Multiple Award Schedule (MAS)

Special Item Numbers:
54151HACS – Highly Adaptive Cybersecurity Services (HACS)
541515S - IT Professional Services
OLM - Order-Level Materials

Business Size: Small

Woman-Owned Small Business (WOSB)
Economically Disadvantage Women-Owned Small Business (EDWOSB)
Veteran-Owned Small Business (VOSB)

L2 Cyber Solutions
6635 S. Dayton Street
Suite 130
Greenwood Village, CO 80111
+1 (303) 495-5908
www.L2Cyber.com
e-mail: connect@L2Cyber.com
Contract Administration: costrom@L2Cyber.com

CONTRACT AWARD NUMBER:
GS-35F-201DA

Contract Period:
February 26, 2016 through February 25, 2026
Contract current through Modification PS-0032, effective September 17, 2021

General Services Administration
Federal Supply Service

Services and ordering information in this Information Technology Schedule Pricelist are also available on the GSA Advantage! System. Agencies can browse GSA Advantage! by accessing the Federal Supply Service at http://www.fss.gsa.gov/
INFORMATION FOR ORDERING ACTIVITIES

1a. AUTHORIZED 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>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>OLM</td>
<td>Order-Level Materials (OLMs)</td>
</tr>
</tbody>
</table>

1b. Lowest Priced Model Number and Price for each SIN: See Price List

1c. SERVICES OFFERED: See Price List

2. MAXIMUM ORDER PER SIN:

<table>
<thead>
<tr>
<th>SIN</th>
<th>MAXIMUM ORDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>$500,000</td>
</tr>
<tr>
<td>54151S</td>
<td>$500,000</td>
</tr>
<tr>
<td>OLM</td>
<td>$100,000</td>
</tr>
</tbody>
</table>

This maximum order threshold is a dollar amount at which it is suggested that the ordering agency request higher discounts from the contractor before issuing the order. The contractor may: (1) Offer a new lower price, (2) Offer the lowest price available under the contract, or (3) Decline the order within five (5) days. In accordance with the Maximum Order provisions contained in the Schedule, a delivery order may be placed against the Schedule contract even though it exceeds the maximum order threshold.

3. MINIMUM ORDER LIMITATION: $100


5. POINT OF PRODUCTION: United States

6. BASIC DISCOUNT: Prices listed are net, discounts have been deducted and the industrial funding fee has been added

7. QUANTITY DISCOUNT: 1% for orders greater than $1,000,000

8. PROMPT PAYMENT TERMS: None, Net 30. Information for Ordering Offices; Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9. FOREIGN ITEMS: None.

10a. TIME OF DELIVERY: As negotiated

10b. EXPEDITED DELIVERY: Contact Contractor

10c. OVERNIGHT AND 2-DAY DELIVERY: Contact Contractor

10d. URGENT REQUIREMENTS: Contact Contractor

11. F.O.B. POINT: FOB Destination

12a. ORDERING ADDRESS: L2 CYBER SOLUTIONS
    6635 S. DAYTON STREET
    SUITE 130
    GREENWOOD VILLAGE, CO 80111-6109
    TAX ID#: 26-2206617
ORDERING PROCEDURES: For supplies and service the ordering procedures, information on Blanket Purchase Agreements (BPAs), and a sample BPA may be found at the GSA/FSS Schedule homepage (gss.gsa.gov/schedule).

PAYMENT ADDRESS: Same as Ordering Address

WARRANTY PROVISION: Standard Commercial Warranty

EXPORT PACKING CHARGES: Not Applicable

TERMS AND CONDITIONS OF RENTAL: Not Applicable

TERMS AND CONDITIONS OF INSTALLATION: Not Applicable

TERMS AND CONDITIONS OF REPAIR PARTS: Not Applicable

TERMS AND CONDITIONS FOR ANY OTHER SERVICES: Not Applicable

LIST OF SERVICE AND DISTRIBUTION POINTS: Not Applicable

LIST OF PARTICIPATING DEALERS: Not Applicable

PREVENTIVE MAINTENANCE: Not Applicable

SPECIAL ATTRIBUTES: Not Applicable

SECTION 508 COMPLIANCE INFORMATION: Not Applicable

UNIQUE ENTITY IDENTIFIER NUMBER: VE1KPVF275D4

CONTRACTOR HAS REGISTERED IN THE SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE.
About L2 Cyber Solutions

L2 Cyber Solutions (L2 Cyber) formerly known as L Squared LLC is a highly technical Economically Disadvantaged Women Owned Small Business (EDWOSB) and Veteran Owned Small Business (VOSB) that has been providing IT Services, Infrastructure expertise and Management Consulting since 2008. L2 Cyber has a proven success record working with clients to solve complex organization and management problems centered around mission-oriented business solutions. Through L2 Cyber’s proprietary process of program planning, audits, evaluations, and approach, we are able to transfer knowledge and capabilities to our clients.

