

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!*<sup>®</sup>, a menu-driven database system. The INTERNET address GSA  
*Advantage!*<sup>®</sup> is: GSAAdvantage.gov.

AUTHORIZED  
INFORMATION TECHNOLOGY SCHEDULE PRICELIST  
GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY  
EQUIPMENT, SOFTWARE AND SERVICES  
IT Schedule 70

SIN 132-45 (Highly Adaptive Cybersecurity Services)

FSC Group, Part, and Section or Standard Industrial Group (as applicable)  
FSC Class(es)/Product code(s) and/or Service Codes (as applicable)

**Contract number: 47QTCA19D008S**

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

**Contract period March 27, 2019 through March 26, 2024**

Business Size: Large

security**METRICS**<sup>®</sup>

1275 W. 1600 N.  
Orem, UT 84057 USA  
P: 801.705.5679  
www.securitymetrics.com

Contract Administration source:

Michelle Morris  
1275 W. 1600 N.  
Orem, UT 84057 USA  
P: 801.705.5679 F: 801-724-9700

**CUSTOMER INFORMATION**

**1a. Table of Awarded special item numbers**

132-45 Highly Adaptive Cybersecurity Services

**1b. Identification of the lowest priced model number and lowest unit price:**

132-45	Consultant	\$257.68
--------	------------	----------

**1c. Hourly Rates**

Consultant / Subject Matter Expert - \$257.68

Primary responsibilities are client service delivery and operations execution on projects ranging in scope including, but not limited to technology strategy, architecture and service management; Cybersecurity; systems integration; data analytics and visualization; application development and maintenance; help desk operations; infrastructure/network design and management; and cloud (e.g., software, platform, infrastructure as a service). Possess competencies in multiple Cybersecurity technologies, business processes, or combination of both. May perform as a project manager on Cybersecurity engagements of moderate size complexity or lead one or multiple work streams on large engagements. Communicates project delivery schedule and milestones while maintaining productive and professional relationships with client. May perform analyses of a technical or non-technical nature.

Education/Exp: Bachelors / 7 years

**2. Maximum Order:**

132-45 - \$500,000

**3. Minimum Order:** \$100.00

**4. GEOGRAPHIC COVERAGE (delivery area):** Domestic Delivery

**5. POINT OF PRODUCTION:** USA

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

**7. QUANTITY DISCOUNTS:** Additional 2% for orders over \$350,000.

**8. PROMPT PAYMENT TERMS:** None - Net 30 days

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

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

**10. FOREIGN ITEMS:** None

**11a. TIME OF DELIVERY:** The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below:

**SPECIAL ITEM NUMBER**

132-45

**DELIVERY TIME (Days ARO)**

To Be Negotiated per Task Order

**11b. EXPEDITED DELIVERY:** may be available. Contact Contractor for more information.

**11c. OVERNIGHT AND 2-DAY DELIVERY:** may be available. Contact Contractor for more information.

**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. FOB point:** Destination

**13a. ORDERING ADDRESS:**

1275 W. 1600 N.  
Orem, UT 84057

**13b. ORDERING PROCEDURES:** Contact Contractor in 13a. above

**14. PAYMENT ADDRESS:** Same as ordering address in 13a. above

**15. WARRANTY PROVISION:** Standard Commercial Warranty

**16. Export packing charges, if applicable:** None

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

**18. Terms and conditions of rental, maintenance, and repair:** None

**19. Terms and conditions of installation:** None

**20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices:** None

**20a. Terms and conditions for any other services:** None

**21. List of service and distribution points:** None.

**22. List of participating dealers:** None

**23. Preventive maintenance:** None

**24a.** Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants) : None

**24b.** 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 (www.atacorporation.com). The EIT standards can be found at: [www.Section508.gov/](http://www.Section508.gov/).

**25. Data Universal Number System (DUNS) number:** 050445308

**26. Notification regarding registration in Central Contractor Registration (CCR) data:** Contractor has an active registration.

**TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)  
(SPECIAL ITEM NUMBER 132-45)**

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 800-37 - Risk Management Framework for Information Systems and Organizations: A Systems Life Cycle Approach for Security and Privacy
- 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 (ISCSMA) 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 132-45 for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.
- b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor's customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.

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

EXAMPLE

Commercial Job Title: Computer Network Defense Analysis

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

Professionals involved in this specialty perform the following tasks:

- Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities



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

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

Minimum Experience: 5 Years

Minimum Education Requirements: a bachelor's of science degree with a concentration in computer science, cybersecurity services, management information systems (MIS), engineering or information science is essential.

Highly Desirable: Offensive Security Certified Professional (OSCP) or commercial Cybersecurity advanced certification(s).

<u>Category</u>	<u>Ed - Exp</u>	<u>Functional Responsibilities</u>	<u>GSA Rate</u>
Consultant/Subject Matter Expert	BA-7	Primary responsibilities are client service delivery and operations execution on projects ranging in scope including, but not limited to technology strategy, architecture and service management; Cybersecurity; systems integration; data analytics and visualization; application development and maintenance; help desk operations; infrastructure/network design and management; and cloud (e.g., software, platform, infrastructure as a service). Possess competencies in multiple Cybersecurity technologies, business processes, or combination of both. May perform as a project manager on Cybersecurity engagements of moderate size complexity or lead one or multiple work streams on large engagements. Communicates project delivery schedule and milestones while maintaining productive and professional relationships with client. May perform analyses of a technical or non-technical nature.	\$257.68