GENERAL SERVICES ADMINISTRATION

Federal Supply Service

Authorized Federal Supply Schedule Price List

On-line 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 GSA Advantage!® is: GSAAdvantage.gov.

Multiple Award Schedule

FSC Group: Federal Supply Group: Professional Services

FSC Class: D399 and 7030

Contract number: 47QTCA19D002K

Contract period: November 30, 2018 – November 29, 2023

CAE USA Mission Solutions Inc.
4908 Tampa West Blvd.
Tampa, FL 33634
Phone: (757) 224-3716
Fax: (757) 224-6191

Web: https://cae.com/cae-usa/cae-usa-msi/

Contract Administrator: Kerry Kuykendall
Email: kerry.kuykendall@caemilusa.com
Phone: (757) 378-5315

Business size: Large

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

Price list current as of Modification #PA-0013 effective December 29, 2021

Prices Shown Herein are Net (discount deducted)
## CUSTOMER INFORMATION

1a. Table of awarded special item number(s) with appropriate cross-reference to item descriptions and awarded price(s).

<table>
<thead>
<tr>
<th>SINs</th>
<th>SIN Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OLM</td>
<td>Order-Level Materials – Subject to Cooperative Purchasing</td>
</tr>
<tr>
<td>511210</td>
<td>Term Software – Subject to Cooperative Purchasing</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS) – Subject to Cooperative Purchasing</td>
</tr>
</tbody>
</table>

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply.

<table>
<thead>
<tr>
<th>Special Item Number</th>
<th>Product/Service</th>
<th>GSA Price with IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>511210</td>
<td>SimSpaceCyberRange–CH-Team-250</td>
<td>$299,244.33</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Project Manager/Team Leader</td>
<td>$95.95 per hour</td>
</tr>
</tbody>
</table>

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate “Not applicable” for this item.

<table>
<thead>
<tr>
<th>Manufacturer Name</th>
<th>Location of Software</th>
<th>Manufacturer Part Number</th>
<th>GSA Price with IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>SimSpace Corporation</td>
<td>Customer’s Site</td>
<td>SimSpaceCyberRange-CH-Team250</td>
<td>$299,244.33</td>
</tr>
<tr>
<td>SimSpace Corporation</td>
<td>Customer’s Site</td>
<td>SimSpaceCyberRange-CH-Team500</td>
<td>$598,488.66</td>
</tr>
<tr>
<td>SimSpace Corporation</td>
<td>Customer’s Site</td>
<td>SimSpaceCyberRange-CH-Team750</td>
<td>$897,733.00</td>
</tr>
<tr>
<td>SimSpace Corporation</td>
<td>Customer’s Site</td>
<td>SimSpaceCyberRange-CH-Team1000</td>
<td>$1,196,977.33</td>
</tr>
<tr>
<td>SimSpace Corporation</td>
<td>SimSpace’s Site</td>
<td>SimSpaceCyberRange-CH-Team250</td>
<td>$473,803.53</td>
</tr>
<tr>
<td>SimSpace Corporation</td>
<td>SimSpace’s Site</td>
<td>SimSpaceCyberRange-CH-Team500</td>
<td>$947,607.05</td>
</tr>
<tr>
<td>SimSpace Corporation</td>
<td>SimSpace’s Site</td>
<td>SimSpaceCyberRange-CH-Team750</td>
<td>$1,421,410.58</td>
</tr>
<tr>
<td>SimSpace Corporation</td>
<td>SimSpace’s Site</td>
<td>SimSpaceCyberRange-CH-Team1000</td>
<td>$1,895,214.11</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Expert/Specialized Consultant Level 1</td>
<td>$287.85</td>
<td>$293.61</td>
<td>$299.48</td>
</tr>
<tr>
<td>Expert/Specialized Consultant Level 2</td>
<td>$191.90</td>
<td>$195.74</td>
<td>$199.65</td>
</tr>
<tr>
<td>Expert/Specialized Consultant Level 3</td>
<td>$167.91</td>
<td>$171.27</td>
<td>$174.70</td>
</tr>
<tr>
<td>Expert/Specialized Consultant Level 4</td>
<td>$143.93</td>
<td>$146.80</td>
<td>$149.74</td>
</tr>
<tr>
<td>Program Manager</td>
<td>$167.91</td>
<td>$171.27</td>
<td>$174.70</td>
</tr>
<tr>
<td>Deputy Program Manager</td>
<td>$119.94</td>
<td>$122.34</td>
<td>$124.78</td>
</tr>
<tr>
<td>Project Manager/Team Leader</td>
<td>$95.95</td>
<td>$97.87</td>
<td>$99.83</td>
</tr>
<tr>
<td>Senior Cybersecurity/Information Technology (IT) Engineer</td>
<td>$191.90</td>
<td>$195.74</td>
<td>$199.65</td>
</tr>
<tr>
<td>Cybersecurity/Information Technology (IT) Engineer</td>
<td>$143.93</td>
<td>$146.80</td>
<td>$149.74</td>
</tr>
<tr>
<td>Senior Systems Engineer</td>
<td>$191.90</td>
<td>$195.74</td>
<td>$199.65</td>
</tr>
<tr>
<td>Systems Engineer</td>
<td>$143.93</td>
<td>$146.80</td>
<td>$149.74</td>
</tr>
</tbody>
</table>

