GENERAL SERVICES ADMINISTRATION
Federal Supply Schedule
Final Authorized Federal Supply Schedule Price List
FSC Group: MAS Schedule

On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order are available through GSA Advantage!®, a menu-driven database system. The INTERNET address GSA Advantage!® is: GSAAdvantage.gov

For more information on ordering from Federal Supply go to this website: www.gsa.gov/schedules

H2L Solutions
2227 Drake Ave., Building 3, Suite A
Huntsville, AL 35805
Tel: 256-679-9427
www.h2lsolutions.com

CONTRACT NUMBER: 47QTCA19D00E4
CONTRACT PERIOD: June 21, 2019 through June 20, 2024

CONTRACTOR’S ADMINISTRATION SOURCE: H2L Solutions
2227 Drake Avenue
Building 3, Suite A
Huntsville, AL 35805
Jonathan Hard
jonathan.hard@h2lsolutions.com

BUSINESS SIZE: Small Business

FSC/PSC Class D301
- IT & Telecom-Facility Operation and Maintenance

FSC/PSC Class D302
- IT & Telecom- Systems Development

FSC/PSC Class D306
- IT & Telecom – Systems Analysis

FSC/PSC Class D307
- IT & Telecom – IT Strategy & Architecture

FSC/PSC Class D308
- IT & Telecom – Programming

FSC/PSC Class D310
- IT & Telecom – Cyber Security & Data Backup

FSC/PSC Class D311
- IT & Telecom – Data Conversion

FSC/PSC Class D316
- IT & Telecom –Telecommunications Network Management

FSC/PSC Class D399
- IT & Telecom –Other IT & Telecommunications
CUSTOMER INFORMATION:

1a. TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs)

<table>
<thead>
<tr>
<th>SIN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>70-500</td>
<td>Order Level Materials (OLM)</td>
</tr>
</tbody>
</table>

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN:

Not Applicable

1c. HOURLY RATES (Services only):

<table>
<thead>
<tr>
<th>SIN</th>
<th>GSA Labor Category</th>
<th>Hourly Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Project Manager</td>
<td>$126.07</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Engineer- Senior</td>
<td>$196.98</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Engineer- Midlevel</td>
<td>$144.19</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Administrator</td>
<td>$112.67</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Associate</td>
<td>$88.25</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Technical Writer</td>
<td>$46.49</td>
</tr>
</tbody>
</table>

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: 48 states, Washington DC

5. POINT(S) OF PRODUCTION: N/A
6. **DISCOUNT FROM LIST PRICES:** 2.25%

7. **QUANTITY DISCOUNT(S):** None

8. **PROMPT PAYMENT TERMS:** None

9.a Government Purchase Cards must be accepted at or below the micro-purchase threshold.

9.b Government Purchase Cards are accepted above the micro-purchase threshold. Contact contractor for limit.

10. **FOREIGN ITEMS:** None

11a. **TIME OF DELIVERY:** Negotiated with Ordering Agency

11b. **EXPEDITED DELIVERY:** Negotiated with Ordering Agency

11c. **OVERNIGHT AND 2-DAY DELIVERY:** Negotiated with Order Agency

11d. **URGENT REQUIREMENTS:** Negotiated with Ordering Agency

12. **FOB POINT:** Destination

13a. **ORDERING ADDRESS:** Same as contractor

13b. **ORDERING PROCEDURES:** Ordering activities shall use the ordering procedures described in Federal Acquisition Regulation 8.405-3 when placing an order or establishing a BPA for supplies or services. The ordering procedures, information on Blanket Purchase Agreements (BPA’s) and a sample BPA can be found at the GSA/FSS Schedule Homepage ([fss.gsa.gov/schedules](http://fss.gsa.gov/schedules)).

