experience:** At least five years of experience in designing, analyzing or defining computer security requirements for network, systems or high-level applications, evaluating approved security product capabilities, and developing proper computer system security solutions.

**Functional Responsibility:** Designs, configures, reviews, or defines security requirements for complex networks, enterprise architecture, computer systems and environments, which may include mainframes, networks, servers, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Responsible for integration and implementation of the computer system security solution. Gathers and organizes technical information about an organization’s mission goals and needs, existing security products, and ongoing programs in computer security. Performs evaluation and risk analyses of computer systems and applications during all phases of the system development lifecycle.

**Minimum Education:** Bachelor’s degree, or equivalent, in Computer Sciences, Information Systems, MIS, Business, Mathematics or Engineering (Electrical, Computer, Mechanical). Industry/vendor certifications in IT and security domains. Candidates having Bachelors/Masters’
Degree in disciplines other than those listed above will also be considered if and only if they have at least six years of experience in defining, implementing and maintaining the Information Security of organizations.

3.17.7 ANALYST I

Minimum Technical Qualifications/Experience: Must have a minimum of two years of experience in at least one discipline. Understands fundamental concepts, processes, practices, and procedures of the specific professional or technical assignment or in specialty area. Performs tasks that are routine and learns to apply training to practice. Uses established procedures and works under close supervision in support of assigned project.

Functional Responsibility: Applies management analysis processes, statistical methods, and/or advanced technical and analytical research techniques to determine solutions based on client requirements with an IT services/solutions-based scope. Analyzes operational activities to obtain a quantitative, rational basis for decision making and resource allocation. Employs process improvements and reengineering methodologies and principles for modernization of systems and projects. Creates project plans to achieve performance-based objectives, enhancing implementation, systems and service. Provides integral support in mission requirements determination, conceptualization, design, development, testing, verification and validation, documentation, and implementation of system applications.

Minimum Education: A.A. or A.S. degree, or equivalent.

3.17.8 ANALYST II

Minimum Technical Qualifications/Experience: Must have a minimum of four years of experience in one or more disciplines. Possesses and applies comprehensive knowledge across multiple functional areas and task environments. Has leadership qualities in strategizing approaches and managing project objectives. Develops, plans, and leads segments of a project. Evaluates results and recommends changes in development and execution of project phases and meeting schedules. Operates across multiple tasks and works independently, contributes to deliverables and performance metrics.

Functional Responsibility: Applies management analysis processes, statistical methods, and/or advanced technical and analytical research techniques to determine solutions based on client requirements with an IT services/solutions-based scope. Analyzes operational activities to obtain a quantitative, rational basis for decision making and resource allocation. Employs process improvements and reengineering methodologies and principles for modernization of systems and projects. Creates project plans to achieve performance-based objectives, enhancing implementation, systems and service. Provides integral support in mission requirements determination, conceptualization, design, development, testing, verification and validation, documentation, and implementation of system applications.

Minimum Education: B.A. or B.S. degree, or equivalent.

3.17.9 SECURITY ANALYST I

Minimum Technical Qualifications/Experience: At least two years of experience in defining security programs or processes for the protection of information and systems.

Functional Responsibility: Analyzes and defines security requirements for information protection. Defines and develops security policies. Analyzes the sensitivity of information and performs vulnerability and risk assessments on the basis of defined sensitivity and information flow.

Minimum Education: A.A. or A.S. degree.
3.17.10 SECURITY ANALYST II

**Minimum Technical Qualifications/Experience:** At least two years of experience in defining security programs or processes for the protection of information and systems.

**Functional Responsibility:** Analyzes and defines security requirements for information protection. Defines and develops security policies. Analyzes the sensitivity of information and performs vulnerability and risk assessments on the basis of defined sensitivity and information flow.

**Minimum Education:** B.A. or B.S. degree, or equivalent,

3.17.11 CONSULTANT I

**Minimum Technical Qualifications/Experience:** At least three years of experience in collecting, analyzing, and reporting to solve technical or management issues.

**Functional Responsibility:** Serves as a consulting team member with an information technology background. Collects data in accordance with plans developed by others. Verifies and analyzes data to identify trends and relationships as well as current and potential technical and management problems. Drafts reports of findings along with related documentation.