2. Maximum order: $1,000,000

3. Minimum order: $100

4. Geographic coverage (delivery area). Domestic

5. Point(s) of production (city, county, and State or foreign country). SimSpace Corporation Software products: Boston, MA (USA)

6. Discount from list prices or statement of net price. Government Net Prices (discounts already deducted.)

7. Quantity discounts. None

8. Prompt payment terms. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions. Net 30 days

9. Foreign items (list items by country of origin). Not Applicable

10a. Time of delivery. (Contractor insert number of days.) To Be Determined at the Task Order level

10b. Expedited Delivery. Items available for expedited delivery are noted in this price list. To Be Determined at the Task Order level

10c. Overnight and 2-day delivery. To Be Determined at the Task Order level
10d. Urgent Requirements. To Be Determined at the Task Order level

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

12a. Ordering address(es). CAE USA Mission Solutions Inc.
4908 Tampa West Blvd.
Tampa, FL 33634
Phone: (757) 224-3716
Fax: (757) 224-6191
E-mail: kerry.kuykendall@caemilusa.com

12b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA’s) are found in Federal Acquisition Regulation (FAR) 8.405-3.

13. Payment address(es). Bank of America Lockbox Services
CAE USA Mission Solutions Inc.
PO Box 74007429
Chicago, IL 60674-7429

14. Warranty provision. SimSpace Corporation: Standard Commercial Warranty passes through to the Ordering Activity

15. Export packing charges, if applicable. Not Applicable

16. Terms and conditions of rental, maintenance, and repair (if applicable). Not Applicable

17. Terms and conditions of installation (if applicable). Not Applicable

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). Not Applicable

18b. Terms and conditions for any other services (if applicable). Not Applicable

19. List of service and distribution points (if applicable). Not Applicable

20. List of participating dealers (if applicable). Not Applicable

21. Preventive maintenance (if applicable). Not Applicable

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). Not Applicable

22b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor’s website or other location.) The EIT standards can be found at: www.Section508.gov/. Not Applicable
23. Unique Entity Identifier (UEI) number. EB7FJB3QNIN8

24. Notification regarding registration in System for Award Management (SAM) database. Contractor registered and active in SAM

**Service Contract Labor Standards:** The Service Contract Labor Standards (SCLS), formerly known as the Service Contract Act (SCA), is applicable to this contract as it applies to the entire Multiple Award Schedule (MAS) and all services provided. While no specific labor categories have been identified as being subject to SCLS/SCA due to exemptions for professional employees (FAR 22.1101, 22.1102 and 29 CRF 541.300), this contract still maintains the provisions and protections for SCLS/SCA eligible labor categories. If and/or when the contractor adds SCLS/SCA labor categories to the contract through the modification process, the contractor must inform the Contracting Officer and establish a SCLS/SCA matrix identifying the GSA labor category titles, the occupational code, SCLS/SCA labor category titles and the applicable WD number. Failure to do so may result in cancellation of the contract.
1. INSPECTION/ACCEPTANCE

The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The ordering activity reserves the right to inspect or test any software that has been tendered for acceptance. The ordering activity may require repair or replacement of nonconforming software at no increase in contract price. The ordering activity must exercise its post acceptance rights (1) within a reasonable time after the defect was discovered or should have been discovered; and (2) before any substantial change occurs in the condition of the software, unless the change is due to the defect in the software.

