General Services Administration

Authorized Federal Supply Schedule Pricelist

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 GSA Advantage!® is: GSAAdvantage.gov

Multiple Award Schedule (MAS)

Information Technology

SIN: 54151S – Information Technology Professional Services
SIN: 54151HACS – Highly Adaptive Cybersecurity Services (HACS)
SIN: OLM- Order Level Materials

PSC Code D310 IT Backup and Security Services
PSC Code D399 Other Information Technology Services, Not Elsewhere Classified

Contract Number: 47QTCA18D0001

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov

Contract Period: October 11, 2017 – October 10, 2022

Stanton Secure Technologies, LLC
Mailing Address: 2054 S Shirlington Rd Arlington, VA 22204
Phone: 703-568-0553 Fax: 703-991-5614
Internet: http://www.sst-llc.com
Business Size: Small Business
Customer Information

1a. Table of Awarded SINs

<table>
<thead>
<tr>
<th>SIN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>OLM</td>
<td>Order Level Materials</td>
</tr>
</tbody>
</table>

1b. Not Applicable

1c. Hourly Rates

<table>
<thead>
<tr>
<th>Years of Experience</th>
<th>Functional Responsibility (Summary)</th>
<th>Education</th>
<th>GSA Rate w/IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager</td>
<td>Responsible for working with the Project Management community to qualify and prioritize resource demand, support project delivery, and serve as a key touch point for customers. Will support a team of subject matter personnel and be responsible for daily operations as well as tracking deliverables and due dates for federal leads. The program manager will seek opportunities to scale operations and drive improvements commensurate with changing business needs and requirements.</td>
<td>Bachelor’s Degree or PMP</td>
<td>$145.08</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Extensive project management experience, including accountability for a team budget and achieving clearly defined project outcomes. Experience with both agile/iterative and traditional SDLC/PMP project management methodologies. Excellent written and oral communication skills, extensive presentation experience, with the ability to interact effectively with all levels of management. Ability to work with technical and non-technical staff and liaise between groups.</td>
<td>Bachelor’s Degree or PMP</td>
<td>$97.20</td>
</tr>
<tr>
<td>Project Manager II</td>
<td>Extensive project management experience, including accountability for a team budget and achieving clearly defined project outcomes. Experience with both agile/iterative and traditional SDLC/PMP project management methodologies. Excellent written and oral communication skills, extensive presentation experience, with the ability to interact effectively with all levels of management. Ability to work with technical and non-technical staff and liaise between groups.</td>
<td>Bachelor’s Degree or PMP and SME certification</td>
<td>$108.81</td>
</tr>
<tr>
<td>Cyber Security SME</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Job Title</td>
<td>Responsibilities</td>
<td>Education/Certification</td>
<td>Salary</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>5</strong> Subject Matter Expert</td>
<td>Responsible for the collection of requirements and contribution of Subject Matter Expertise (SME) advice in the areas of security design, policies, and control standards. Proactively engages staff throughout to communicate cloud security standards, guidelines, and strategies. Works with project teams to ensure technical quality of cloud security focused deliverables and adherence to security standards, governance, and controls practices. Considered a security and technical expert in security technology, design, systems implementation, and integration. Conducts technical research when necessary to contribute to setting security direction and strategy. Assists others on own team, or other teams where applicable with security projects or security-relevant tasks on technical projects.</td>
<td>Bachelor’s Degree or CISSP and CCSP</td>
<td>$168.29</td>
</tr>
<tr>
<td><strong>10</strong> Subject Matter Expert</td>
<td>Responsible for the collection of requirements and contribution of Subject Matter Expertise (SME) advice in the areas of Cloud security design, policies, and control standards. Proactively engages staff throughout to communicate cloud security standards, guidelines, and strategies. Works with project teams to ensure technical quality of cloud security focused deliverables and adherence to security standards, governance, and controls practices. Considered a security and technical expert in cloud security technology, design, systems implementation, and integration. Familiarity with IaaS, PaaS, and SaaS as well as different deployment models. Conducts technical research when necessary to contribute to setting cloud security direction and strategy. Assists others on own team, or other teams where applicable, on cloud security projects or security-relevant tasks on technical projects.</td>
<td>Bachelor’s Degree or SME certification</td>
<td>$168.29</td>
</tr>
<tr>
<td><strong>5</strong> Security Lead/Manager</td>
<td>Serve as an Information Assurance Compliance Specialist for a government client and help to continue to evolve the use of the NIST Risk Management Framework or the current standard, in the client’s enterprise. Sustain current security policies, processes, and procedures. Use DIACAP and NIST doctrine to sustain various baselines, standards, policies, procedures, and other business tools that tailor the NIST controls and processes for use by the client's various business units. Assess the impacts, help to orchestrate updates and changes in the client’s enterprise, and provide expert advice about how to address the evolving Risk Management Framework most effectively as NIST and other doctrine sources update their body of knowledge. Support efforts to improve overall security practices by raising general information security awareness and best security practices.</td>
<td>Bachelor’s Degree or CISSP</td>
<td>$121.14</td>
</tr>
<tr>
<td><strong>Security Consultant I</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Responsible for the planning, implementation and upgrade of security measures and protocols. Maintenance of data security access. Perform vulnerability testing, risk analyses and security assessments. Conduct internal and external security audits. Anticipate security alerts, incidents and disasters and reduce their likelihood. Manage network, intrusion detection and prevention systems. Analyze security breaches to determine their root cause. Recommend and install appropriate tools and countermeasures. Define, implement, and maintain corporate security policies. Coordinate security plans with outside vendors.</td>
<td>Bachelor’s Degree or CAP/CISSP</td>
<td>$108.81</td>
</tr>
</tbody>
</table>