**Minimum Education:** B.A. or B.S. degree, or equivalent.

3.17.12 CONSULTANT II

**Minimum Technical Qualifications/Experience:** At least five years of experience in collecting, analyzing, and reporting to solve technical or management issues.

**Functional Responsibility:** Serves as a senior member of consulting teams as a task manager or as a project leader on projects of limited scope and complexity. As a consulting team member, collects, analyzes, and interprets data in one or more information technology specialties. Develops, or participates in the development of assignment methodology.

**Minimum Education:** B.A. or B.S. degree, or equivalent.

3.17.13 CONSULTANT III

**Minimum Technical Qualifications/Experience:** At least seven years of experience in collecting, analyzing, and reporting to solve technical or management issues.

**Functional Responsibility:** Serves as independent expert or senior member of consulting teams or acts as a task manager or as a project leader on projects of substantial scope and complexity. As a consulting team member or independent expert, collects, analyzes, and interprets data in one or more information technology or management specialties. Develops or participates in the development of assignment methodology.

**Minimum Education:** B.A. or B.S. degree, or equivalent. Masters’ Degree is desirable.

3.17.14 CONSULTANT IV

**Minimum Technical Qualifications/Experience:** At least 10 years of experience in collecting, analyzing, and reporting to solve technical or management issues.

**Functional Responsibility:** Serves as independent expert or senior member of consulting teams or acts as a task manager or as a project leader on projects of substantial scope and complexity. As a consulting team member or independent expert, collects, analyzes, and interprets data in one or
more information technology or management specialties. Develops or participates in the development of assignment methodology.

**Minimum Education:** B.A. or B.S. degree, or equivalent, Masters’ Degree is desirable.

### 3.17.15 PROJECT MANAGER I

**Minimum Technical Qualifications/Experience:** At least five years of experience in managing projects of varying sizes, with two years of specialized IT project management.

**Functional Responsibility:** Leads the project or multiple tasks and retains overall responsibility for performance including cost, schedule, deliverables and overall contractual compliance. Provides the interface to the customer and other project leaders. Identifies, acquires, and utilizes company resources to achieve project technical objectives. Performs staff assignments to meet all project priorities and deadlines. Ensures quality and productivity standards are maintained while meeting project/client deadlines and budget constraints. Supervises the training of new personnel under the project to assure compliance with regulations, standards, policies, and procedures.

**Minimum Education:** B.A. or B.S. degree, or equivalent.

### 3.17.16 SUBJECT MATTER EXPERT

**Minimum Technical Qualifications/Experience:** At least 10 years of highly specialized IT and/or management experience in the required subject matter.

**Functional Responsibility:** Defines and analyzes the problem and develops plans and requirements in the subject matter area to meet client requirements. Coordinates and manages the technical analysis and implementations for the following specialties: Risk, Compliance, and Security; Enterprise Resilience; Information Technology; Program & Project Management; and Intelligence services.

**Minimum Education:** B.A. or B.S. degree. Masters’ Degree is desirable.

### 3.18 SIN 54151S LABOR CATEGORY QUALIFICATION EQUIVALENCIES

Education and experience may be substituted for each other as follows:

<table>
<thead>
<tr>
<th>Education and Years of Experience</th>
<th>Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>High School Diploma + 2 years relevant experience</td>
<td>Associate Degree</td>
</tr>
<tr>
<td>High School Diploma + 4 years relevant experience or Associate Degree + 2 years additional relevant experience</td>
<td>Bachelor's Degree</td>
</tr>
<tr>
<td>Bachelor's Degree + 2 years additional relevant experience</td>
<td>Master's Degree</td>
</tr>
<tr>
<td>Master's Degree + 4 years additional relevant experience</td>
<td>Ph.D.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Degree</th>
<th>Substituted for</th>
<th>Education and Years of Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ph.D.</td>
<td>substituted for</td>
<td>Master's Degree + 4 years relevant experience or Bachelor's Degree + 6 years relevant experience</td>
</tr>
<tr>
<td>Master's Degree</td>
<td>substituted for</td>
<td>Bachelor's Degree + 2 years relevant experience</td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
<td>substituted for</td>
<td>High School Diploma + 4 years relevant experience</td>
</tr>
<tr>
<td>Associate Degree</td>
<td>substituted for</td>
<td>High School Diploma + 2 years relevant experience</td>
</tr>
</tbody>
</table>