2. ENTERPRISE USER LICENSE AGREEMENTS REQUIREMENTS (EULA)

The Contractor shall provide all Enterprise User License Agreements in an editable Microsoft Office (Word) format.

3. GUARANTEE/WARRANTY

a. Unless specified otherwise in this contract, the Contractor’s standard commercial guarantee/warranty as stated in the contract’s commercial pricelist will apply to this contract.

b. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract. If no implied warranties are given, an express warranty of at least 60 days must be given in accordance with FAR 12.404(b) (2).

c. Limitation of Liability. Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.

4. TECHNICAL SERVICES

The Contractor, without additional charge to the ordering activity, has provided (757) 224-3716 as the hot line technical support number for the purpose of providing user assistance and guidance in the implementation of the software. The technical support number is available Monday – Friday, 8 am to 5 pm Eastern.

5. SOFTWARE MAINTENANCE

a. Software maintenance as it is defined: (select software maintenance type):

(1) Software Maintenance as a Product (SIN 511210) Software maintenance as a product includes the publishing of bug/defect fixes via patches and updates/upgrades in function and technology to maintain the operability and usability of the software product. It may also include other no charge support that is included in the purchase price of the product in the commercial marketplace. No charge support includes items such as user blogs, discussion forums, on-line help libraries and
FAQs (Frequently Asked Questions), hosted chat rooms, and limited telephone, email and/or web-based general technical support for user’s self- diagnostics. Software maintenance as a product does NOT include the creation, design, implementation, integration, etc. of a software package. These examples are considered software maintenance as a service. Software Maintenance as a product is billed at the time of purchase.

(2) Software Maintenance as a Service (SIN 54151) Software maintenance as a service creates, designs, implements, and/or integrates customized changes to software that solve one or more problems and is not included with the price of the software. Software maintenance as a service includes person-to- person communications regardless of the medium used to communicate: telephone support, online technical support, customized support, and/or technical expertise which are charged commercially. Software maintenance as a service is billed arrears in accordance with 31 U.S.C. 3324.

Software maintenance as a service is billed in arrears in accordance with 31 U.S.C. 3324.

b. Invoices for maintenance service shall be submitted by the Contractor on a quarterly or monthly basis, after the completion of such period. Maintenance charges must be paid in arrears (31 U.S.C. 3324). PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.

6. PERIODS OF TERM LICENSES (SIN 511210)

a. The Contractor shall honor orders for periods for the duration of the contract period or a lessor period of time.

b. Term licenses may be discontinued by the ordering activity on thirty (30) calendar days written notice to the Contractor.

c. Annual Funding. When annually appropriated funds are cited on an order for term licenses, the period of the term licenses shall automatically expire on September 30 of the contract period, or at the end of the contract period, whichever occurs first. Renewal of the term licenses orders citing the new appropriation shall be required, if the term license is to be continued during any remainder of the contract period.

d. Cross-Year Funding Within Contract Period. Where an ordering activity’s specific appropriation authority provides for funds in excess of a 12 month (fiscal year) period, the ordering activity may place an order under this schedule contract for a period up to the expiration of the contract period, notwithstanding the intervening fiscal years.

e. Ordering activities should notify the Contractor in writing thirty (30) calendar days prior to the expiration of an order, if the term license is to be terminated at that time. Orders for the continuation of a term license will be required if the term license is to be continued during the subsequent period.

7. CONVERSION FROM TERM LICENSE TO PERPETUAL LICENSE

a. The ordering activity may convert term licenses to perpetual licenses for any or all software at any time following acceptance of software. At the request of the ordering activity the Contractor shall furnish, within ten (10) calendar days, for each software product that is contemplated for conversion,
the total amount of conversion credits which have accrued while the software was on a term license and the date of the last update or enhancement.

b. Conversion credits which are provided shall, within the limits specified, continue to accrue from one contract period to the next, provided the software remains on a term license within the ordering activity.

c. The term license for each software product shall be discontinued on the day immediately preceding the effective date of conversion from a term license to a perpetual license.

d. The price the ordering activity shall pay will be the perpetual license price that prevailed at the time such software was initially ordered under a term license, or the perpetual license price prevailing at the time of conversion from a term license to a perpetual license, whichever is the less, minus an amount equal to % of all term license payments during the period that the software was under a term license within the ordering activity.

