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 (MAS)
FSC Group: 54151S, 54151 HACS and 811212
Contract Number: 47QTCA18D00DC
Contract Period: June 15, 2018 – June 14, 2023

For more information on ordering from Federal Supply Schedules click on the GSA Schedules link at www.gsa.gov

Contractor: United One Communications LLC
808 N Franklin St Ste 3204
Tampa, FL 33602
Phone number: (813) 278-3020
Fax number: (813) 278-3020
www.getuoc.com

Contractor’s Administration Source: Carl C. Chaisson
Business Size: Small Business
Minority Owned Business
SBA Certified 8(a) Program Participant
DOT Certified DBE

Current as of Modification PO-0017 effective February 24, 2022

Prices Shown Herein are Net (discount deducted)
CUSTOMER INFORMATION:

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

<table>
<thead>
<tr>
<th>SIN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services</td>
</tr>
<tr>
<td>811212</td>
<td>Maintenance of Equipment, Repair Services, and/or Repair/Spare Parts</td>
</tr>
<tr>
<td>OLM</td>
<td>Order Level Materials</td>
</tr>
</tbody>
</table>

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


2. MAXIMUM ORDER*: $500,000

*Ordering activities may request a price reduction at any time before placing an order, establishing a BPA, or in conjunction with the annual BPA review. However, the ordering activity shall seek a price reduction when the order or BPA exceeds the simplified acquisition threshold. Schedule contractors are not required to pass on to all schedule users a price reduction extended only to an individual ordering activity for a specific order or BPA.

3. MINIMUM ORDER: $100

4. GEOGRAPHIC COVERAGE: 50 States and Washington D.C.

5. POINT(S) OF PRODUCTION: Not Applicable

6. DISCOUNT FROM LIST PRICES: GSA Net Prices are shown on the attached GSA Pricelist.

7. QUANTITY DISCOUNT(S): Not Applicable

8. PROMPT PAYMENT TERMS: Net 30 Days.

Information for Ordering Offices: Prompt Payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9. FOREIGN ITEMS: Not Applicable

10a. TIME OF DELIVERY: Determined on task order level

10b. EXPEDITED DELIVERY: Contact contractor

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

10d. URGENT REQUIREMENTS: Agencies can contact the Contractor’s representative to affect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.

11. FOB POINT: Destination

12a. ORDERING ADDRESS: 808 N Franklin St Ste 3204 Tampa, FL 33602

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

13. PAYMENT ADDRESS: 808 N Franklin St Ste 3204 Tampa, FL 33602

14. WARRANTY PROVISION: Not Applicable
15. EXPORT PACKING CHARGES: N/A

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

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

18a. TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE): N/A

18b. TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE): N/A

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

20. LIST OF PARTICIPATING DEALERS (IF APPLICABLE): N/A

21. PREVENTIVE MAINTENANCE (IF APPLICABLE): N/A

22a. SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants): N/A

22b. Section 508 Compliance

   Section 508 compliance information on the supplies and services in this contract are available at the following website address (URL): www.unitedonecommunications.com

   The EIT standard can be found at: www.Section508.gov/

23. Unique Entity Identifier (UEI) number: MZ3PA733M1A9

24. Contractor has an active registration in the SAM database.
Information Technology Category Instructions and Regulations

Section III Terms and Conditions for all IT Contractors

NOTE: All non-professional labor categories must be incidental to, and used solely to support professional services, and cannot be purchased separately.

1) Organizational Conflicts Of Interest

   a) Definitions.

      i) Contractor" means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

      ii) "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.

      iii) 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

2) Services Performed

   a) All 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.

   b) The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

   c) The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

3) Travel.

   a) Any contractor travel required in the performance of services must comply with the Pub. L.99-234 and FAR Part 31.205-46, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel.
4) Warranty

a) Unless otherwise specified in this contract, the Contractor's standard commercial warranty as stated in the contract's commercial pricelist will apply to this contract.

b) The Contractor's commercial guarantee/warranty shall be included in the Commercial Supplier Agreement to include Enterprise User License Agreements or Terms of Service (TOS) agreements, if applicable.

c) Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.

Terms and Conditions for SIN 54151HACS Highly Adaptive Cybersecurity Services (HACS)

5. Only IT Professional Highly Adaptive Cybersecurity Services (HACS) shall be offered under this special item number. The following are the approved subcategories:

