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 GSAAvantage.gov

54151HACS: Highly Adaptive Cybersecurity Services (HACS)

Contract number 47QTCA20D008C
Contract period April 1, 2020 – March 31, 2025
Financial Institution Information Security Compliance, LLC
(DBA Security Compliance Associates)
2727 Ulmerton Rd. Ste. 310, Clearwater, FL 33762
727-571-1141
www.scasecurity.com
Brian Fischer
Small Business

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

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

54151HACS: Highly Adaptive Cybersecurity Services (HACS)

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract.

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor category or part #</th>
<th>$</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Project Manager</td>
<td>$169.57</td>
</tr>
</tbody>
</table>

1c. Hourly rates: For Labor category rates and descriptions see pages 4-5

2. Maximum order: $500,000

3. Minimum order: $100

4. Geographic coverage (delivery area): CONUS, AK, HI, PR

5. Point(s) of production: same as contractor address or where product is produced

6. Discount from list prices or statement of net price. All prices listed herein are net, and all discounts have been deducted.

7. Quantity discounts: None

8. Prompt payment terms. None, Net 30

9a. Government purchase cards are accepted at or below the micro-purchase threshold. Yes

9b. Government purchase cards are not accepted above the micro-purchase threshold.

10. Foreign items: None

11a. Time of delivery: As Negotiated

11b. Expedited Delivery: As Negotiated

11c. Overnight and 2-day delivery: schedule customer may contact the Contractor for rates.

11d. Urgent Requirements: As Negotiated

12. F.O.B. point: Destination
13a. Ordering address: 2727 Ulmerton Rd. Ste. 310, Clearwater, FL 33762

13b. Ordering procedures: as found in Federal Acquisition Regulation (FAR) 8.405-3.

14. Payment address: 2727 Ulmerton Rd. Ste. 310, Clearwater, FL 33762

15. Warranty provision: None

16. Export packing charges: Not Applicable

17. Terms and conditions of Government purchase card acceptance: Not Applicable

18. Terms and conditions of rental, maintenance, and repair: Not Applicable

19. Terms and conditions of installation: Not Applicable

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

20a. Terms and conditions for any other services: Not Applicable

21. List of service and distribution points: Not Applicable

22. List of participating dealers: Not Applicable

23. Preventive maintenance: Not Applicable

24a. Special attributes such as environmental attributes: Not Applicable

24b. Section 508: Not Applicable

25. Data Universal Number System (DUNS) number: 014545808

26. Notification regarding registration in System for Award Management (SAM) Database: (Company) has an active registration in SAM
## Labor Category Descriptions

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>Functional Responsibilities</th>
<th>Minimum Education</th>
<th>Minimum Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal</td>
<td>Corporate manager directing all aspects of the organization. Ensures that client project goals are attained. Plans, directs and coordinates activities to pursue company mission.</td>
<td>Bachelor Degree</td>
<td>20</td>
</tr>
<tr>
<td>VP Information Security Services</td>
<td>Manages all security analysts. Reviews reports prior to delivery. Assists in developing new services. May personally deliver services as needed. Reports to Principal.</td>
<td>Bachelor Degree CISSP certification</td>
<td>10</td>
</tr>
<tr>
<td>VP Compliance Services</td>
<td>Oversees and may personally deliver compliance related services including policy, business continuity, incident response, privacy and employee training. Reports to Principal.</td>
<td>Master Degree</td>
<td>5</td>
</tr>
<tr>
<td>Director - Cybersecurity Services</td>
<td>Manages team of Junior and entry security analysts. Directs the delivery of external services such as external vulnerability assessments and penetration testing. Reports to VP Information Security.</td>
<td>Master Degree + C</td>
<td>EH and OSCP certifications</td>
</tr>
<tr>
<td>Senior Security Analyst</td>
<td>Performs information security assessment services for larger clients. Writes technical reports. Is main technical point of contact during engagements. Reports to VP Information Security.</td>
<td>Master Degree + CISSP certification</td>
<td>10</td>
</tr>
<tr>
<td>Junior Security Analyst</td>
<td>Performs information security assessment services for medium size clients. Supports Senior Analysts as needed. Writes technical reports. Is main technical point of contact during engagements. Reports to VP Information Security.</td>
<td>Bachelor Degree</td>
<td>5</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>Performs externally delivered information security assessment services. Supports Senior and Junior Analysts as needed. Writes technical reports. Reports to Director - Cybersecurity.</td>
<td>Bachelor Degree</td>
<td>1</td>
</tr>
<tr>
<td>Project Manager</td>
<td>Main client relationship point of contact - usually sales executive. Oversees service delivery across internal services, external services and compliance teams. Ensures project completion on-time and within budget.</td>
<td>Bachelor Degree</td>
<td>5</td>
</tr>
</tbody>
</table>

**SUBSTITUTIONS:** Bachelors Degree + 2 Years Experience = Masters Degree
Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SIN must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Federal Acquisition Regulation (FAR) Part 52.204-21
- OMB Memorandum M-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
- OMB Memorandum M-19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 2017 Report to the President on Federal IT Modernization
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
• NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View
• NIST SP 800-44 - Guidelines on Securing Public Web Servers
• NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
• NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
• NIST SP 800-61 - Computer Security Incident Handling Guide
• NIST SP 800-64 - Security Considerations in the System Development Life Cycle
• NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
• NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
• NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
• NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems
• NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
• NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
• NIST SP 800-160 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
• 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 132-45 Highly Adaptive Cybersecurity Services (HACS) apply exclusively to Highly Adaptive Cybersecurity Services within the scope of this Information Technology 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 IT Schedule 70 (e.g. 132-32, 132-33, 132-8), 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:

132-45 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