Not Applicable

8. TERM LICENSE CESSION

a. After a software product has been on a continuous term license for a period of * months, a fully paid-up, non-exclusive, perpetual license for the software product shall automatically accrue to the ordering activity. The period of continuous term license for automatic accrual of a fully paid-up perpetual license does not have to be achieved during a particular fiscal year; it is a written Contractor commitment which continues to be available for software that is initially ordered under this contract, until a fully paid-up perpetual license accrues to the ordering activity. However, should the term license of the software be discontinued before the specified period of the continuous term license has been satisfied, the perpetual license accrual shall be forfeited.

b. The Contractor agrees to provide updates and maintenance service for the software after a perpetual license has accrued, at the prices and terms of Special Item Number 54151, if the licensee elects to order such services. Title to the software shall remain with the Contractor.

Not Applicable

9. UTILIZATION LIMITATIONS - (SIN 511210)

a. Software acquisition is limited to commercial computer software defined in FAR Part 2.101.

b. When acquired by the ordering activity, commercial computer software and related documentation so legend shall be subject to the following:

(1) Title to and ownership of the software and documentation shall remain with the Contractor, unless otherwise specified.

(2) Software licenses are by site and by ordering activity. An ordering activity is defined as a cabinet level or independent ordering activity. The software may be used by any subdivision of the ordering activity (service, bureau, division, command, etc.) that has access to the site the software is placed at, even if the subdivision did not participate in the acquisition of the software.
Further, the software may be used on a sharing basis where multiple agencies have joint projects that can be satisfied by the use of the software placed at one ordering activity's site. This would allow other agencies access to one ordering activity's database. For ordering activity public domain databases, user agencies and third parties may use the computer program to enter, retrieve, analyze and present data. The user ordering activity will take appropriate action by instruction, agreement, or otherwise, to protect the Contractor's proprietary property with any third parties that are permitted access to the computer programs and documentation in connection with the user ordering activity's permitted use of the computer programs and documentation. For purposes of this section, all such permitted third parties shall be deemed agents of the user ordering activity.

(3) Except as is provided in paragraph 8.b(2) above, the ordering activity shall not provide or otherwise make available the software or documentation, or any portion thereof, in any form, to any third party without the prior written approval of the Contractor. Third parties do not include prime Contractors, subcontractors and agents of the ordering activity who have the ordering activity's permission to use the licensed software and documentation at the facility, and who have agreed to use the licensed software and documentation only in accordance with these restrictions. This provision does not limit the right of the ordering activity to use software, documentation, or information therein, which the ordering activity may already have or obtains without restrictions.

(4) The ordering activity shall have the right to use the computer software and documentation with the computer for which it is acquired at any other facility to which that computer may be transferred, or in cases of Disaster Recovery, the ordering activity has the right to transfer the software to another site if the ordering activity site for which it is acquired is deemed to be unsafe for ordering activity personnel; to use the computer software and documentation with a backup computer when the primary computer is inoperative; to copy computer programs for safekeeping (archives) or backup purposes; to transfer a copy of the software to another site for purposes of benchmarking new hardware and/or software; and to modify the software and documentation or combine it with other software, provided that the unmodified portions shall remain subject to these restrictions.

(5) "Commercial Computer Software" may be marked with the Contractor's standard commercial restricted rights legend, but the schedule contract and schedule pricelist, including this clause, "Utilization Limitations" are the only governing terms and conditions, and shall take precedence and supersede any different or additional terms and conditions included in the standard commercial legend.

10. SOFTWARE CONVERSIONS - (SIN 511210)

Full monetary credit will be allowed to the ordering activity when conversion from one version of the software to another is made as the result of a change in operating system, or from one computer system to another. Under a term license (51210), conversion credits which accrued while the earlier version was under a term license shall carry forward and remain available as conversion credits which may be applied towards the perpetual license price of the new version.