Waivers for any labor qualifications listed above may be granted by ordering activity.
SECTION 4.0 TERMS AND CONDITIONS (HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (SINS 54151HACS))

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

- Federal Acquisition Regulation (FAR) Part 52.204-21
- OMB Memorandum M-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

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

****NOTE: All labor categories under the Special Item Number 54151S Information Technology Professional Services may remain under SIN 54151S unless the labor categories are specific to the Highly Adaptive Cybersecurity Services SINs.

4.1 SCOPE

4.1.1 The labor categories, prices, terms and conditions stated under Special Item Numbers 54151HACS High Adaptive Cybersecurity Services (HACS) apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.
4.1.b Services under this SIN is limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on IT Schedule 70 (e.g. 511210 and 33411) and may be quoted along with services to provide a total solution.

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

4.1.d Highly Adaptive Cybersecurity Services provided under this SIN shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

4.1.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.

4.1.f Highly Adaptive Cybersecurity Services (HACS) - SUBJECT TO COOPERATIVE PURCHASING - includes proactive and reactive cybersecurity services that improve the customer’s enterprise-level security posture.

The scope of this category encompasses a wide range of fields that include, but are not limited to, Risk Management Framework (RMF) services, information assurance (IA), virus detection, network management, situational awareness and incident response, secure web hosting, and backup and security services.

The seven-step RMF includes preparation, information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCMMA) that evaluate ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization’s incident management functions.

The scope of this category also includes Security Operations Center (SOC) services. The SOC scope includes services such as: 24x7x365 monitoring and analysis, traffic analysis, incident response and coordination, penetration testing, anti-virus management, intrusion detection and prevention, and information sharing.

HACS vendors are able to identify and protect a customer’s information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge.

Sub-Categories –
- **High Value Asset (HVA)** 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. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing. 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.

- **Risk and Vulnerability Assessment (RVA)** 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. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing.

- **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. Support 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.

- **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.

- **Cyber Hunt** activities respond to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunts start with the premise that threat actors known to target some organizations in a specific industry or with specific systems are likely to also target other organizations in the same industry or with the same systems.

### 4.2 ORDER

4.2.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 that 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.

4.2.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.

### 4.3 PERFORMANCE OF SERVICES

4.3.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.

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

4.3.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.

4.3.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.

4.4 INSPECTION OF SERVICES
Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS – COMMERCIAL ITEMS (JAN 2017) (ALTERNATE I – JAN 2017) for Time-and-Materials and Labor-Hour orders placed under this contract.

4.5 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.

4.6 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.

4.7 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.

4.8 ORGANIZATIONAL CONFLICTS OF INTEREST
4.8.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.

4.8.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.

4.9 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.

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

4.11 APPROVAL OF SUBCONTRACTS
The ordering activity may require that the Contractor receive, from the ordering activity Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

4.12 DESCRIPTION OF HACS SERVICES AND PRICING
The following pages contain a description of categories of HACS services offered along with the corresponding prices.

