GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE CATALOG/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 is available through GSA Advantage!, a menu-driven database system. The INTERNET address for GSA Advantage! is http://www.gsaadvantage.gov

SCHEDULE TITLE: Multiple Award Schedule

FEDERAL SUPPLY GROUP: Professional Services

FSC Classes/Product Codes:
- DJ01 - IT and Telecom - Security and Compliance Support Services (Labor)

CONTRACT NUMBER: 47QTCA22D0037

CONTRACT PERIOD: January 14, 2022 through January 13, 2027

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

CONTRACTOR: Innovative Systems Group, Inc.
8480 Honeycutt Rd, Suite 200
Raleigh, NC, 27615-2261
919.844.8075
Keith.Kregg@ISGcyber.com
https://isgcyber.com/

CONTRACTOR’S ADMINISTRATION SOURCE:
Keith Kregg
8480 Honeycutt Rd, Suite 200
Raleigh, NC, 27615-2261
919.844.8075
Keith.Kregg@ISGcyber.com

BUSINESS SIZE: Small

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

*This is the MOST RECENTLY awarded Contractor Initiated Modification and does NOT include any Mass Modifications
Prices Shown Herein are Net (discount deducted)
CUSTOMER INFORMATION

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

<table>
<thead>
<tr>
<th>SINs</th>
<th>Recovery</th>
<th>SIN Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
</tbody>
</table>

1b. Lowest Priced Item: See Pricelist (Government net price based on a unit of one).

1c. Hourly Rates: See Pricelist (includes discount and IFF).

2. Maximum order: $500,000

Note to Ordering Activities: *If the best value selection places your order over the Maximum Order identified in this catalog/pricelist, you have an opportunity to obtain a better schedule contract price. Before placing your order, contact the aforementioned contactor for a better price. The contractor may (1) offer a new price for this requirement (2) offer the lowest price available under this contract or (3) decline the order. A delivery order that exceeds the maximum order may be placed under the schedule contract in accordance with FAR 8.404.

3. Minimum order: $100

4. Geographic coverage (delivery area): Domestic

5. Point(s) of production (city, county, and State or foreign country): 8480 Honeycutt Rd, Suite 200 Raleigh, NC, 27615-2261

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

7. Quantity discounts: 1.5% for orders over $150K; 1.75% for order over $275K

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

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

10a. Time of delivery: (Contractor insert number of days.) 30 days

10b. Expedited Delivery. Items available for expedited delivery are noted in this price list: 30 days or less, as negotiated with customer
10c. Overnight and 2-day delivery: Contact Contractor

10d. Urgent Requirements: Contact Contractor

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

12a. Ordering address(es): 8480 Honeycutt Rd, Suite 200, Raleigh, NC, 27615-2261

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

13. Payment address(es): 8480 Honeycutt Rd, Suite 200, Raleigh, NC, 27615-2261

14. Warranty provision: Standard Commercial Warranty Terms & Conditions

15. Export packing charges, if applicable: Not Applicable

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

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

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

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

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

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

21. Preventive maintenance (if applicable): Not Applicable

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

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

23. SAM UEI Number: ZSRQJNKH823
LABOR CATEGORY DESCRIPTIONS

**Cybersecurity Intrusion Analyst 1**

<table>
<thead>
<tr>
<th>Minimum Education: Bachelors</th>
<th>Minimum Experience: Two (2) years</th>
</tr>
</thead>
</table>

- Ensure security solutions are properly deployed and configured to protect the confidentiality, integrity and availability of the systems and data.
- Monitor, configure and tune security systems, such as Nessus, etc.
- Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. Research and make recommendations for new security controls and configurations.
- Work with other teams to troubleshoot issues and verify systems are deployed following security standards and guidelines.
- Create and maintain documentation for security tools used, and procedures followed as part of performing duties.
- Assist with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes) Work with end users to identify and mitigate security threats.
- Audit firewall configurations.
- Analyze the security policies and configurations and evaluate compliance with State laws, regulations and agency specific policies.
- Perform technical (evaluation of Technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, and supporting infrastructure).
- Perform analysis of log files from a variety of sources (e.g., Security Information and Event Management (SIEM) systems, individual host logs, network traffic logs, firewall logs, and Intrusion Detection Systems [IDS] logs) to identify possible threats to network security.
- Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.
- Ability to work individually or as a member of a team to design, develop, implement and maintain information security systems.
- Conduct and/or support authorized penetration testing on enterprise network assets
- Willingness and ability to learn other security concepts and tools.
- Knowledge, Skills and Abilities Recommended in this Position

- An understanding of network operations (i.e. how to configure and monitor networks, provide patches and updates)
- Knowledge of network theory, protocol and security practices (i.e. physical security controls, vulnerabilities and threats, network hardening techniques)
• Recognition of common threats, vulnerabilities, and malware and strategies to combat them
• Knowledge of security disciplines: identification, authentication, authorization, access control, administration and audit.
• Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
• Ability to identify systemic security issues based on the analysis of vulnerability and configuration data
• Knowledge of general attacks stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)
• Through understanding of the principles related to information technology security and risk assessment
• Understanding of information security concepts and terms including attack vectors, malware, APTs, backdoors, phishing, social engineering, etc.
• Strong analytical and problem-solving skills, customer-focus and expectation management and team-oriented interpersonal skills