11. DESCRIPTIONS AND EQUIPMENT COMPATIBILITY
The Contractor shall include, in the schedule pricelist, a complete description of each software product and a list of equipment on which the software can be used. Also, included shall be a brief, introductory explanation of the modules and documentation which are offered.

12. RIGHT-TO-COPY PRICING

The Contractor shall insert the discounted pricing for right-to-copy licenses.
Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Federal Acquisition Regulation (FAR) Part 52.204-21
- OMB Memorandum M-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memorandum M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- OMB Memorandum M-16-03 - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- OMB Memorandum M-16-04 – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
- NIST SP 800-44 - 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

1. SCOPE
a. The labor categories, prices, terms and conditions stated under Special Item Number 54151HACS Highly Adaptive Cybersecurity Services (HACS) apply exclusively to Highly Adaptive Cybersecurity Services within the scope of this Multiple Award Schedule.

b. Services under this SIN are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on the MAS Schedule (e.g. 511210, 33411), and may be quoted along with services to provide a total solution.

c. This SIN provides ordering activities with access to Highly Adaptive Cybersecurity services only.

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.

e. SCOPE:

54151HACS -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 (ISCMA) which evaluate organization-wide 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 - (not all vendors have been placed within the following subcategories. To view a complete list of vendors, click on the SIN)

- 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.
- 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.
- 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.
- 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.

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

2. ORDER

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

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

3. PERFORMANCE OF SERVICES

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

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

c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor’s travel.

4. INSPECTION OF SERVICES

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

5. RESPONSIBILITIES OF THE CONTRACTOR

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

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

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

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

7. INDEPENDENT CONTRACTOR

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

8. ORGANIZATIONAL CONFLICTS OF INTEREST

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

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

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

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

9. INVOICES

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

10. RESUMES

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

11. APPROVAL OF SUBCONTRACTS

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

12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Number 54151HACS for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.
b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.
LABOR CATEGORY DESCRIPTIONS

Expert/Specialized Consultant Level 1

Description: Considered a leading expert in the cybersecurity/information technology field.

Persons involved in this specialty perform the following tasks: Provides lead analysis for translating customer needs into usable products, plans or implementation plans. Provides leadership or direction on innovative research associated with project execution. Performs management responsibilities for a program or staff for assigned projects. Provides in-depth analysis on network interoperability, topologies, technologies, interfaces, and protocols. May perform other duties as required.

Knowledge, Skills and Abilities: Possesses the capability to direct, design, or develop plans, implementation or cutover plans, integration plans, or interoperability plans based on different cybersecurity/information technology environments. Has the ability to use experience and technical judgment to reach conclusions in the face of limited and/or uncertain data. Capable of supervising multiple teams of specialty individuals working on highly complex projects.

Minimum Experience: Ten (10) years of general work experience in cybersecurity/information technology field. Has broad, high-level knowledge and experience relevant to the cybersecurity/information technology task being performed.

Minimum Education Requirements: Ph.D. or Doctorate Degree in a relevant field.

Highly Desirable: Industry certifications in relevant field.

<table>
<thead>
<tr>
<th>Substitutions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
<td>Experience</td>
</tr>
<tr>
<td>Master’s Degree</td>
<td>12 years of general work experience in cybersecurity/information technology field</td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
<td>14 years of general work experience in cybersecurity/information technology field</td>
</tr>
</tbody>
</table>

Expert/Specialized Consultant Level 2

Description: Considered an expert in the cybersecurity/information technology field.

Persons involved in this specialty perform the following tasks: Provides lead analysis for translating customer needs into usable products, plans or implementation plans. Provides leadership or direction on innovative research associated with project execution. Performs management responsibilities for a program or staff for assigned projects. Provides in-depth analysis on network interoperability, topologies, technologies, interfaces, and protocols. May perform other duties as required.
Knowledge, Skills and Abilities: Possesses the capability to direct, design, or develop plans, implementation or cutover plans, integration plans, or interoperability plans based on different cybersecurity/information technology environments. Has the ability to use experience and technical judgment to reach conclusions in the face of limited and/or uncertain data. Capable of supervising multiple teams of specialty individuals working on highly complex projects.

Minimum Experience: Eight (8) years of general work experience in cybersecurity/information technology field. Has broad, high-level knowledge and experience relevant to the cybersecurity/information technology task being performed.

