GENERAL SERVICES ADMINISTRATION
Federal Supply Service
Authorized Federal Supply Schedule Price List

Multiple Award Schedule

54151HACS- Highly Adaptive Cybersecurity Services

Subcategories- High Value Asset (HVA) Assessments
Risk and Vulnerability Assessment (RVA)
Penetration Testing
Cyber Hunt
Incident Response

CONTRACT NUMBER: 47QTCA21D003U, Mod A815, effective January 6, 2021
CONTRACT PERIOD: January 6, 2021 through January 5, 2026

Next Level Solutions, LLC DBA CyberAssure
1025 Connecticut Avenue, NW, Suite 1000
Washington, DC 20037
Tel: (202) 625-4343
Web: www.next-level-solutions.com & www.cyberassure.net
SBA 8(a), MDOT MBE

Contracts Administrator
Andrew Valencia
Vice President
Tel: 202-625-4343 (Office)
202-681-5703 (Mobile)
E-mail: andrew.valencia@cyberassure.net
Customer Information

1.1 Authorized SINs

1.1.1 54151HACS- Highly Adaptive Cybersecurity Services
   Subcategories: High Value Asset (HVA) Assessments
   Risk and Vulnerability Assessment (RVA)
   Penetration Testing
   Cyber Hunt
   Incident Response
   Please see 54151HACS Subcategories Descriptions.

1.1.2 Labor Rates:
   Please see CyberAssure Labor Rates for Labor Rates.

1.1.3 Labor Category Descriptions:
   Please CyberAssure Labor Descriptions for Labor Descriptions.

1.2 Maximum Order:
   All approved SINs have a Maximum Order of $500,000.

1.3 Minimum Order:
   $100

1.4 Geographic Coverage (Delivery Area):
   W - World Wide

1.5 Point of Production:
   N/A.

1.6 Discount from List Prices:
   All prices listed are net prices.

1.7 Quantity Discounts:
   2% discount for all orders equal to or above $400,000

1.8 Prompt Payment Terms:
   No special discount is offered for prompt payment. Payment terms are net 30 days.

1.9 Acceptance of Government Credit Cards:
1.9.1 Government credit cards will be accepted for orders at or below the micro-purchase threshold.

1.9.2 Government credit cards will be accepted for orders above the micro-purchase threshold.

1.10 Foreign Items:
N/A

1.11 Time of Delivery:
To be specified for each task order by customer need

1.11.1 Expedited Delivery:
N/A

1.11.2 Overnight and 2-Day Delivery:
N/A

1.11.3 Urgent Requirements:
N/A

1.12 F.O.B. Points(s):
Destination

1.13 Ordering Address:
Next Level Solutions, LLC
Attention: Michael C. Hill, CEO & Andrew Valencia, Vice President
8220 Waterside Court
Fort Washington, MD 20744
(202) 681-5703 (Office)
(202)-498-0219 (Mobile)
Email: andrew.valencia@cyberassure.net

1.13.1 Ordering Procedures:
The ordering procedures for supplies and services, information on
Blanket Purchase Agreements (BPA), and a sample BPA can be found at the GSA/FSS Schedule homepage (http://fss.gsa.gov/schedules).

1.14 Payment Address:
Attn: Accounts Receivable
Next Level Solutions, LLC
8220 Waterside Court
Fort Washington, MD 20744
(202) 681-5703

1.15 Warranty Provision:
N/A
1.16 Export Packing Charges:
N/A

1.17 Terms and Conditions of Government Purchase Card Acceptance:
Government commercial credit cards will be acceptable for payments. Bank account information will be shown on the invoices.

1.18 Terms and Conditions of Rental, Maintenance, and Repair:
N/A

1.19 Terms and Conditions of Installation:
N/A

1.20 Terms and Conditions of Repair Parts Indicating Date of Parts Price Lists and Any Discounts from List Prices:
N/A

1.20.1 Terms and Conditions for Any Other Services:
N/A

1.21 List of Service and Distribution Points:
N/A

1.22 List of Participating Dealers:
N/A

1.23 Preventive Maintenance:
N/A

1.24 Special Attributes:
N/A

1.24.1 Section 508. If applicable, Section 508 compliance information on Electronic and Information Technology (EIT) supplies and services will be addressed on a task order basis. The EIT standards can be found at www.Section508.gov