Table 2: SIN 54151HACS Government Site Hourly Rates

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Labor Category</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Technical Project Lead</td>
<td>$252.69</td>
<td>$258.75</td>
<td>$264.96</td>
<td>$271.32</td>
<td>$277.83</td>
</tr>
<tr>
<td>18</td>
<td>Lead Penetration Tester</td>
<td>$224.62</td>
<td>$230.01</td>
<td>$235.53</td>
<td>$241.18</td>
<td>$246.97</td>
</tr>
<tr>
<td>19</td>
<td>Penetration Tester</td>
<td>$196.54</td>
<td>$201.25</td>
<td>$206.08</td>
<td>$211.03</td>
<td>$216.09</td>
</tr>
<tr>
<td>20</td>
<td>Senior Hunt Analyst</td>
<td>$235.84</td>
<td>$241.50</td>
<td>$247.30</td>
<td>$253.23</td>
<td>$259.31</td>
</tr>
<tr>
<td>21</td>
<td>Hunt Analyst</td>
<td>$190.92</td>
<td>$195.50</td>
<td>$200.20</td>
<td>$205.00</td>
<td>$209.92</td>
</tr>
<tr>
<td>22</td>
<td>RVA SME</td>
<td>$280.77</td>
<td>$287.51</td>
<td>$294.41</td>
<td>$301.47</td>
<td>$308.71</td>
</tr>
<tr>
<td>23</td>
<td>Senior RVA Tester</td>
<td>$197.61</td>
<td>$202.35</td>
<td>$207.21</td>
<td>$212.18</td>
<td>$217.27</td>
</tr>
<tr>
<td>24</td>
<td>RVA Tester</td>
<td>$170.80</td>
<td>$174.90</td>
<td>$179.10</td>
<td>$183.40</td>
<td>$187.80</td>
</tr>
<tr>
<td>25</td>
<td>Incident Response Lead</td>
<td>$205.55</td>
<td>$210.48</td>
<td>$215.53</td>
<td>$220.71</td>
<td>$226.00</td>
</tr>
<tr>
<td>26</td>
<td>Incident Response Senior</td>
<td>$189.33</td>
<td>$193.87</td>
<td>$198.52</td>
<td>$203.29</td>
<td>$208.17</td>
</tr>
<tr>
<td>27</td>
<td>Incident Response Mid</td>
<td>$150.48</td>
<td>$154.09</td>
<td>$157.79</td>
<td>$161.58</td>
<td>$165.46</td>
</tr>
<tr>
<td>28</td>
<td>Incident Response Junior</td>
<td>$102.78</td>
<td>$105.24</td>
<td>$107.77</td>
<td>$110.36</td>
<td>$113.00</td>
</tr>
<tr>
<td>29</td>
<td>HVA Assessment Lead</td>
<td>$210.96</td>
<td>$216.02</td>
<td>$221.21</td>
<td>$226.52</td>
<td>$231.96</td>
</tr>
<tr>
<td>30</td>
<td>HVA Assessment Senior</td>
<td>$178.51</td>
<td>$182.79</td>
<td>$187.18</td>
<td>$191.67</td>
<td>$196.27</td>
</tr>
<tr>
<td>31</td>
<td>HVA Assessment Mid</td>
<td>$151.46</td>
<td>$155.09</td>
<td>$158.82</td>
<td>$162.63</td>
<td>$166.53</td>
</tr>
<tr>
<td>32</td>
<td>HVA Assessment Junior</td>
<td>$129.82</td>
<td>$132.94</td>
<td>$136.13</td>
<td>$139.40</td>
<td>$142.74</td>
</tr>
</tbody>
</table>

*Coalfire Federal applies a fixed escalation rate of 2.4% based on the Bureau of Labor Statistics Employment Cost Index (ECI), Table 5: Compensation – Not Seasonally Adjusted – Employment Cost Index for Total Compensation, for Private Industry Workers, by Occupational Group and Industry.

Note: The rates listed above include the Industrial Funding Fee (IFF).

4.12.a Basic Discount Terms = 1% to 39.78% Rounded 1% to 40%
4.13 SIN 54151HACS LABOR CATEGORY DESCRIPTIONS

4.13.1 TECHNICAL PROJECT LEAD

**Minimum Technical Qualifications/Experience:** Seven (7) years of substantive IT knowledge and demonstrate hands-on expertise and/or training in areas of emerging technologies. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, secure coding practices and/or threat modeling. Will have a strong understanding of penetration testing - especially initial exploitation and post-exploitation phases.

**Functional Responsibility:** Duties include scoping assessments, identification and exploitation of vulnerabilities, writing report, briefing event details to stakeholders and a coordinating remediation.

**Minimum Education:** Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT (or other Penetration Testing certifications), CISSP, or Certified Ethical Hacker.