Minimum Education Requirements: Master’s Degree in a relevant field.

Highly Desirable: Industry certifications in relevant field.

<table>
<thead>
<tr>
<th>Substitutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
</tr>
</tbody>
</table>

Expert/Specialized Consultant Level 3

Description: Highly knowledgeable in the cybersecurity/information technology field.

Persons involved in this specialty perform the following tasks: Provides analysis for translating customer needs into usable products, plans or implementation plans. Provides support on innovative research associated with project execution. Provides analysis on network interoperability, topologies, technologies, interfaces, and protocols. May perform other duties as required.

Knowledge, Skills and Abilities: Possesses the capability to support the design or development of plans, implementation or cutover plans, integration plans, or interoperability plans based on different cybersecurity/information technology environments.

Minimum Experience: Four (4) years of general work experience in cybersecurity/information technology field. Has broad, high-level knowledge and experience relevant to the cybersecurity/information technology task being performed.

Minimum Education Requirements: Bachelor’s Degree in a relevant field.

Highly Desirable: Industry training in relevant field.
<table>
<thead>
<tr>
<th>Substitutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Education</strong></td>
</tr>
<tr>
<td>Master’s Degree</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
</tr>
</tbody>
</table>

**Expert/Specialized Consultant Level 4**

**Description:** Knowledgeable in the cybersecurity/information technology field.

**Persons involved in this specialty perform the following tasks:** Provides analysis for translating customer needs into usable products, plans or implementation plans. Provides support on innovative research associated with project execution. Provides analysis on network interoperability, topologies, technologies, interfaces, and protocols. May perform other duties as required.

**Knowledge, Skills and Abilities:** Possesses the capability to support the design or development of plans, implementation or cutover plans, integration plans, or interoperability plans based on different cybersecurity/information technology environments.

**Minimum Experience:** Zero (0) years of general work experience in cybersecurity/information technology field. Has broad, high-level knowledge and experience relevant to the cybersecurity/information technology task being performed.

**Minimum Education Requirements:** Bachelor’s Degree in a relevant field.

**Highly Desirable:** Industry training in relevant field.

<table>
<thead>
<tr>
<th>Substitutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Education</strong></td>
</tr>
<tr>
<td>Master’s Degree</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
</tr>
</tbody>
</table>

**Program Manager**

**Description:** Knowledgeable in the management of cybersecurity/information technology activities.

**Persons involved in this specialty perform the following tasks:** Plans, directs, coordinates, and controls technical and administrative activities of designated projects to ensure goals or objectives are accomplished within prescribed time frame and funding parameters. Supervises project managers in accomplishing assigned tasks. Reviews and maintains the quality of work performed on the project. Makes administrative judgments and provides advice on resolving problems. Coordinates project activities with activities of government regulatory or other governmental agencies. In the absence of the
Cybersecurity Specialist, the Program Manager will support cybersecurity engineering functions and technical task completion.

**Knowledge, Skills and Abilities:** Provides management and technical direction to program managers or other program or project personnel. Regularly exercises independent judgment as well as a high level of analytical skill in solving complex and unusual technical and cybersecurity program execution problems. Establishes work plan and staffing for each phase of project, and arranges for recruitment or assignment of project personnel. Ultimately responsible for project planning, execution, and performance. Serves as counterpart to Government Senior Agency, Program, or Project Manager. Demonstrates extensive subject matter expertise and communication skills to interface with all levels of management.

**Minimum Experience:** Minimum eight (8) years of experience including supervisory or management experience. Specific experience areas include requirements definition, work planning, control of budget, schedule, and task execution, and personnel management and supervision.

**Minimum Education Requirements:** Master’s Degree in a relevant field.

**Highly Desirable:** Project Management Professional (PMP) certification.

<table>
<thead>
<tr>
<th>Substitutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
</tr>
</tbody>
</table>

**Deputy Program Manager**

**Description:** Knowledgeable in the management of cybersecurity/information technology activities.

**Persons involved in this specialty perform the following tasks:** Plans, directs, coordinates, and controls technical and administrative activities of designated projects to ensure goals or objectives are accomplished within prescribed time frame and funding parameters. Supervises project managers in accomplishing assigned tasks. Reviews and maintains the quality of work performed on the project. Makes administrative judgments and provides advice on resolving problems. Coordinates project activities with activities of government regulatory or other governmental agencies. In the absence of the Cybersecurity Specialist, the Program Manager will support cybersecurity engineering functions and technical task completion.

