Sybersense, LLC
10597 Brookeville Ct.
Great Falls, VA 22066
(P) 571-379-6671
www.sybersense.net

Multiple Award Schedule (MAS)
Contract Number: GS35F438CA
Period Covered by Contract: July 22, 2015 through July 22, 2025
GSA IT Schedule Contract Number: GS-35F-438CA

FEDERAL SUPPLY SERVICE
AUTHORIZED MULTIPLE AWARD SCHEDULE (MAS) PRICELIST

GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY EQUIPMENT, SOFTWARE, AND SERVICES

Special Item Number 54151S    Information Technology Professional Services
Special Item Number 54151HACS  Highly Adaptive Cyber Security Services (HACS)
Special Item Number OLM       Order-Level Materials

SIN 54151S - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES
✓ FPDS Code D301    IT Facility Operation and Maintenance
✓ FPDS Code D302    IT Systems Development Services
✓ FPDS Code D306    IT Systems Analysis Services
✓ FPDS Code D307    Automated Information Systems Design and Integration Services
✓ FPDS Code D308    Programming Services
✓ FPDS Code D310    IT Backup and Security Services
✓ FPDS Code D311    IT Data Conversion Services
✓ FPDS Code D316    IT Network Management Services
✓ FPDS Code D399    Other Information Technology Services, Not Elsewhere Classified

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

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

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

NAIC Codes 541511, 541512, 541513, 541519

Sybersense, LLC
10597 Brookeville Ct.
Great Falls, VA 22066
571.379.6671
DUNS: 07-829-9155

Contract No. GS-35F-438CA

Period Covered: 07/22/2015 – 07/22/2025; Inclusive of Modification PO-0019
Pricelist current through Modification A826, dated 12/30/2020

Sybersense, LLC – 10597 Brookeville Ct., Great Falls, VA 22066 //Email: info@Sybersense.net //www.sybersense.net
**About Us**

Sybersense is an 8(a) certified small, disadvantaged business (SDB) with 10+ years of experience providing best practices in Cybersecurity, Project Management, Information Technology, and Application Development to the Federal Government. Within our Federal Practice, Sybersense provides project management, systems engineering, cybersecurity architecture, operations & maintenance, and agile software development services.

We have excellent past performance in a wide range of IT projects, all supporting Federal government customers, such as the Department of the Navy, General Services Administration, Commodity Futures Trading Commission, Federal Reserve Board, and the U.S. Coast Guard.

**Services**

To bring excellent service to our customers, we provide best value and effective collaborations to each project by working closely with each customer and vendors. We leverage well-established business relationships with our strategic partners to provide best value solutions and deliver the necessary personnel, and services to our customer. We provide end-to-end engineering and integration, logistics, training, and support to ensure success. These factors combined represent significant strength and low performance risk in meeting specific customer requirements. We apply our cyber, analytics, and engineering expertise to anticipate, identify and resolve our customers' most demanding information related challenges, including the effective management and integration of large and complex government systems, the efficient collection and analysis of large quantities of critical data, the migration of applications and data to the cloud and the implementation of effective cybersecurity measures to successfully detect, prevent and mitigate cyber-attacks.

**Customer Information:**

1a. Awarded Special Item Number(s):

<table>
<thead>
<tr>
<th>SIN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Information Technology Services</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cyber Security Services (HACS)</td>
</tr>
<tr>
<td>OLM</td>
<td>Order-Level Materials</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: Not applicable.
1c. Descriptions of all corresponding commercial job titles with experience, function responsibility and education are provided beginning on page 10.

2. Maximum order: $500,000.00

3. Minimum order: $100.00

4. Geographic Coverage: Domestic Delivery Only

5. Point of Production: Not Applicable

6. Prices Shown Herein are Net (discount deducted)

7. Quantity Discount: None

8. Prompt Payment Terms: 2.0% - 10 days from receipt of invoice or date of acceptance, whichever is later.

9a. Government Purchase Cards are accepted below the micropurchase threshold.