4.13.2 LEAD PENETRATION TESTER

**Minimum Technical Qualifications/Experience:** Five (5) years of substantive IT knowledge and demonstrate hands-on expertise and/or training in areas of emerging technologies. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, secure coding practices and/or threat modeling. Will have a strong understanding of penetration testing - especially initial exploitation and post-exploitation phases.

**Functional Responsibility:** Duties include scoping assessments, identification and exploitation of vulnerabilities, writing report, briefing event details to stakeholders and a coordinating remediation.

**Minimum Education:** Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT (or other Penetration Testing certifications), CISSP, or Certified Ethical Hacker.

4.13.3 PENETRATION TESTER

**Minimum Technical Qualifications/Experience:** Three (3) years of substantive IT knowledge and demonstrate hands-on expertise and/or training in areas of emerging technologies. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, secure coding practices and/or threat modeling. Will have a strong understanding of penetration testing - especially initial exploitation and post-exploitation phases.

**Functional Responsibility:** Follow industry best practices and methodologies, to perform penetration testing services to uncover vulnerabilities across platforms. Research new threats, attack vectors and risk.

**Minimum Education:** Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT (or other Penetration Testing certifications), CISSP, or Certified Ethical Hacker.

4.13.4 SENIOR HUNT ANALYST

**Minimum Technical Qualifications/Experience:** Five (5) years of experience in cybersecurity. 2–5 years of experience doing network security monitoring.

**Functional Responsibility:** Organizes and leads proactive hunts to identify anomalous activity. Triages and investigates alerts generated from multiple detection technologies and takes action to identify, scope and develop a successful remediation.

**Minimum Education:** Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT (or other Penetration Testing certifications), CISSP, or Certified Ethical Hacker.
4.13.5  HUNT ANALYST

**Minimum Technical Qualifications/Experience:** Three (3) years of experience in cybersecurity. 1–2 years of experience doing network security monitoring.

**Functional Responsibility:** Organizes and leads proactive hunts to identify anomalous activity. Triages and investigates alerts generated from multiple detection technologies and takes action to identify, scope and develop a successful remediation.

**Minimum Education:** Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT (or other Penetration Testing certifications), CISSP, or Certified Ethical Hacker.

4.13.6  RVA SME

**Minimum Technical Qualifications/Experience:** Six (6) years of substantive IT knowledge and demonstrate hands-on expertise and/or training in areas of emerging technologies. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, secure coding practices and/or threat modeling. Will have a strong understanding of penetration testing - especially initial exploitation and post-exploitation phases.

**Functional Responsibility:** Duties include scoping assessments, identification and exploitation of vulnerabilities, writing report, briefing event details to stakeholders and a coordinating remediation.

**Minimum Education:** Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT (or other Penetration Testing certifications), CISSP, or Certified Ethical Hacker.

4.13.7  SENIOR RVA TESTER

**Minimum Technical Qualifications/Experience:** Six (6) years of substantive IT knowledge and demonstrate hands-on expertise and/or training in areas of emerging technologies. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, secure coding practices and/or threat modeling. Will have a strong understanding of penetration testing - especially initial exploitation and post-exploitation phases.

**Functional Responsibility:** Duties include scoping assessments, identification and exploitation of vulnerabilities, writing report, briefing event details to stakeholders and a coordinating remediation.

**Minimum Education:** Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT (or other Penetration Testing certifications), CISSP, or Certified Ethical Hacker.

4.13.8  RVA TESTER

**Minimum Technical Qualifications/Experience:** Three (3) years of substantive IT knowledge and demonstrate hands-on expertise and/or training in areas of emerging technologies. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, secure coding practices and/or threat modeling. Will have a strong understanding of penetration testing - especially initial exploitation and post-exploitation phases.

**Functional Responsibility:** Follow industry best practices and methodologies, to perform penetration testing services to uncover vulnerabilities across platforms. Research new threats, attack vectors and risk.

**Minimum Education:** Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT (or other Penetration Testing certifications), CISSP, or Certified Ethical Hacker.
4.13.9 INCIDENT RESPONSE LEAD

**Minimum Technical Qualifications/Experience:** More than seven (7) years of substantive IT knowledge and demonstrated hands-on expertise and/or training in incident response. Hands-on experience leading analysis and correlation of indicators of compromise, forensics data, malware, log data, and network package captures in order to detect, triage, and/or reconstruct a security incident. Will have experience leading incident containment and eradication of compromised hosts/networks.