14. **PAYMENT ADDRESS:** Same as contractor

15. **WARRANTY PROVISION:** N/A

16. **EXPORT PACKING CHARGES:** N/A

17. **TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE:** N/A

18. **TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR (IF APPLICABLE):** N/A

19. **TERMS AND CONDITIONS OF INSTALLATION (IF APPLICABLE):** N/A

20. **TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE):** N/A

20a. **TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE):** N/A

21. **LIST OF SERVICE AND DISTRIBUTION POINTS (IF APPLICABLE):** N/A

22. **LIST OF PARTICIPATING DEALERS (IF APPLICABLE):** N/A
23. PREVENTIVE MAINTENANCE (IF APPLICABLE): N/A

24a. SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants): N/A

24b. Section 508 Compliance for Electronic and Information Technology (EIT): As applicable

25. DUNS NUMBER: 079515723

26. NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE: Contractor has an Active Registration in the SAM database

Awarded Labor Categories

<table>
<thead>
<tr>
<th>Cybersecurity Project Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Plans, directs and coordinates the efforts involving resources necessary to accomplish cyber program objectives.</td>
</tr>
<tr>
<td>- Initiates, supports and participates in overall cyber program management, coordinating with Program Managers on any and all cybersecurity tasks.</td>
</tr>
<tr>
<td>- Tracks development lifecycle of systems and software and implements SDLC best practices and methodology</td>
</tr>
<tr>
<td>- Analyzes current situation and contract requirements and develops plans, strategy, and implementation of efforts to achieve program goals and to mitigate further risk.</td>
</tr>
<tr>
<td>- Tracks progress of cybersecurity compliance and accreditation processes and development of authorization packages.</td>
</tr>
<tr>
<td>- Determines cyber requirements and translates these requirements into operational plans for penetration testing, vulnerability assessments, and software architectural review.</td>
</tr>
<tr>
<td>- Determines, monitors, and reviews costs, operational budgets, and schedules and staffing requirements for cyber project team, including cybersecurity training standards and requirements.</td>
</tr>
<tr>
<td>- Analyzes effects of project upon various operating and support areas, such as information processing/data centers, incident response, assembly and manufacturing, to determine the most practical and cost-effective method to obtain the required resources.</td>
</tr>
<tr>
<td>- Provides guidance to project cyber team and management in directing development of new applications and formulating contingency plans in areas such as penetration testing, schedule revisions, manpower adjustments, fund allocations, and work requirements.</td>
</tr>
<tr>
<td>- Provides guidance in strategic systems planning to project team.</td>
</tr>
</tbody>
</table>

**Knowledge, Skills, Abilities:**
The ability to assist in the development of tasks during project development, expertise in the management and control of funds and resources using electronic reporting mechanisms, demonstrated capability in managing multi-task contracts and/or subcontracts of various types, and complexity. General experience includes increasing responsibilities in information systems design and/or management. Excellent communication skills and experience multitasking in a high-pressure environment. Experience with Microsoft Project or other project management software.

**Minimum Experience:** 4 years

**Minimum Education Requirements:** Bachelor’s Degree
### Cybersecurity Engineer Senior Level

**Description:**
Provides knowledge in design, architecture, development and administration. The Cyber Security Engineer may:

- Monitor existing cyber systems for structural integrity for future risk.
- Oversee the development and installation of new hardware and software so as to mitigate potential threats.
- Install and configure operating systems and other software and routinely test installed software for glitch detection and other issues.
- Create scalable, automated solutions for our customer base.
- Establish multi-platform versions of the software package and network mapping.
- Write penetration tests for existing and created code to ensure compatibility and stability.
- Design, implement, and conduct test and evaluation procedures to ensure system requirements are met and to identify specific vulnerabilities.
- Evaluate cyber hardware and software and resolve LAN/MAN/WAN network related problems.

**Knowledge, Skills, Abilities:**
Ability to provide technical direction to cyber IT support staff, design and implement cost effective cyber security systems and redundant backups to maintain data safety to mitigate risk, and write custom scripts to reduce the need for human intervention. Knowledge of applicable regulations and directives (e.g. Army Regulations, Department of Defense Directives, etc.) and published resources (e.g. National Institute of Standards and Technology [NIST] Special Publications [SPs] and Federal Information Processing Standards [FIPs]) and how they relate to technical security control implementation and development of policies and procedures. Understanding of Risk Management Framework (RMF) and NIST SP 800-53 security controls.