Founded to help customers meet their mission needs, L2 Cyber leverages technology to identify and implement the right solutions. As a strategic partner and advisor, L2 Cyber helps organizations achieve enterprise-wide, mission critical IT solutions through innovation, security, reliability, and efficiency. These solutions are built on mature enterprise architecture and best practices, which enables us to deliver cost saving services.

Our staff is comprised of highly experienced consultants and practitioners who work at all levels of an organization from executive office to the front line. Our core strengths include mission critical operations and maintenance, infrastructure domain consolidation, big data storage, business management, information assurance, and risk management.

IT SERVICES

<table>
<thead>
<tr>
<th>CYBERSECURITY</th>
<th>INFRASTRUCTURE</th>
<th>IT SUPPORT SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk and Vulnerability Assessments</td>
<td>Cloud Strategies</td>
<td>Security Engineering</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>Data Storage</td>
<td>Program Governance</td>
</tr>
<tr>
<td>Continuous Monitoring</td>
<td>High Performance Computing</td>
<td>Operations &amp; Management Support</td>
</tr>
<tr>
<td>Security Operations</td>
<td></td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>Business Continuity Plan</td>
<td></td>
<td>Network Design</td>
</tr>
<tr>
<td>Enterprise Cybersecurity Solutions</td>
<td></td>
<td>System Implementation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Property Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technical Documentation</td>
</tr>
</tbody>
</table>
L2 Cyber Solutions has the following labor categories. Each labor category’s commercial job title, minimum education requirements, minimum general experience, as well as functional responsibilities are outlined below. L2 Cyber Solutions hourly GSA price (with IFF) for each labor category is included in the table.

**GSA RATES**

**HIGHLY ADAPTIVE CYBERSECURITY SERVICES**

**SIN 54151HACS**

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>September 17, 2021-September 16, 2022</th>
<th>September 17, 2022-September 16, 2023</th>
<th>September 17, 2023-September 16, 2024</th>
<th>September 17, 2024-September 16, 2025</th>
<th>September 17, 2025-February 25, 2026</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSA Hourly Rate</td>
<td>$130.89</td>
<td>$133.51</td>
<td>$136.18</td>
<td>$138.91</td>
<td>$141.68</td>
</tr>
<tr>
<td>Cybersecurity Subject Matter Expert (SME) II</td>
<td>$144.55</td>
<td>$147.44</td>
<td>$150.39</td>
<td>$153.39</td>
<td>$156.46</td>
</tr>
<tr>
<td>Cybersecurity Subject Matter Expert (SME) III</td>
<td>$162.89</td>
<td>$162.89</td>
<td>$166.15</td>
<td>$169.47</td>
<td>$172.86</td>
</tr>
<tr>
<td>Cybersecurity Program Manager IV</td>
<td>$121.19</td>
<td>$123.61</td>
<td>$126.08</td>
<td>$128.61</td>
<td>$131.18</td>
</tr>
<tr>
<td>Cybersecurity Project Manager II</td>
<td>$124.22</td>
<td>$126.70</td>
<td>$129.24</td>
<td>$131.83</td>
<td>$134.46</td>
</tr>
<tr>
<td>Cybersecurity Architect II</td>
<td>$124.22</td>
<td>$126.70</td>
<td>$129.24</td>
<td>$131.83</td>
<td>$134.46</td>
</tr>
<tr>
<td>Cybersecurity Architect III</td>
<td>$141.71</td>
<td>$144.55</td>
<td>$147.44</td>
<td>$150.39</td>
<td>$153.39</td>
</tr>
<tr>
<td>Cybersecurity Technical Specialist II</td>
<td>$120.60</td>
<td>$123.02</td>
<td>$125.48</td>
<td>$127.99</td>
<td>$130.55</td>
</tr>
<tr>
<td>Cybersecurity Analyst II</td>
<td>$124.22</td>
<td>$126.70</td>
<td>$129.24</td>
<td>$131.82</td>
<td>$134.46</td>
</tr>
<tr>
<td>Cybersecurity Analyst III</td>
<td>$134.38</td>
<td>$137.07</td>
<td>$139.81</td>
<td>$142.61</td>
<td>$145.46</td>
</tr>
<tr>
<td>Cybersecurity Information Assurance Specialist III</td>
<td>$124.22</td>
<td>$126.70</td>
<td>$129.24</td>
<td>$131.83</td>
<td>$134.46</td>
</tr>
<tr>
<td>Cybersecurity Disaster Recovery Specialist IV</td>
<td>$121.19</td>
<td>$123.61</td>
<td>$126.08</td>
<td>$128.61</td>
<td>$131.18</td>
</tr>
<tr>
<td>Cybersecurity Technical Writer-Documentation Specialist</td>
<td>$117.44</td>
<td>$119.79</td>
<td>$122.19</td>
<td>$124.63</td>
<td>$127.12</td>
</tr>
</tbody>
</table>
**CYBERSECURITY SUBJECT MATTER EXPERT (SME) II**