**Functional Responsibility:** Duties may include serving as an incident coordinator, identification and triage of a security incident, directing analysis during an incident response, coordinating cross-functionally and with executive stakeholders, and leading a team during execution of an incident response.

**Minimum Education:** Bachelor’s Degree or equivalent. Must have one of the following certifications: OSCP, OSCE, GIAC GREM, GIAC GCIH or comparable certification.

4.13.10 INCIDENT RESPONDER SENIOR

**Minimum Technical Qualifications/Experience:** More than four (4) years of substantive IT knowledge and demonstrated hands-on expertise and/or training in incident response. Hands-on experience performing analysis and correlation of indicators of compromise, forensics data, malware, log data, and network package captures in order to detect, triage, and/or reconstruct a security incident. Will have experience with incident containment and eradication of compromised hosts/networks.

**Functional Responsibility:** Duties may include scoping response activities, identification and triage of incident related indicators of compromise, analysis of malware and incident related data, report writing, and performing research on cyber threat intelligence in order to help enrich an incident investigation or aid in post-incident mitigations.

**Minimum Education:** Bachelor’s Degree or equivalent. Must have one of the following certifications: OSCP, OSCE, GIAC GREM, GIAC GCIH or comparable certification.

4.13.11 INCIDENT RESPONDER MID

**Minimum Technical Qualifications/Experience:** More than two (2) years of substantive IT knowledge and demonstrated hands-on expertise and/or training in incident response. Hands-on experience performing analysis and correlation of indicators of compromise, forensics data, malware, log data, and/or network package captures in order to detect, triage, and/or reconstruct a security incident. Will have experience with incident containment and eradication of compromised hosts/networks.

**Functional Responsibility:** Duties may include identification and triage of incident related indicators of compromise, analysis of malware and incident related data, report writing, and performing research on cyber threat Intelligence in order to help enrich an incident investigation or aid in post-incident mitigations.

**Minimum Education:** Bachelor’s Degree or equivalent. Must have one of the following certifications: Security+, Network+, CEH or comparable certification.

4.13.12 INCIDENT RESPONDER JR

**Minimum Technical Qualifications/Experience:** Substantive IT knowledge and demonstrated hands-on expertise and/or training in incident response. Will have knowledge of performing analysis and correlation of indicators of compromise, forensics data, malware, log data, and/or
network package captures in order to detect, triage, and/or reconstruct a security incident. Will have experience with incident containment and eradication of compromised hosts/networks. There is no minimum number of years of experience required.

**Functional Responsibility:** Duties may include identification of incident related indicators of compromise, analysis of malware and incident related data, report writing, and performing research on cyber threat intelligence in order to help enrich an incident investigation or aid in post-incident mitigations.

**Minimum Education:** Bachelor’s Degree or equivalent. Must have one of the following certifications: Security+, Network+, CEH or comparable certification.

4.13.13 HVA ASSESOR LEAD

**Minimum Technical Qualifications/Experience:** More than seven (7) years of substantive IT knowledge and demonstrated hands-on expertise leading penetration testing and vulnerability assessment related to HVAs. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, and secure coding practices. Will have experience working with agencies to perform high value asset identification and threat modeling.

**Functional Responsibility:** Working with agency executive stakeholders to understand high value asset protections and mitigations in place. Leading research to understand what tactics techniques and procedures (TTPs) real-world threat actors may employ against an agency or HVA. Design and lead the execution of cyber exercises in order to evaluate the HVA protections in place and in order to help recommend further security enhancements in order to protect HVAs.

**Minimum Education:** Bachelor’s Degree or equivalent. Must have one of the following certifications: OSCP, OSCE, GIAC GPEN, GWAPT or comparable certification.

4.13.14 HVA ASSESOR SENIOR

**Minimum Technical Qualifications/Experience:** More than four (4) years of substantive IT knowledge and demonstrated hands-on expertise performing penetration testing and vulnerability assessment related to HVAs. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, and secure coding practices. Will have experience working with agencies to perform high value asset identification and threat modeling.