**Knowledge, Skills and Abilities:** Provides management and technical direction to program managers or other program or project personnel. Regularly exercises independent judgment as well as a high level of analytical skill in solving complex and unusual technical and cybersecurity program execution problems. Establishes work plan and staffing for each phase of project, and arranges for recruitment or assignment of project personnel. Ultimately responsible for project planning, execution, and performance. Serves as counterpart to Government Senior Agency, Program, or Project Manager.
Demonstrates extensive subject matter expertise and communication skills to interface with all levels of management.

**Minimum Experience:** Minimum four (4) years of experience including supervisory or management experience. Specific experience areas include requirements definition, work planning, control of budget, schedule, and task execution, and personnel management and supervision.

**Minimum Education Requirements:** Bachelor’s Degree in a relevant field.

**Highly Desirable:** Project Management Professional (PMP) certification.

<table>
<thead>
<tr>
<th>Substitutions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Education</strong></td>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td>Master’s Degree</td>
<td>2 years of general work experience in cybersecurity/information technology field</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
<td>0 years of general work experience in cybersecurity/information technology field</td>
</tr>
</tbody>
</table>

**Project Manager/Project Lead**

**Description:** Knowledgeable in the management of cybersecurity/information technology activities.

**Persons involved in this specialty perform the following tasks:** Plans, directs, coordinates, and controls technical and administrative activities of designated projects to ensure goals or objectives are accomplished within prescribed time frame and funding parameters. Supervises project managers in accomplishing assigned tasks. Reviews and maintains the quality of work performed on the project. Makes administrative judgments and provides advice on resolving problems. Coordinates project activities with activities of government regulatory or other governmental agencies. In the absence of the Cybersecurity Specialist, the Program Manager will support cybersecurity engineering functions and technical task completion.

**Knowledge, Skills and Abilities:** Provides management and technical direction to program managers or other program or project personnel. Regularly exercises independent judgment as well as a high level of analytical skill in solving complex and unusual technical and cybersecurity program execution problems. Establishes work plan and staffing for each phase of project, and arranges for recruitment or assignment of project personnel. Ultimately responsible for project planning, execution, and performance. Serves as counterpart to Government Senior Agency, Program, or Project Manager. Demonstrates extensive subject matter expertise and communication skills to interface with all levels of management.

**Minimum Experience:** Minimum four (4) years of experience including supervisory or management experience. Specific experience areas include requirements definition, work planning, control of budget, schedule, and task execution, and personnel management and supervision.

**Minimum Education Requirements:** Bachelor’s Degree in a relevant field.
Highly Desirable: Project Management Professional (PMP) certification.

<table>
<thead>
<tr>
<th>Substitutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
</tr>
<tr>
<td>Master’s Degree</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
</tr>
</tbody>
</table>

Senior Cybersecurity/Information Technology (IT) Engineer

Description: Considered an expert in the cybersecurity/information technology engineering field.

Persons involved in this specialty perform the following tasks: Provides technical and administrative direction for personnel performing knowledge management and/or software analysis tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinates with the Project and/or Program Manager to ensure problem solution and user satisfaction. Makes recommendations, if needed, for approval of major systems installations. Prepares milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives.

Knowledge, Skills and Abilities: Provides structure and ensures progression of working groups and teams by maintaining focus and avoiding unnecessary digression. Works closely with group members to enhance team building, communication, interpersonal relations, meetings, and decision-making. Provides support for task teams involved in quality and process improvement projects. Supports technical training and documentation for various subject matters in both a classroom environment and a one-on-one/small group setup. Organizes or conducts the necessary research to develop and revise training courses. Prepares appropriate training materials. Responsible for liaison with client senior staff.

Minimum Experience: Minimum eight (8) years of experience with a knowledge of applicable standard applications and, if required, subject matter expertise in cybersecurity.

Minimum Education Requirements: Master’s Degree in a relevant field.