Provide technical knowledge and analysis of highly specialized cyber/information assurance applications and operational environment, high-level functional systems analysis, design, integration, documentation, and implementation advice on moderately complex problems that require an appropriate level of knowledge of the subject matter for effective implementation. Apply principles, methods, and knowledge of the cyber functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions. Assist other senior consultants with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: information systems architecture, networking; telecommunications, automation; communications protocols, risk management/electronic analysis, software; lifecycle management, software development methodologies, and modeling and simulation.

**Minimum Education:** Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Six (6) years

**CYBERSECURITY SUBJECT MATTER EXPERT (SME) III**

Provide technical knowledge and analysis of highly specialized cyber/information assurance applications and operational environment, high-level functional systems analysis, design, integration, documentation, and implementation advice on moderately complex problems that require an appropriate level of knowledge of the subject matter for effective implementation. Apply principles, methods, and knowledge of the cyber functional area of capability to specific task order requirements, advanced mathematical principles, and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions. Assist other senior consultants with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: information systems architecture, networking; telecommunications, automation; communications protocols, risk management/electronic analysis, software; lifecycle management, software development methodologies, and modeling and simulation.

**Minimum Education:** Master's Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Eight (8) years

**CYBERSECURITY PROGRAM MANAGER IV**

Required to have at least eight (8) years of Program Management experience and/or Cyber management experience. Exercises independent judgment and solves technical, administrative, and managerial problems. Has ultimate responsibility for planning and coordinating staff, and managing costs, quality, and schedule. Manages teams of contract support personnel at multiple locations and maintains and manages the client interface at senior levels of the client organization. Meets with customer and contractor personnel to formulate and review task plan and deliverables. Ensures conformance with program task schedules and costs.

**Minimum Education:** Master’s Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Eight (8) years

**CYBERSECURITY PROJECT MANAGER II**
Provides support in the planning and execution of Assessment and Authorization (A&A) Projects. Develops project schedules, tracks milestones and deliverables. Conducts meetings and communicates status to project stakeholders. Provides technical and subject matter oversight and takes corrective action as necessary to ensure project success. Manages staffing, budget, prioritization, and other personnel matters. Provides project management oversight for each step in the NIST RMF Process.

**Minimum Education:** Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Four (4) years

**CYBERSECURITY PROJECT MANAGER III**

Responsible for the planning and execution of Assessment and Authorization (A&A) Projects. Prepares and delivers status reports to the customer. Primary point contact for the customer. Provides technical and subject matter oversight and takes corrective action as necessary to ensure project success. Manages staffing, budget, prioritization, and other personnel matters. Provides project management oversight for each step in the NIST RMF Process.

**Minimum Education:** Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Six (6) years

**CYBERSECURITY ARCHITECT II**

Assists in the development of enterprise-wide or large-scale information systems. Design architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross functional cyber requirements and interfaces. Ensure these systems are compatible and in compliance with industry best practices and standards. Ensure that the common operating environment is compliant with the Agency enterprise architecture and applicable reference models. Evaluate analytically and systematically problems of workflows, organization, and planning and develop appropriate corrective action.

**Minimum Education:** Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Four (4) years

**CYBERSECURITY ARCHITECT III**

Responsible system information cyber requirements using analysis of the information engineer(s) in the development of enterprise-wide or large-scale information systems. Design architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross functional cyber requirements and interfaces. Ensure these systems are compatible and in compliance with best practices and standards. Ensure that the common operating environment is compliant with the Agency enterprise architecture and applicable reference models. Evaluate analytically and systematically problems of workflows, organization, and planning and develop appropriate corrective action.