**Functional Responsibility:** Performing research to understand what tactics techniques and procedures (TTPs) real-world threat actors may employ against an agency or HVA. Performing cyber exercises in order to evaluate the HVA protections in place and in order to help recommend further security enhancements in order to protect HVAs.

**Minimum Education:** Bachelor’s Degree or equivalent. Must have one of the following certifications: OSCP, OSCE, GIAC GPEN, GWAPT or comparable certification.

4.13.15 HVA ASSESOR MID

**Minimum Technical Qualifications/Experience:** More than two (2) years of substantive IT knowledge and demonstrated hands-on expertise performing penetration testing and vulnerability assessment related to HVAs. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, and/or secure coding practices. Will have experience working with agencies to perform high value asset identification and threat modeling.

**Functional Responsibility:** Performing research to understand what tactics techniques and procedures (TTPs) real-world threat actors may employ against an agency or HVA. Performing
cyber exercises in order to evaluate the HVA protections in place and in order to help identify further security enhancements in order to protect HVAs.

**Minimum Education:** Bachelor’s Degree or equivalent. Must have one of the following certifications: Security+, Network+, CEH or comparable certification.

4.13.16 **HVA ASSESOR JUNIOR**

**Minimum Technical Qualifications/Experience:** Substantive IT knowledge and demonstrated hands-on expertise performing penetration testing and vulnerability assessment related to HVAs. Will have hands-on experience and expertise with ethical hacking, firewall and intrusion detection/prevention technologies, and/or secure coding practices. Will have experience working with agencies to perform high value asset identification and threat modeling. There is no minimum number of years of experience required.

**Functional Responsibility:** Performing research to understand what tactics techniques and procedures (TTPs) real-world threat actors may employ against an agency or HVA. Performing cyber exercises in order to evaluate the HVA protections in place.

**Minimum Education:** Bachelor’s Degree or equivalent. Must have one of the following certifications: Security+, Network+, CEH or comparable certification.

Waivers for any labor qualifications listed above may be granted by ordering activity.
SECTION 5.0 USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS

5.1 PREAMBLE
Coalfire Federal 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.

5.2 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 ensure 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.

Point of Contact: William E. Malone
Title: President
Tel: 571-392-5071
Fax: 703-880-7590
Email: william.malone@coalfirefederal.com
SECTION 6.0 BLANKET PURCHASE AGREEMENT

(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 Schedule Contract(s) ____________.

Federal Supply 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 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

Ordering Activity ____________ Date ____________

Contractor ____________ Date ____________
BPA NUMBER _________________

(Customer Name)

Blanket Purchase Agreement

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

1.0 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>
</tbody>
</table>

2.0 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>

3.0 The ordering activity estimates, but does not guarantee, that the volume of purchases through this agreement will be ________.

4.0 This BPA does not obligate any funds.

5.0 This BPA expires on ___________ or at the end of the contract period, whichever is earlier.

6.0 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>

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

8.0 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.

9.0 The requirements of a proper invoice are specified in the Federal Supply Schedule contract. Invoices will be submitted to the address specified within the purchase order transmission issued against this BPA.
10.0 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.
Basic Guidelines for Using “Contractor Team Agreements”

Federal Supply Schedule Contractors may use “Contractor Team Arrangements” (see FAR 9.6) to provide solutions when responding to an ordering activity requirements. These Team Arrangements can be included under a Blanket Purchase Agreement (BPA). BPAs are permitted under all Federal Supply Schedule contracts. Orders under a Team Arrangement are subject to terms and conditions or the Federal Supply Schedule Contract.

Participation in a Team Arrangement is limited to Federal Supply Schedule Contractors. Customers should refer to FAR 9.6 for specific details on Team Arrangements.