9b. Government Purchase Cards are not accepted above the micropurchase 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:

<table>
<thead>
<tr>
<th>SPECIAL ITEM NUMBER</th>
<th>DELIVERY TIME (Days ARO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cyber Security Services</td>
</tr>
</tbody>
</table>

11b. Expedited Delivery: Consult with Contractor

11c. Overnight/2-day Delivery: Consult with Contractor

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:
Sybersense, LLC
10597 Brookeville Ct.
Great Falls, VA 22066
571.379.6671
Email: rjavaid@sybersense.net

13b. 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.

14. Payment Address:
Sybersense, LLC
10597 Brookeville Ct.
Great Falls, VA 22066
571.379.6671
Email: rjavaid@sybersense.net

15. Warranty Provisions: Contractor’s Standard Warranty

16. Export Packing Charges: 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.

20b. Terms and Conditions of any other service parts: Not applicable.

21. List of Service and Distribution Points: Not applicable.

22. List of Participating Dealers: Not applicable.

23. Preventative Maintenance: Not applicable.

24. Section 508 compliance information is available by contacting Sybersense, LLC directly.

25. DUNS: 07-829-9155

26. Sybersense, LLC is registered in the System for Award Management (SAM) Database.
1. SCOPE
   a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively within the scope of this 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
   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 in accordance with this clause.
   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/EC 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.

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-

1) Cancel the stop-work order; or

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

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

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

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

c. 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.

d. 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

The Inspection of Services–Fixed Price (AUG 1996) (Deviation – May 2003) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection–Time-and-Materials and Labor-Hour (JAN 1986) (Deviation – May 2003) clause at FAR 52.246-6 applies to time-and-materials and labor-hour orders placed under this contract.
7. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Deviation – May 2003) 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 Professional 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:

✓ “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.

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 preceding month.

12. PAYMENTS
For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order.

For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003)) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(c) (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.

16. DESCRIPTION OF IT SERVICES AND PRICING
a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 54151S IT Professional Services 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 IT Services shall be in accordance with the Contractor's customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices.

## Sybersense, LLC
GSA Price List
SIN 54151S
(Effective January 1, 2020)

<table>
<thead>
<tr>
<th>Commercial Labor Category</th>
<th>GSA Schedule Rate w/ IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Developer I</td>
<td>$86.01</td>
</tr>
<tr>
<td>Application Developer II</td>
<td>$102.62</td>
</tr>
<tr>
<td>Data Architect I</td>
<td>$80.14</td>
</tr>
<tr>
<td>Enterprise Architect II</td>
<td>$161.26</td>
</tr>
<tr>
<td>Information Security Analyst I</td>
<td>$126.08</td>
</tr>
<tr>
<td>Information Security Analyst II</td>
<td>$143.67</td>
</tr>
<tr>
<td>Information Systems Security Officer I</td>
<td>$112.39</td>
</tr>
<tr>
<td>Program Manager II</td>
<td>$152.46</td>
</tr>
<tr>
<td>Subject Matter Expert III</td>
<td>$244.33</td>
</tr>
</tbody>
</table>

## Sybersense, LLC
Labor Category Descriptions
SIN 54151S

1. **Application Developer I**

**General Experience**

Three (3) years of relevant experience required.

**Functional Responsibility**

Application developer I builds, maintains and manages all aspects of a web application. ("Web application" is a catchall term for several interfaces that utilize the world wide web.) One example would be a website, and another could be a mobile phone or tablet app. Web application developers must plan, build and subsequently manage every process of the application's
development. Sometimes this is done as part of a team, but it can also be done independently or under the supervision of the employer. Fluent understanding of common developer languages such as HTML and PHP will nearly always be necessary and may need to be demonstrated via a test or a strong portfolio.

**Minimum Education**

Bachelor's Degree in computer science, electronics engineering or other engineering or technical discipline is required.

2. **Application Developer II**

**General Experience**

Five (5) years of relevant experience required.