Cybersecurity Intrusion Analyst 2

<table>
<thead>
<tr>
<th>Minimum Education: Bachelors</th>
<th>Minimum Experience: Two (2) years</th>
</tr>
</thead>
</table>

• Ensure security solutions are properly deployed and configured to protect the confidentiality, integrity and availability of the systems and data.
• Monitor, configure and tune security systems, such as Nessus, etc.
• Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. Research and make recommendations for new security controls and configurations.
• Work with other teams to troubleshoot issues and verify systems are deployed following security standards and guidelines.
• Create and maintain documentation for security tools used, and procedures followed as part of performing duties.
• Assist with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes) Work with end users to identify and mitigate security threats.
• Audit firewall configurations.
• Analyze the security policies and configurations and evaluate compliance with State laws, regulations and agency specific policies.
• Perform technical (evaluation of Technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, and supporting infrastructure).
• Perform analysis of log files from a variety of sources (e.g., Security Information and Event Management (SIEM) systems, individual host logs, network traffic logs, firewall logs, and Intrusion Detection Systems [IDS] logs to identify possible threats to network security.
• Prepare audit reports that identify technical and procedural findings, and provide recommended remediation
strategies/solutions.

Ability to work individually or as a member of a team to design, develop, implement and maintain information security systems.

- Conduct and/or support authorized penetration testing on enterprise network assets.
- Willingness and ability to learn other security concepts and tools.
- Knowledge, Skills and Abilities Recommended in this Position.
- An understanding of network operations (i.e. how to configure and monitor networks, provide patches and updates).
- Knowledge of network theory, protocol and security practices (i.e. physical security controls, vulnerabilities and threats, network hardening techniques).
- Recognition of common threats, vulnerabilities, and malware and strategies to combat them.
- Knowledge of security disciplines: identification, authentication, authorization, access control, administration and audit.
- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
- Knowledge of general attacks stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- Through understanding of the principles related to information technology security and risk assessment.
- Understanding of information security concepts and terms including attack vectors, malware, APTs, backdoors, phishing, social engineering, etc.
- Strong analytical and problem-solving skills, customer-focus and expectation management and team-oriented interpersonal skills.

---

**Cybersecurity Senior Analyst**

<table>
<thead>
<tr>
<th>Minimum Education:</th>
<th>Bachelors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Experience:</td>
<td>Two (2) years</td>
</tr>
</tbody>
</table>
• Implements computer system requirements by defining and analyzing system problems; designing and testing standards and solutions.
• Defines application problem by conferring with clients; evaluating procedures and processes.
• Develops solution by preparing and evaluating alternative workflow solutions.
• Controls solution by establishing specifications and coordinating production with programmers.
• Validates results by testing programs.
• Ensures operation by training client personnel and providing support.
• Provides reference by writing documentation.
• Accomplishes information systems and organization mission by completing related results as needed.
• In-depth knowledge of the TCP/IP protocol suite; security architecture; securing and hardening Operating Systems; Networks; Databases; and Applications.
• Knowledge of the Incident Response life-cycle, working independently to investigate and effectively respond to cyber security incidents

Cybersecurity Project Manager 1

Minimum Education: Bachelors
Minimum Experience: Two (2) years

• Manage and oversee all aspects of a project to ensure it is completed on-time and within budget.
• Define business requirements.
• Responsible for managing scope, cost, and schedule.
• Responsible for internal staffing.
• Manage outside vendors.
• Manage contractual deliverable.
• Prepare reports for upper management regarding status of project.

Cybersecurity Project Manager 2

Minimum Education: Bachelors
Minimum Experience: Two (2) years
| Manage and oversee all aspects of a project to ensure it is completed on-time and within budget. |
| Define business requirements. |
| Responsible for managing scope, cost, and schedule. |
| Responsible for internal staffing. |
| Manage outside vendors. |
| Manage contractual deliverable. |
| Prepare reports for upper management regarding status of project. |
## PRICING

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>Year 1 + IFF</th>
<th>Year 2 + IFF</th>
<th>Year 3 + IFF</th>
<th>Year 4 + IFF</th>
<th>Year 5 + IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Intrusion Analyst 1</td>
<td>$22.96</td>
<td>$23.51</td>
<td>$24.08</td>
<td>$24.65</td>
<td>$25.24</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Intrusion Analyst 2</td>
<td>$59.70</td>
<td>$61.13</td>
<td>$62.60</td>
<td>$64.10</td>
<td>$65.64</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Senior Analyst</td>
<td>$39.80</td>
<td>$40.76</td>
<td>$41.73</td>
<td>$42.73</td>
<td>$43.76</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Project Manager 1</td>
<td>$59.70</td>
<td>$61.13</td>
<td>$62.60</td>
<td>$64.10</td>
<td>$65.64</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Project Manager 2</td>
<td>$62.05</td>
<td>$63.54</td>
<td>$65.06</td>
<td>$66.63</td>
<td>$68.22</td>
</tr>
</tbody>
</table>

### Service Contract Labor Standards Matrix:

<table>
<thead>
<tr>
<th>SCLS Eligible Contract Labor Category/Fixed Price Service</th>
<th>SCLS Equivalent Code Title</th>
<th>WD Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>