**Minimum Education:** Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Six (6) years

**CYBERSECURITY TECHNICAL SPECIALIST II**

GS-35F-201DA

**Minimum Education:** Bachelor's Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Four (4) years

**CYBERSECURITY ANALYST II**

Supports security compliance audits IAW NIST and industry best practices and standards. Reviews management, operational and technical control implementation against organizational policies and procedures and identifies deficiencies. Validates technical control implementation by performing vulnerability scanning, penetration testing, audit log reviews etc. Assists in the development and implements assessment validation tools. Provides technical input for the development of Rules of Engagement (ROE), Pentest and Vulnerability Assessment Reports (VAR) and provides input in preparing risk assessment reports (RAR) and security assessment reports (SAR).

**Minimum Education:** Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Four (4) years

**CYBERSECURITY ANALYST III**

Responsible for conducting security compliance audits IAW NIST and industry best practices and standards. Reviews management, operational and technical control implementation against organizational policies and procedures and identifies deficiencies. Validates technical control implementation by performing vulnerability scanning, penetration testing, audit log reviews etc. Assists in the development and implements assessment validation tools and determining overall risk assessment and recommend mitigations. Provides technical input for the development of Rules of Engagement (ROE), Pentest and Vulnerability Assessment Reports (VAR) and provides input in preparing risk assessment reports (RAR) and security assessment reports (SAR). Responsible for the development of assessment scenarios, and Security Assessment Plan (SAP).

**Minimum Education:** Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:** Six (6) years

**CYBERSECURITY INFORMATION ASSURANCE SPECIALIST III**

Responsible for the implementation of the Risk Management Framework and ensures information system-related security risks are implemented and managed consistent with organizational business and mission objectives and the overall risk strategy. Develop, maintain, and implement the security documentation (SSP, security CONOPS, business cases, and risk management matrices) IAW customer directives throughout the information systems RMF lifecycle Interprets government regulations, directives, policies and procedures. Draft and implement local operating instructions, procedures, and guidelines. Evaluate and approve addition of hardware and software. Present security briefings and train users on information systems security requirements, policy, and procedures. Identify, investigate, report, and implement corrective actions regarding security violations and incidents.
Minimum Education: Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

Minimum/General Experience: Six (6) years

CYBERSECURITY DISASTER RECOVERY SPECIALIST IV

Provide support in the development of a Government Agencies cyber incident management and business recovery plans; perform functions pertaining to the agencies business risk assessments; review and develop business cyber recovery strategies; draft procedures for identifying failures and invoking contingency plans; create response procedures and identifying communications channels; communicate with various response teams during testing and actual execution of recovery procedures. Support the design, development, installation, implementation, and administration of backup solutions. Make recommendations to the user community and the operations group on system enhancements.

Minimum Education: Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

Minimum/General Experience: Six (6) years

CYBERSECURITY TECHNICAL WRITER-DOCUMENTATION SPECIALIST

Assists in writing cyber-related technical documents, including reports, user manuals, briefings and presentations, functional descriptions, system specifications, guidelines, special reports, and other project deliverables to meet contract requirements. Develop outlines and drafts for review and approval by technical cyber specialists and project management ensuring that final documents meet applicable contract requirements and regulations. Research and gather cyber-related technical and background information for inclusion in project documentation and deliverables.

Minimum Education: Bachelor’s Degree. Three years of experience may be substituted for degree requirements.

Minimum/General Experience: Four (4) years
### IT PROJECT MANAGER II

Responsible for planning and execution of IT projects. Prepares and oversees project schedules, budgets and work of assigned personnel, applying relevant experience and expertise in the implementation of technical and operational projects and programs. Provides technical and subject matter oversight anticipating technical and operational challenges and risks. Coordinates with the client stakeholders to address program/project related issues. Provides day-to-day management of client engagements, potentially over multiple projects and/or sites, with minimal oversight and support. Monitors project tasks and keeps leadership informed of project status. Prepares and delivers status report to stakeholders as primary point of contact for the customer.

**Minimum Education:** Bachelor’s Degree in Computer Science, Engineering or Information Systems or related discipline. Three years of experience may be substituted for degree requirements.

**Minimum/General Experience:**

Four (4) or more years managing and performing client engagements in consulting, cybersecurity, IT, systems analysis and solutions architecture, system design and implementation. The Project Manager is typically able to manage one or more client engagement with minimal executive oversight and support. A relevant advanced degree may be substituted for 1 to 2 years of experience. Major professional certifications typically required (PgMP, PMP, CAP, CISSP, CISA, CEH, CISM, etc.)