Responsible for ensuring that Stakeholders adhere to Federal Information Assurance policies and procedures to acquire and maintain an Information System’s Authority to Operate (ATO) under The Federal Information Security Modernization Act (FISMA) of 2014 following NIST 800-53 guidelines and NIST 800-53a security controls assessment practices. Strong knowledge of Risk Management Framework (RMF).


Security Consultant II

| 5 | See Security Consultant I | Bachelor’s Degree or two industry certifications | $116.06 |

Security Control Assessor I

| 4 | Responsible for performing security control compliance reviews, tracking, and continuous monitoring of assessment packages. Advise and assist with the Lifecycle Assessment and Authorization (A&A) process and developing a Security Assessment Report (SAR). Monitor and track projects in the assessment test queue. Maintain a document repository where A&A project documentation is stored. Record/register actions concerning project approvals to operate. Read and analyze SSPs and develop understanding of systems and applications into security test plans. Coordinate A&A actions and system testing with appropriate security personnel. Develop risk assessment reports. Assemble and submit C&A packages to Principal Accreditation Authority/Designated Accreditation Authority. Review IA Compliance Validation Tests and Reports. Responsible for execution, review and interpretation of automated vulnerability scans utilizing industry standard tools. | Bachelor’s Degree or Industry Certification | $104.46 |

Security Control Assessor II
8 | Responsible for performing security control compliance reviews, tracking, and continuous monitoring of assessment packages. Advise and assist with the Lifecycle Assessment and Authorization (A&A) process and developing a Security Assessment Report (SAR). Monitor and track projects in the assessment test queue. Maintain a document repository where A&A project documentation is stored. Record/register actions concerning project approvals to operate. Read and analyze SSPs and develop understanding of systems and applications into security test plans. Coordinate A&A actions and system testing with appropriate security personnel. Develop risk assessment reports. Assemble and submit C&A packages to Principal Accreditation Authority/Designated Accreditation Authority. Review IA Compliance Validation Tests and Reports. Responsible for execution, review and interpretation of automated vulnerability scans utilizing industry standard tools. Experience with FedRAMP | Bachelor’s Degree and/or Industry Certification | $108.81

Analyst

5 | Responsible for partnering with stakeholder teams in the analysis of systems requirements, development of systems processes and documentation. Responsible for the ongoing customer support and response to customer inquiries performing required research and analysis as needed. Responsible for regular status reporting, updates and executive brief preparation and delivery. | Bachelor’s Degree or Industry Certification | $90.68

Analyst II

10 | Responsible for partnering with stakeholder teams in the analysis of systems requirements, development of systems processes and documentation. Responsible for the ongoing customer support and response to customer inquiries performing required research and analysis as needed. Responsible for regular status reporting, updates and executive brief preparation and delivery. | Bachelor’s Degree and/or Industry Certification | $94.30

Technical Writer

5 | Gathers, analyzes, and composes technical information. Conducts research and ensures the use of proper technical terminology. Translates technical information into clear, readable documents to be used by technical and non-technical personnel. Supports the development of all types of documents and reports by developing and updating graphics presentations to improve the quality and enhance the usability of these documents. Responsible for integrating the graphics generated with automated tools and the deliverable documents. | Bachelor’s Degree and/or Industry Certification | $72.54

2. Maximum Order (All dollar amounts are exclusive of any discount for prompt payment.)

<table>
<thead>
<tr>
<th>Item Code</th>
<th>Description</th>
<th>Maximum Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
<td>$500,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
<td>$500,000</td>
</tr>
<tr>
<td>OLM</td>
<td>Order Level Materials</td>
<td>$250,000</td>
</tr>
</tbody>
</table>
3. **Minimum Order** The minimum dollar value of orders to be issued is $500

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 areas, for orders received from overseas activities.