**Functional Responsibility**

Application Developer II designs, creates, and implements software code in order to improve the effectiveness of a website. They work on a team with graphic designers and web designers to develop websites with HTML, JavaScript, PHP, CSS, and other coding methods. Web developers focus on the concept, interface design, and layout of a website from design to launch. They may build and test the integration of a website to make it easy to use and navigate for end users and clients. For ongoing websites, web developers troubleshoot and debug existing code in order to enhance the website’s functionality. The field of web development is currently shifting toward the optimization of mobile device applications and web browsing.

**Minimum Education**

Bachelor's Degree in computer science, electronics engineering or other engineering or technical discipline is required.

3. **Data Architect I**

**General Experience**

Data Architect I possesses at least four (4) years of related experience.

**Functional Responsibility**

Data Architect I contributes to the development of system and data architectures, to include documentation such as the System Architecture plan, logical and physical data diagrams, use cases, data flows, interface documentation, and requirements and specifications. Creates and implement methods of storing and maintaining data. Adhere to quality standards for new data. Develop methods of warehouse implementation, data acquisition and archive recovery.

**Minimum Education**
Data Architect I possesses either a Bachelor’s Degree in Business, Computer Science, Communications or Engineering.

4. **Enterprise Architect II**

**General Experience**
Enterprise Architect II possesses at least eight (8) years of related experience.

**Functional Responsibility**
Enterprise Architect II possesses the ability to architect solutions to provide timely update of large databases and assuring high performance across the architecture; works with other team members to improve the business process, information and technology of client organizations; designs, implements and develops Integration solutions for providing state of the art solutions capable of handling high volume transaction rates for real-time processing and delivery; supports enterprise design by in developing enterprise schemas to map data and process flows between systems and solutions. Manages the activities of multiple LVL I enterprise architects. Demonstrates the ability to work independently with minimal supervision.

**Minimum Education**
Enterprise Architect II possesses either a Bachelor’s Degree in Business, Computer Science, Communications or Engineering.

5. **Information Security Analyst I**

**General Experience**
Four (4) years of relevant experience required.

**Functional Responsibility**
An Information Security Analyst I has extensive IT experience in all aspects of Cyber Security with a vast array of IT systems involving end user as well as enterprise level networks. Experience in designing and implementing systems that meet agency Cyber Security policy and regulations. Must have extensive experience in Cyber Security Tools, network topologies, intrusion detection, PKI, and secured networks.

**Minimum Education**
Bachelor’s in computer science, electronics engineering or other engineering or technical discipline is required.

6. **Information Security Analyst II**

**General Experience**
Six (6) years of relevant experience required.

**Functional Responsibility**

An Information Security Analyst II has extensive IT experience with Cyber Security Policy and threat mitigation. Must be well versed in Cyber Security Tools, network topologies, intrusion detection, PKI, and secured networks. Analyst must possess a high level of expertise in developing long term strategies and be knowledgeable about various cyber threats and their mitigation.

**Minimum Education**

Master's Degree in computer science, electronics engineering or other engineering or technical discipline is required.

7. **Information Systems Security Officer I**

**General Experience**

An Information Systems Security Officer I possesses at least four (4) years of experience in IT security or related assignments.

**Functional Responsibility**

An Information Systems Security Officer I provides minimally supervised support for difficult analysis and evaluation assignments. Has the ability to provide analysis and consulting to management level personnel. Performs analysis and evaluation of existing or proposed processes, applications, systems, or software. Performs, and/or may direct, project planning, scope, control, management, tracking, or review. May perform functional requirements gathering for projects, to include security requirements. Performs analysis and evaluation throughout the process, application, system, or software development life-cycle which includes, but is not limited to: planning, requirements, design, acquisition, development, integration, installation/deployment, performance tuning, testing, or training. Performs, or may direct, document development/ preparation at various stages of a project life-cycle (e.g., planning through implementation) to detail analysis results and solution recommendations. Assists with testing to support the project life-cycle, as applicable. Uses methodologies, modeling/ estimating techniques, tools, applications, systems, software, or databases at advanced levels to perform assigned tasks.