**Minimum Experience:** 4 years

**Minimum Education Requirements:** Bachelor’s Degree

### Cybersecurity Engineer Mid Level

**Description:**
Provides knowledge in design, architecture, development and administration. The Cyber Security Engineer may:

- Monitor existing cyber systems for structural integrity for future risk.
- Oversee the development and installation of new hardware and software so as to mitigate potential threats.
- Install and configure operating systems and other software and routinely test installed software for glitch detection and other issues.
- Create scalable, automated solutions for our customer base.
- Establish multi-platform versions of the software package and network mapping.
- Write penetration tests for existing and created code to ensure compatibility and stability.
- Evaluate, recommend, and implement automated test tools and strategies intended to help...
with incident response.
- Design, implement, and conduct test and evaluation procedures to ensure system requirements are met and to identify specific vulnerabilities.
- Evaluate cyber hardware and software and resolve LAN/MAN/WAN network related problems.

**Knowledge, Skills, Abilities:**
Ability to provide technical direction to cyber IT support staff, design and implement cost effective cyber security systems and redundant backups to maintain data safety to mitigate risk, and write custom scripts to reduce the need for human intervention. Basic knowledge of applicable regulations and directives (e.g. Army Regulations, Department of Defense Directives, etc.) and published resources (e.g. National Institute of Standards and Technology [NIST] Special Publications [SPs] and Federal Information Processing Standards [FIPs]) and how they relate to technical security control implementation. Understanding of Risk Management Framework (RMF), safeguarding Controlled Unclassified Information (CUI), and implementation of security controls.

**Minimum Experience:** 2 years

**Minimum Education Requirements:** Associate’s Degree

---

**Cybersecurity Administrator**

**Description:**
- Provide mission applications focused expertise for the IT user.
- Assist with installation and configuration of new software applications.
- Produce and/or contribute to IT knowledge articles.
- Network Mapping - consists of identifying assets on an agreed upon IP address space or network range(s).
- Vulnerability Scanning - comprehensively identifies IT vulnerabilities associated with agency systems that are potentially exploitable by attackers.
- Phishing Assessment - includes activities to evaluate the level of awareness of the agency workforce with regard to digital form of social engineering that uses authentic looking, but bogus, emails request information from users or direct them to a fake Website that requests information. Phishing assessments can include scanning, testing, or both and can be conducted as a one- time event or as part of a larger campaign to be conducted over several months.
- Wireless Assessment - includes wireless access point (WAP) detection, penetration testing or both and is performed while onsite at a customer’s facility.
- Web Application Assessment - includes scanning, testing or both of outward facing web applications for defects in Web service implementation may lead to exploitable vulnerabilities. Provide report on how to implement Web services securely and that traditional network security tools and techniques are used to limit access to the Web Service to only those networks and systems that should have legitimate access.
- Operating System Security Assessment (OSSA) - assesses the configuration of select host operating systems (OS) against standardized configuration baselines. Database Assessment - assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities.
- Penetration Testing - conducting and/or supporting authorized Penetration Testing on enterprise network assets.
Knowledge, Skills, Abilities:
Has working knowledge of computer operations, platforms, systems, architectures, functions, and terminology.
Ability to read, write and implement standard operating procedures and technical documentation. Has the ability to interact effectively, courteously, and directly with the user to resolve technical issues. Respond to queries and requests for service. Knowledge of applicable regulations and directives and published resources. Understanding of risk management process and frameworks, safeguarding information according to classifications, and implementation of security controls.