Highly Desirable: Industry certifications in relevant field.

<table>
<thead>
<tr>
<th>Substitutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
</tr>
</tbody>
</table>
Cybersecurity/Information Technology (IT) Engineer

Description: Considered an expert in the cybersecurity/information technology engineering field.

Persons involved in this specialty perform the following tasks: Provides technical and administrative direction for personnel performing knowledge management and/or software analysis tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinates with the Project and/or Program Manager to ensure problem solution and user satisfaction. Makes recommendations, if needed, for approval of major systems installations. Prepares milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives.

Knowledge, Skills and Abilities: Provides structure and ensures progression of working groups and teams by maintaining focus and avoiding unnecessary digression. Works closely with group members to enhance team building, communication, interpersonal relations, meetings, and decision-making. Provides support for task teams involved in quality and process improvement projects. Supports technical training and documentation for various subject matters in both a classroom environment and a one-on-one/small group setup. Organizes or conducts the necessary research to develop and revise training courses. Prepares appropriate training materials. Responsible for liaison with client senior staff.

Minimum Experience: Minimum four (4) years of experience with a knowledge of applicable standard applications and, if required, subject matter expertise in cybersecurity.

Minimum Education Requirements: Bachelor’s Degree in a relevant field.

Highly Desirable: Industry certifications in relevant field.

<table>
<thead>
<tr>
<th>Substitutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
</tr>
<tr>
<td>Master’s Degree</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
</tr>
</tbody>
</table>

Senior Systems Engineer

Description: Considered an expert in the cybersecurity/information technology and computer systems engineering field.

Persons involved in this specialty perform the following tasks: Provides structure and ensures progression of working groups and teams by maintaining focus and avoiding unnecessary digression. Works closely with group members to enhance team building, communication, interpersonal relations, meetings, and decision-making. Provides support for task teams involved in quality and process improvement projects. Supports technical training and documentation for various subject matters in both a classroom environment and a one-on-one/small group setup. Organizes or conducts the necessary research to develop and revise training materials.
Knowledge, Skills and Abilities: Provides technical and administrative direction for personnel performing knowledge management and/or software analysis tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinates with the Project and/or Program Manager to ensure problem solution and user satisfaction. Makes recommendations, if needed, for approval of major systems installations. Prepares milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives.

Minimum Experience: Minimum eight (8) years of experience with a knowledge of applicable standard applications and, if required, subject matter expertise in cybersecurity.

Minimum Education Requirements: Master’s Degree in a relevant field.

Highly Desirable: Industry certifications in relevant field.

<table>
<thead>
<tr>
<th>Education</th>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bachelor’s Degree</td>
<td>10 years of general work experience in cybersecurity/information technology field</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
<td>6 years of general work experience in cybersecurity/information technology field</td>
</tr>
</tbody>
</table>

Systems Engineer

Description: Considered knowledgeable in the cybersecurity/information technology and computer systems engineering field.

Persons involved in this specialty perform the following tasks: Provides structure and ensures progression of working groups and teams by maintaining focus and avoiding unnecessary digression. Works closely with group members to enhance team building, communication, interpersonal relations, meetings, and decision-making. Provides support for task teams involved in quality and process improvement projects. Supports technical training and documentation for various subject matters in both a classroom environment and a one-on-one/small group setup. Organizes or conducts the necessary research to develop and revise training materials.

Knowledge, Skills and Abilities: Provides technical and administrative direction for personnel performing knowledge management and/or software analysis tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinates with the Project and/or Program Manager to ensure problem solution and user satisfaction. Makes recommendations, if needed, for approval of major systems installations. Prepares milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives.

Minimum Experience: Minimum four (4) years of experience with a knowledge of applicable standard applications and, if required, subject matter expertise in cybersecurity.
**Minimum Education Requirements:** Bachelor’s Degree in a relevant field.

**Highly Desirable:** Industry certifications in relevant field.

<table>
<thead>
<tr>
<th>Substitutions</th>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master’s Degree</td>
<td>2 years of general work experience in cybersecurity/information technology field</td>
</tr>
<tr>
<td>Ph.D. or Doctorate Degree</td>
<td>0 years of general work experience in cybersecurity/information technology field</td>
</tr>
</tbody>
</table>