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

6. Resumes shall be provided to the GSA Contracting Officer or the ordering activity upon request.

7. Services offered SIN 54151HACS shall 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-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
- OMB Memorandum M-19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 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 800-44 - 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 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations.
<table>
<thead>
<tr>
<th>Job Title</th>
<th>Information Assurance Engineer I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Years of Experience</td>
<td>2 years</td>
</tr>
<tr>
<td>Minimum Education Level</td>
<td>Bachelor’s Degree</td>
</tr>
<tr>
<td>Detailed Position Description and Functional Responsibilities</td>
<td>The Information Assurance Engineer I ensures availability, integrity, authentication, confidentiality, and non-repudiation. They incorporate protection, detection, and reaction capabilities to ensure the preservation and restoration of systems; develop and manage IA risk management plans; and certify and accredit systems. They may also provide network intrusion detection and monitoring, HBSS-related monitoring, correlation analysis using security event and incident management (SEIM) analysis tools, and support as required for the fielded CND analysis suite for network subscribers and other supported components. Typical duties include:</td>
</tr>
<tr>
<td></td>
<td>• Work with client to identify overall security requirements for the proper handling of data</td>
</tr>
<tr>
<td></td>
<td>• Assist architects and system developers in the identification and implementation of appropriate information security</td>
</tr>
<tr>
<td></td>
<td>• Enforce the design and implementation of trusted relationships among external systems and architectures</td>
</tr>
<tr>
<td></td>
<td>• Provides interface to certification and accreditation organization</td>
</tr>
<tr>
<td></td>
<td>• Provide guidance to development and operational efforts on IA functions, particularly those focused on strategic planning, infrastructure protection, and defensive strategy</td>
</tr>
<tr>
<td></td>
<td>• Executing, drafting, editing, and maintaining standard operating procedures</td>
</tr>
<tr>
<td></td>
<td>• Provide coordination of significant incidents with clients and supported entities to ensure proper analysis is performed and timely and accurate reporting of the incident is affected</td>
</tr>
<tr>
<td></td>
<td>• Provide, develop, and maintain a network forensic analysis capability to enhance response to, support of, and investigation into significant incidents to provide a clearer view of the exploits, vulnerabilities, and tactics, techniques, and procedures used</td>
</tr>
<tr>
<td></td>
<td>• Provide support for CND analysis, fusion, and monitoring 24x7</td>
</tr>
<tr>
<td></td>
<td>• Coordinate with client incident response, cyber threat analyst, IAVM, HBSS support, and CND infrastructure support staff as necessary</td>
</tr>
<tr>
<td></td>
<td>• Expected to interact with all areas affected by the project including end users, computer services, and client services</td>
</tr>
<tr>
<td>Job Title</td>
<td>Information Assurance Engineer II</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Minimum Years of Experience</td>
<td>5 years</td>
</tr>
<tr>
<td>Minimum Education Level</td>
<td>Bachelor’s Degree</td>
</tr>
</tbody>
</table>
| Detailed Position Description and Functional Responsibilities | The Information Assurance Engineer II ensures availability, integrity, authentication, confidentiality, and non-repudiation. They incorporate protection, detection, and reaction capabilities to ensure the preservation and restoration of systems; develop and manage IA risk management plans; and certify and accredit systems. They may also provide network intrusion detection and monitoring, HBSS-related monitoring, correlation analysis using security event and incident management (SEIM) analysis tools, and support as required for the fielded CND analysis suite for network subscribers and other supported components. Typical duties include:

- Work with client to identify overall security requirements for the proper handling of data
- Assist architects and system developers in the identification and implementation of appropriate information security
- Enforce the design and implementation of trusted relationships among external systems and architectures
- Provides interface to certification and accreditation organization
- Provide guidance to development and operational efforts on IA functions, particularly those focused on strategic planning, infrastructure protection, and defensive strategy
- Executing, drafting, editing, and maintaining standard operating procedures
- Provide coordination of significant incidents with clients and supported entities to ensure proper analysis is performed and timely and accurate reporting of the incident is affected
- Provide, develop, and maintain a network forensic analysis capability to enhance response to, support of, and investigation into significant incidents to provide a clearer view of the exploits, vulnerabilities, and tactics, techniques, and procedures used
- Provide support for CND analysis, fusion, and monitoring 24x7
- Coordinate with client incident response, cyber threat analyst, IAVM, HBSS support, and CND infrastructure support staff as necessary
- Expected to interact with all areas affected by the project including end users, computer services, and client services |
Develops detailed work plans, schedules, estimates, resource plans, and status reports
Conducts project meetings and is responsible for tracking and analysis of progress

Qualifications

- Industry standard certification such as Security+ CE, CASP, CISSP, CISA, GSEC, MCSA, MCSE, etc.
- Public Key Infrastructure
- Cyber security best practices
- INFOSEC and IA industry policies/standards
- Risk Management Framework
- Certification and Accreditation
- Vulnerability Analyses
- Knowledge of DoD 8570 IAT standards
- Experience conducting analysis at the packet level
- Experience reading and analyzing firewall logs
- Experience administering UNIX-based systems
- Experience with Snort, McAfee, eTrust, and Cisco intrusion detection sensors
- Experience with vulnerability assessment tools (e.g. Retina, Nessus, FoundScan, ArcSight, etc.)