Minimum Experience: 4 years
Minimum Education Requirements: Bachelor’s Degree

Cybersecurity Associate

Description:
- Provide mission applications focused expertise for the IT user.
- Assist with installation and configuration of new software applications.
- Produce and/or contribute to IT knowledge articles.
- Network Mapping - consists of identifying assets on an agreed upon IP address space or network range(s).
- Vulnerability Scanning - comprehensively identifies IT vulnerabilities associated with agency systems that are potentially exploitable by attackers.
- Phishing Assessment - includes activities to evaluate the level of awareness of the agency workforce with regard to digital form of social engineering that uses authentic looking, but bogus, emails request information from users or direct them to a fake Website that requests information. Phishing assessments can include scanning, testing, or both and can be conducted as a one-time event or as part of a larger campaign to be conducted over several months.
- Wireless Assessment - includes wireless access point (WAP) detection, penetration testing or both and is performed while onsite at a customer’s facility.
- Web Application Assessment - includes scanning, testing or both of outward facing web applications for defects in Web service implementation may lead to exploitable vulnerabilities. Provide report on how to implement Web services securely and that traditional network security tools and techniques are used to limit access to the Web Service to only those networks and systems that should have legitimate access.
- Operating System Security Assessment (OSSA) - assesses the configuration of select host operating systems (OS) against standardized configuration baselines. Database Assessment - assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities.
- Penetration Testing - conducting and/or supporting authorized Penetration Testing on enterprise network assets.

Knowledge, Skills, Abilities:
Has working knowledge of computer operations, platforms, systems, architectures, functions, and terminology.
Ability to read, write and implement standard operating procedures and technical documentation. Has the ability to interact effectively, courteously, and directly with the user to resolve technical issues. Respond to queries and requests for service. Basic knowledge of applicable regulations and directives (e.g. Army Regulations, Department of Defense Directives, etc.) and published resources (e.g. National
Institute of Standards and Technology [NIST] Special Publications [SPs] and Federal Information Processing Standards [FIPs]). Basic understanding of Risk Management Framework (RMF) and DFARS 252.204-7012 compliance.

**Minimum Experience:** 2 years  
**Minimum Education Requirements:** Associate’s Degree

---

**Technical Writer**

**Description:**
- Functions as a communications and information specialist, preparing material for publications and other media internally and externally.
- Works with customers to develop documentation necessary for compliance and accreditation packages, including system categorization memorandums, security control family policies, standard operating procedures (SOPs), system security plans (SSPs), system descriptions, system configuration guides, risk assessment reports, privacy impact assessments, configuration management plans, contingency plans, incident response (IR) plans, and continuous monitoring strategies.
- Develop, draft, and conduct quality control (QC) of technical reports, tailoring them for different audiences: (1) Executive summaries for system owners and general management, (2) High-level technical reports for IT managers and CISOs, and (3) Detailed technical reports for IT implementers and software developers. These reports are used to establish and/or document system and process milestones and objectives.
- Gathers information; writes and edits technical, promotional and general interest materials; and coordinates publications and other collateral material using both print and electronic media including the web and desktop publishing software to draft, edit, and lay out material for distribution.
- Has responsibility for final reviews of proposed publications for style, design, layout, and editorial aspects before government approval.

**Knowledge, Skills, Abilities:**
Must have ability to write clearly and the skills to express ideas graphically. Ability to interact with SMEs. General understanding of cyber security activities and published resources.

**Minimum Experience:** 2 years  
**Minimum Education Requirements:** Bachelor’s degree in related field

---

Due to the availability or limitation of education, occasionally substitution of experience as referenced below for a professional labor type with additional years of experience will be provided to the Federal Agency when responding to their IT requirements and it is solely the acquiring agency’s determination, if the substitution is considered acceptable prior to an award.

**Experience Substitutions:**
- An Associate’s Degree may be substituted for 3 years of required relevant IT experience with a High School Diploma
- A Bachelor’s Degree may be substituted with Associate Degree + 1 years additional relevant IT experience
A Bachelor’s Degree may be substituted for 4 years of required relevant IT experience with a High School Diploma
A Master’s Degree may be substituted with Bachelor’s Degree + 2 years additional relevant IT experience
A Master’s Degree may be substituted for 2 years of required relevant IT experience with a Bachelor’s Degree
A Ph.D. may be substituted with Master’s Degree + 4 years additional relevant IT experience
A Ph.D. may be substituted with 6 years relevant IT experience with a Bachelor’s Degree