5. **Point(s) of Production:** Arlington, Arlington County, VA

6. **Discounts:** Prices shown are NET Prices; Basic Discounts have been deducted.

7. **Quantity Discounts:** None

8. **Prompt Payment Terms:** 1% Net 15 Days Prompt Payment Terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9. **Government Purchase Cards**

9a. Contractor must accept the credit card for payments equal to or less than the micro-purchase for oral or written orders under this contract.

9b. The Contractor and the ordering agency may agree to use the credit card for dollar amounts over the micro-purchase threshold (See GSAR 552.232-79 Payment by Credit Card). In addition, bank account information for wire transfer payments will be shown on the invoice.

10. **Foreign Items:** None

11a. **Time of Delivery:** Determined at Task Level

11b. **Expedited Delivery:** Determined at Task Level

11c. **Overnight and 2-day delivery:** Determined at Task Level

11d. **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.

12. **F.O.B. point(s):** Destination

13a. **Ordering Address:**

   **Stanton Secure Technologies, LLC**  
   2054 S. Shirlington Road Arlington, VA 22204
13b. Ordering Procedures: Ordering activities shall use the ordering procedures of Federal Acquisition Regulation (FAR) 8.405 when placing an order or establishing a BPA for supplies or services.

14. Payment Address:

Stanton Secure Technologies, LLC  
2054 S. Shirlington Road Arlington, VA 22204  
Tel: 703-563-0558 www.sst-llc.com

15. Warranty Provision: Standard Commercial

16. Export Packing Charges: Not Applicable

17. Terms and conditional of Government purchase card acceptance (any thresholds above the micro-purchase level): None

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

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

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

20a. Terms and conditions for any other services (if applicable): None

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

22. List of participating dealers (if applicable): Not Applicable

23. Preventive maintenance (if applicable): Not Applicable

24a. Special attributes such as environmental attributes (e.g. recycled content, energy efficiency, and/or reduced pollutants): Not Applicable

24b. Section 508 Compliance for Electronic and Information Technology (EIT): Compliant. The EIT standard can be found at: www.Section508.gov/

25. DUNS Number: 60-9449108

26. Notification Regarding Registration in System for Award Management (SAM) Database: Contractor has an active registration in the System for Award Management (SAM) database.

27. Terms and conditions APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S)

1. SCOPE
   a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT
Professional Services within the scope of this Information Technology Schedule.
b. 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. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)
a. 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.
b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
c. 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. ORDER
a. 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.
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. PERFORMANCE OF SERVICES
a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
b. The Contractor agrees to render services only 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 IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed.
e. Established Federal Government per diem rates will apply to all Contractor travel.
Contractors cannot use GSA city pair contracts.

5. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)
   a. 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-
   b. Cancel the stop-work order; or
   c. Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.
   d. 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-
   e. 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
   f. 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.
   g. 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.
   h. 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.

6. INSPECTION OF SERVICES
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 (Dec 2007) Rights in Data – General, may apply.

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 Professional Services.

9. INDEPENDENT CONTRACTOR
All IT 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.

10. ORGANIZATIONAL CONFLICTS OF INTEREST
   a. Definitions.
   b. “Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.
   c. “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.
   d. 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.
   e. 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.

11. INVOICES
The Contractor, upon completion of the work ordered, shall submit invoices for IT Professional 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
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 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIAITION I – FEB 2007) 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 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIAITION I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

   a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
   b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—
      1) The offeror;
      2) Subcontractors; and/or
      3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

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

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.

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.
28. Terms and conditions APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (54151HACS)

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

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

1. SCOPE

The labor categories, prices, terms and conditions stated under Special Item Number 54151HACS High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.

   a. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on MAS Information Technology and may be quoted along with services to provide a total solution.
   
   b. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.
   
   c. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.
   
   d. 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
   
   b. 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.
   
   c. 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

5. RESPONSIBILITIES OF THE CONTRACTOR
The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (MAY 2014) Rights in Data – General, may apply.
The Contractor shall comply with contract clause (52.204-21) to the Federal Acquisition Regulation (FAR) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY
Subject to the ordering activity’s security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.

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

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

c. “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.

d. 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.

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

9. INVOICES
The Contractor, upon completion of the work ordered, shall submit invoices for Highly Adaptive Cybersecurity Services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products.

Invoices shall be submitted monthly for recurring services performed during the preceding month.

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

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

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

c. EXAMPLE

Commercial Job Title: Computer Network Defense Analysis

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

Professionals involved in this specialty perform the following tasks:

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

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

Minimum Experience: 5 Years

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