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Information Assurance Engineer III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Years of Experience</td>
<td>7 years</td>
</tr>
<tr>
<td>Minimum Education Level</td>
<td>Master’s Degree</td>
</tr>
</tbody>
</table>
| Detailed Position Description and Functional Responsibilities | The Information Assurance Engineer III ensures availability, integrity, authentication, confidentiality, and non-repudiation. They incorporate protection, detection, and reaction capabilities to ensure the preservation and restoration of systems; develop and manage IA risk management plans; and certify and accredit systems. They may also provide network intrusion detection and monitoring, HBSS-related monitoring, correlation analysis using security event and incident management (SEIM) analysis tools, and support as required for the fielded CND analysis suite for network subscribers and other supported components. Typical duties include:

- Work with client to identify overall security requirements for the proper handling of data
- Assist architects and system developers in the identification and implementation of appropriate information security
- Enforce the design and implementation of trusted relationships among external systems and architectures
- Provides interface to certification and accreditation organization
- Provide guidance to development and operational efforts on IA functions, particularly those focused on strategic planning, infrastructure protection, and defensive strategy
- Executing, drafting, editing, and maintaining standard operating procedures
- Provide coordination of significant incidents with clients and supported entities to ensure proper analysis is performed and timely and accurate reporting of the incident is affected
- Provide, develop, and maintain a network forensic analysis capability to enhance response to, support of, and investigation into significant incidents to provide a clearer view of the exploits, vulnerabilities, and tactics, techniques, and procedures used
- Provide support for CND analysis, fusion, and monitoring 24x7
- Coordinate with client incident response, cyber threat analyst, IAVM, HBSS support, and CND infrastructure support staff as necessary
- Expected to interact with all areas affected by the project including end users, computer services, and client services
<table>
<thead>
<tr>
<th>Job Title</th>
<th>Cybersecurity Specialist I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Years of Experience</td>
<td>2 years</td>
</tr>
<tr>
<td>Minimum Education Level</td>
<td>Bachelor’s Degree</td>
</tr>
<tr>
<td>Detailed Position Description and Functional Responsibilities</td>
<td>Specialized in providing the full range of security/cybersecurity incident data collection and correlation, engineering, analysis, testing, and/or support. The scope of responsibility relates to one or more of the following IT areas: information/data, computer hardware or software, networks, mobile computing, cloud, and/or applications. Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Qualifications</th>
<th>Industry standard certification such as Security+ CE, CASP, CISSP, CISA, GSEC, MCSA, MCSE, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Cyber security best practices</td>
</tr>
<tr>
<td></td>
<td>INFOSEC and IA industry policies/standards</td>
</tr>
<tr>
<td></td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td></td>
<td>Certification and Accreditation</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Analyses</td>
</tr>
<tr>
<td></td>
<td>Knowledge of DoD 8570 IAT standards</td>
</tr>
<tr>
<td></td>
<td>Experience conducting analysis at the packet level</td>
</tr>
<tr>
<td></td>
<td>Experience reading and analyzing firewall logs</td>
</tr>
<tr>
<td></td>
<td>Experience administering UNIX-based systems</td>
</tr>
<tr>
<td></td>
<td>Experience with Snort, McAfee, eTrust, and Cisco intrusion detection sensors</td>
</tr>
<tr>
<td></td>
<td>Experience with vulnerability assessment tools (e.g. Retina, Nessus, FoundScan, ArcSight, etc.)</td>
</tr>
<tr>
<td>Job Title</td>
<td>Cybersecurity Specialist I</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Minimum Years of Experience</td>
<td>5 years</td>
</tr>
<tr>
<td>Minimum Education Level</td>
<td>Bachelor’s Degree</td>
</tr>
</tbody>
</table>

**Detailed Position Description and Functional Responsibilities**

Specialized in providing the full range of security/cybersecurity incident data collection and correlation, engineering, analysis, testing, and/or support. The scope of responsibility relates to one or more of the following IT areas: information/data, computer hardware or software, networks, mobile computing, cloud, and/or applications. Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediation.

**Qualifications**

- Industry standard certification such as Security+ CE, CASP, CISSP, CISA, GSEC, MCSA, MCSE, etc.
- Public Key Infrastructure
- Cyber security best practices
- INFOSEC and IA industry policies/standards
- Risk Management Framework
- Certification and Accreditation
- Vulnerability Analyses
- Knowledge of DoD 8570 IAT standards
- Experience conducting analysis at the packet level
- Experience reading and analyzing firewall logs
- Experience administering UNIX-based systems
- Experience with Snort, McAfee, eTrust, and Cisco intrusion detection sensors
- Experience with vulnerability assessment tools (e.g. Retina, Nessus, FoundScan, ArcSight, etc.)

**SIN(s)**

<table>
<thead>
<tr>
<th>SIN(s)</th>
<th>Labor Categories</th>
<th>Unit of Issue</th>
<th>GSA Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Information Assurance Engineer I</td>
<td>Hour</td>
<td>$111.10</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Assurance Engineer II</td>
<td>Hour</td>
<td>$123.67</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Assurance Engineer III</td>
<td>Hour</td>
<td>$143.35</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Specialist I</td>
<td>Hour</td>
<td>$60.18</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Specialist II</td>
<td>Hour</td>
<td>$69.67</td>
</tr>
</tbody>
</table>