Here is a general outline on how it works:

- The customer identifies their requirements.
- Federal Supply Schedule Contractors may individually meet the customer’s needs, or -
- Federal Supply Schedule Contractors may individually submit a Schedules “Team Solution” to meet the customer’s requirement.
- Customers make a best value selection.
SECTION 7.0 ORDER-LEVEL MATERIALS

a) Order-Level Materials (OLMs) are supplies and/or services acquired in direct support of an individual task or delivery order placed against a Federal Supply Schedule (FSS) contract or FSS blanket purchase agreement (BPA). OLMs are not defined, priced, or awarded at the FSS contract level. They are unknown before a task or delivery order is placed against the FSS contract or FSS BPA. OLMs are only authorized for inclusion at the order level under a Time-and-Materials (T&M) or Labor-Hour (LH) Contract Line Item Number (CLIN) and are subject to a Not-To-Exceed (NTE) ceiling price. OLMs include direct materials, subcontracts for supplies and incidental services for which there is not a labor category specified in the FSS contract, other direct costs (separate from those under ODC SINs), and indirect costs. OLMs are purchased under the authority of the FSS Program and are not “open market items.”

b) Items awarded under ancillary supplies/services or other direct cost (ODC) SINs are not OLMs. These items are defined, priced, and awarded at the FSS contract level, whereas OLMs are unknown before an order is placed. Ancillary supplies/services and ODC SINs are for use under all order type CLINs (Fixed Price (FP), T&M, and LH), whereas the Order-Level Materials SIN is only authorized for use under T&M and LH order CLINs. The Order-Level Materials SIN is only authorized for use in direct support of another awarded SIN. Price analysis for OLMs is not conducted when awarding the FSS contract or FSS BPA; therefore, GSAR 538.270 and 538.271 do not apply to OLMs. OLMs are defined and priced at the ordering activity level in accordance with GSAR clause 552.238-115 Special Ordering Procedures for the Acquisition of Order-Level Materials. Prices for items provided under the Order-Level Materials SIN must be inclusive of the Industrial Funding Fee (IFF). The cumulative value of OLMs in an individual task or delivery order cannot exceed 33.33% of the total value of the order.

c) The Maximum Order Threshold for the OLM SINs is $100,000.

d) See clauses 552.212-4 Contract Terms and Conditions - Commercial Items and 552.238-115 Special Ordering Procedures for the Acquisition of Order-Level Materials for additional information on inclusion of OLMs in task and delivery orders placed against an FSS contract or BPA.

e) OLMs are only authorized for inclusion at the order level under a T&M or LH CLIN and are subject to an NTE ceiling price.

f) The Order-Level Materials SIN contains no items or pricing, since by definition OLMs are unknown at the time of FSS contract award. The ordering activity contracting officer is responsible for defining OLMs and determining proposed OLM pricing fair and reasonable for a particular order.

g) OLMs are purchased under the authority of the FSS Program and are not “open market items.”

h) Items awarded under ancillary supplies/services and other direct cost (ODC) SINs are not Order-Level Materials. These SINs are reserved for items that can be defined and priced up-front at the FSS contract level.

i) The Order-Level Materials SIN cannot be the only SIN awarded on a contract. The Order-Level Materials SIN is only authorized for use in direct support of another awarded SIN.

j) The Order-Level Materials SIN is exempt from Commercial Sales Practices disclosure requirements.

k) The Order-Level Materials SIN is exempt from the following clauses:
   - 552.216-70 Economic Price Adjustment - FSS Multiple Award Schedule Contracts
   - I-FSS-969 Economic Price Adjustment - FSS Multiple Award Schedule
   - 552.238-71 Submission and Distribution of Authorized FSS Schedule Pricelists, 552.238-75 Price Reductions.
l) Terms and conditions that otherwise apply to the FSS contract also apply to the Order-Level Materials SIN. Examples include but are not limited to:
   - Trade Agreements Act (TAA)
   - Sales reporting and IFF remittance
   - Environmental Attributes clauses
   - AbilityOne Program Essentially the Same (ETS) compliance

m) The Order-Level Materials SIN is subject to any transactional data reporting (TDR) requirements in effect under the FSS contract.

n) Prices for items provided under the Order-Level Materials SIN must be inclusive of the IFF. The cumulative value of OLMs in an individual task or delivery order cannot exceed 33.33% of the total value of the order.