1.25 Data Universal Numbering System (DUNS) Number:
049084836

1.26 Central Contractor Registration (CCR) Database:
Next Level Solutions, d/b/a CyberAssure, is registered in the System for Award Management.
## CyberAssure Labor Rates

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>Year 1 GSA PRICE + IFF</th>
<th>Year 2 GSA PRICE + IFF</th>
<th>Year 3 GSA PRICE + IFF</th>
<th>Year 4 GSA PRICE + IFF</th>
<th>Year 5 GSA PRICE + IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Specialist</td>
<td>$126.93</td>
<td>$129.21</td>
<td>$131.54</td>
<td>$133.91</td>
<td>$136.32</td>
</tr>
<tr>
<td></td>
<td>HVA Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RVA Penetration Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cyber Hunt Incident Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cybersecurity Specialist

Cybersecurity Specialists are experts in multiple cybersecurity disciplines, able to apply their expertise in an effort to meet customer requirements under 54151HACS and applicable subcategories.

Functional Responsibilities:

- Responsible for providing expert and technical advisement to the customer on advanced technical matters relating to the development, testing, evaluation, security, and utilization of new system architectures and computing technologies.
- Provides guidance and perspective on security threats and mitigation.
- Responsible for the design, development, implementation, and/or integration of new cybersecurity capabilities into IC enterprise architecture, system, or system component for use within computing environment (CE), network environment (NE), and enclave environments.
- Responsible for establishing authorization boundaries; establishing security or privacy alerts; assessing the severity of deficiencies in the system or controls; developing plans of action and milestones; creating risk mitigation approaches; and potential adverse effects of identified vulnerabilities or privacy risks.
- Performs comprehensive assessments, using both passive and active evaluations to determine the effectiveness of the security and privacy controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization).
- Responsible for testing and evaluating the security of CSSP security operations including auditing activities to test the “protect, detect, respond, and recover” (PDRR) capability of the CSSP through passive evaluations (compliance audits) and active evaluations (penetration tests and/or vulnerability assessments).
- Works autonomously on advanced, complex technical projects or business issues requiring state of the art technical or industry knowledge.
- Serves as a principal advisor on all matters, technical and otherwise, involving the security risk countermeasures and controls
- Conducts analysis, investigates and recommends security technologies. Ensures site security and provides consultation on security issues staying abreast of current malware and other potential internet security threats.
- Coordinates and conducts the day-to-day activities associated with managing risk to information systems and organizations
Minimum Experience/Education:

- Must possess a broad technical background and comprehensive expertise in cybersecurity implementation.
- Must be an expert on the NIST SP 800-53A, 800-37, ICD 503, CNSSI 1253, and related guidance.
- Must be an expert on both the technologies employed by target systems and the TTPs required to assess the effectiveness of controls.
- Must possess experience working within SIEM environments (expertise with Splunk, QRadar, ArcSight, NetWitness, LogRhythm, Tripwire, and similar technologies)

<table>
<thead>
<tr>
<th>Certification Requirements</th>
<th>Degree Requirements</th>
<th>Experience Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Workforce Management Program (DoDD 8140.01 &amp; DoD 8570.01-m) IAM III, IAT III, and IASAE II baseline certifications</td>
<td>Bachelor's degree (Computer Science, Information System Security, Network Security, and/or Cybersecurity)</td>
<td>5+ Years</td>
</tr>
</tbody>
</table>
CyberAssure Cybersecurity Specialists are qualified to provide specified services as designated under 54151HACS SIN Subcategories. CyberAssure has passed the required technical evaluation and received authorization to perform services in the following subcategories.

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Value Asset (HVA) Assessment</td>
<td>HVA Assessments include <strong>Risk and Vulnerability Assessment (RVA)</strong> 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 subcategory include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing. <strong>Security Architecture Review (SAR)</strong> 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. <strong>Systems Security Engineering (SSE)</strong> 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.</td>
</tr>
<tr>
<td>Risk and Vulnerability Assessment (RVA)</td>
<td>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.</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td><strong>Penetration Testing</strong> is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.</td>
</tr>
<tr>
<td>Cyber Hunt</td>
<td><strong>Cyber Hunt</strong> 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.</td>
</tr>
<tr>
<td>Incident Response</td>
<td><strong>Incident Response</strong> 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.</td>
</tr>
</tbody>
</table>