**Minimum Education**

Information Systems Security Officer I possesses a four year degree from an accredited college/ university and may possess advanced degrees and/or industry certification.

8. **Program Manager II**

**General Experience**
Eight (8) years of professional experience in an information technology /information management or related field.

**Functional Responsibility**

A Program Manager II is responsible for project oversight and direction. Ensures conformance with work standards; interprets policies, procedures, goals and objectives of the organization. Ensures appropriate resources are applied to the project. Nature of work involves complex information technology project management, strategic and tactical planning, coordination, control, and critical decision-making. Requires experience related to work being performed. May also involve complex technical engineering design and technology architectural tasks.

**Minimum Education**

A Bachelor's Degree in Information Technology.

9. **Subject Matter Expert III**

**General Experience**

Minimum of twelve (12) years of experience in an area of specialization associated with the requirement. Experience with Government or industry standards, processes, procedures, methodologies, or tools that support analysis as relative to the requirement.

**Functional Responsibility**

Has substantial expertise in a specific functional area. May direct analyses of requirements for information systems. May direct the design of adaptations to software. May be knowledgeable in process analysis techniques such as flowcharting, process mapping, benchmarking, and activity-based costing. May have subject matter expertise in areas such as facilitation, organizational development, and change management. May have specific expertise in business or functional areas such as Reliability-Centered Maintenance principles and methodology, or logistics policy development. May have demonstrated experience in configuration management, maintenance planning, supply management, outfitting/fitting out, data management, training, or logistics/configuration information systems.

**Minimum Education**

Bachelor's Degree in computer science, electronics engineering or other engineering or technical discipline is required.
TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)  
(SPECIAL ITEM NUMBER 54151HACS)

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-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
• OMB Memorandum M-17-09 – Management of Federal High Value Assets
• OMB Memorandum M-17-12 – Preparing for and Responding to a Breach of PII
• 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
1. SCOPE

a. The labor categories, prices, terms, and conditions stated under Special Item Number 54151HACS High Adaptive Cybersecurity Services (HACS) apply exclusively to High Adaptive Cybersecurity Services within the scope of this 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 Schedule MAS 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) 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 six-step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control 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 sub-category):

- **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 subcategory 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.

c. 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 Firm-Fixed Price and Time and-Materials and Labor-Hour Contracts 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.

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 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).

Sybersense, LLC
GSA Price List
SIN 54151HACS
(Effective January 1, 2021)

<table>
<thead>
<tr>
<th>Commercial Labor Category</th>
<th>GSA Schedule Rate w/ IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Security Architect</td>
<td>$219.90</td>
</tr>
<tr>
<td>Cybersecurity Engineer II</td>
<td>$143.67</td>
</tr>
<tr>
<td>Cybersecurity Engineer III</td>
<td>$157.35</td>
</tr>
<tr>
<td>Cyber Program Manager II</td>
<td>$175.74</td>
</tr>
<tr>
<td>Subject Matter Expert II</td>
<td>$153.44</td>
</tr>
<tr>
<td>Subject Matter Expert III</td>
<td>$244.33</td>
</tr>
</tbody>
</table>
1. **Cloud Security Architect**

**General Experience**
Eight (8) years of relevant experience required.

**Functional Responsibility**
Cloud Security Architect possesses the ability to architect solutions to provide timely update of large databases and assuring high performance across the architecture; works with other team members to improve the business process, information and technology of client organizations; designs, implements and develops Integration solutions for providing state of the art solutions capable of handling high volume transaction rates for real-time processing and delivery; supports enterprise design by in developing enterprise schemas to map data and process flows between systems and solutions. Demonstrates the ability to work independently with minimal supervision.

**Minimum Education**
Bachelor's Degree in computer science, electronics engineering or other engineering or technical discipline is required.