### SYSTEM SECURITY ENGINEER II

Applies experience and technical knowledge to support security architecture, policy and design guidance for systems and networks. Provides certification and accreditation support for application systems, and networks in accordance with appropriate customer policies. Roles could include plan of action and milestone analysis, privacy analysis and policy analysis. Documentation support could include scan results, system security plans (SSPs), system assessment plans (SAPs), system assessment reports (SARs), contingency plans. May support defining and assessing appropriate security procedures, network access rules, configuration management, and technical controls. May develop risk assessment schedules, reviewing continuous monitoring and vulnerability scans. Works under general supervision.

**Minimum Education:** Bachelor’s Degree in Computer Science, Engineering or Information Systems or related discipline.
Minimum/General Experience:

Four (4) years of information technology (IT) or related experience. A relevant advanced degree may be substituted for 1 to 2 years of experience. Each major professional certification (PgMP, PMP, CAP, CISSP, CISA, CEH, CISM, etc.) may also be substituted for 1 year of experience.

Familiar with standard concepts, practices, and procedures within the cybersecurity field. Experience in security control assessments, penetration testing, risk and vulnerability analysis, incident response, information assurance, system analysis and solution architecture, testing, implementation, program management and other related services.

**SYSTEM SECURITY ENGINEER III**

Applies highly specialized experience and highly advanced technical knowledge to advise team members and client. Analyzes information security system, applications, and requirements. Designs, develops, engineers, and implements solutions aligned with organizational security requirements and architecture. Develops security measures to protect information against unauthorized modification or loss. Gathers technical information about an organization's mission, goals and needs, existing security products and ongoing security initiatives. Serves as a subject matter specialist resource in one or more IT fields such as cybersecurity and governance, system implementation, disaster recovery, IT contingency planning, IT infrastructure modernization. Stays abreast of new technologies, regulatory compliance requirements, and changing practices in IT management. May perform daily supervision and direct staff. Typically reports to a project leader or manager.

Minimum Education: Master's Degree in Computer Science, Engineering or Information Systems or related discipline.

Minimum/General Experience:

Six years or more years managing and performing client engagements in consulting, cybersecurity, IT, systems analysis and solutions architecture, system design and implementation. Experience in security control assessments, penetration testing, risk and vulnerability analysis, incident response, information assurance, system analysis and solution architecture, testing, implementation, program management, or other related services. A relevant advanced degree may be substituted for 1 to 2 years of experience. Each major professional certification (PgMP, PMP, CAP, CISSP, CISA, CEH, CISM, etc.) may also be substituted for 1 year of experience.

**SYSTEM SECURITY ENGINEER IV**

Applies highly specialized experience and advanced technical knowledge to advise team members and client. Responsible for supporting the development and implementation of technical methodologies in risk and vulnerability, analysis, incident response, disaster recovery, database protection, software development and information assurance. Typically serves as primary point of contact for client projects working directly with the project sponsor and stakeholders. Serves as a subject matter expert in one or more IT fields such as cybersecurity and governance, system implementation, disaster recovery, IT contingency planning, IT infrastructure modernization. Works with client leadership in resolving project issues related to technical compatibility, stakeholder requirements, timing, and sequencing of initiatives. Able to manage large teams and/or complex projects and coordinate across multiple client engagements. Supervises subordinate staff and/or managers, and assures quality of work products, services, and deliverables.

Minimum Education: Master's Degree in Computer Science, Engineering or Information Systems or related discipline.
Minimum/General Experience:

Eight (8) years or more years managing and performing client engagements in consulting, cybersecurity, IT, systems analysis and solutions architecture, system design and implementation. Experience in security control assessments, penetration testing, risk and vulnerability analysis, incident response, information assurance, system analysis and solution architecture, testing, implementation, program management, or other related services. A relevant advanced degree may be substituted for 1 to 2 years of experience. Each major professional certification (PgMP, PMP, CAP, CISSP, CISA, CEH, CISM, etc.) may also be substituted for 1 year of experience.

SERVICE CONTRACT LABOR STANDARDS (SCLS)

L2 Cyber Solutions understands that the Service Contract Labor Standards (SCLS) is applicable to this contract as it applies to the entire Multiple Award Schedule (MAS) and all services provided. While no specific labor categories have been identified as being subject to SCLS due to exemptions for professional employees (FAR 22.1101, 22.1102 and 29 CFR 541.300), this contract still maintains the provisions and protections for SCLS eligible labor categories. If and/or when SCLS labor categories/employees are added to the contract through the modification process, L2 Cyber Solutions will inform the Contracting Officer and establish a SCLS matrix identifying the GSA labor category titles, the occupational code, SCLS labor category titles and the applicable WD number.