2. **Cybersecurity Engineer II**

**General Experience**
Five (5) years of relevant experience required.

**Functional Responsibility**
An Information Security Analyst II has extensive IT experience with Cyber Security Policy and threat mitigation. Must be well versed in Cyber Security Tools, network topologies, intrusion detection, PKI, and secured networks. Analyst must possess a high level of expertise in developing long term strategies and be knowledgeable about various cyber threats and their mitigation.

**Minimum Education**
Bachelor’s Degree in computer science, electronics engineering or other engineering or technical discipline is required.

3. **Cybersecurity Engineer III**

**General Experience**
Six (6) years of relevant experience required.

Functional Responsibility
A Cybersecurity Engineer III has extensive IT experience in all aspects of Cyber Security with a vast array of IT systems involving end user as well as enterprise level networks. Experience in designing and implementing systems that meet agency Cyber Security policy and regulations. Must have extensive experience in Cyber Security Tools, network topologies, intrusion detection, PKI, and secured networks.

Minimum Education
Bachelor’s in computer science, electronics engineering or other engineering or technical discipline is required

4. Cyber Program Manager II

General Experience
Eight (8) years of professional experience in an information technology, management or related field.

Functional Responsibility
A Program Manager II is responsible for project oversight and direction. Ensures conformance with work standards; interprets policies, procedures, goals and objectives of the organization. Ensures appropriate resources are applied to the project. Nature of work involves complex information technology project management, strategic and tactical planning, coordination, control, and critical decision-making. Requires experience related to work being performed. May also involve complex technical engineering design and technology architectural tasks.

Minimum Education
A Bachelor's Degree in Information Technology, Business, Communications, or other technical or business discipline is required.

5. Subject Matter Expert II

General Experience
Minimum of seven (7) years of experience in an area of specialization associated with the requirement. Experience with Government or industry standards, processes, procedures, methodologies, or tools that support analysis as relative to the requirement.

Functional Responsibility
Has substantial expertise in a specific functional area. May direct analyses of requirements for information systems. May direct the design of adaptations to software. May be knowledgeable in
process analysis techniques such as flowcharting, process mapping, benchmarking, and activity-based costing. May have subject matter expertise in areas such as facilitation, organizational development, and change management. May have specific expertise in business or functional areas such as Reliability-Centered Maintenance principles and methodology, or logistics policy development. May have demonstrated experience in configuration management, maintenance planning, supply management, outfitting/fitting out, data management, training, or logistics/configuration information systems.

Minimum Education
Bachelor's Degree in computer science, electronics engineering or other engineering or technical discipline is required.

General Experience
Six (6) years of relevant experience required.

Functional Responsibility
A Cybersecurity Engineer III has extensive IT experience in all aspects of Cyber Security with a vast array of IT systems involving end user as well as enterprise level networks. Experience in designing and implementing systems that meet agency Cyber Security policy and regulations. Must have extensive experience in Cyber Security Tools, network topologies, intrusion detection, PKI, and secured networks.

Minimum Education
Bachelor’s in computer science, electronics engineering or other engineering or technical discipline is required

6. Subject Matter Expert III

General Experience
Minimum of ten (10) years of experience in an area of specialization associated with the requirement. Experience with Government or industry standards, processes, procedures, methodologies, or tools that support analysis as relative to the requirement.

Functional Responsibility
Has substantial expertise in a specific functional area. May direct analyses of requirements for information systems. May direct the design of adaptations to software. May be knowledgeable in process analysis techniques such as flowcharting, process mapping, benchmarking, and activity-based costing. May have subject matter expertise in areas such as facilitation, organizational development, and change management. May have specific expertise in business or functional areas such as Reliability-Centered Maintenance principles and methodology, or logistics policy development. May have demonstrated experience in configuration management, maintenance planning, supply management, outfitting/fitting out, data management, training, or
logistics/configuration information systems.

**Minimum Education**

Bachelor's Degree in computer science, electronics engineering or other engineering or technical discipline is required.