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)

CONTRACT NUMBER: 47QTCA21D00EK

CONTRACT PERIOD: Sept 7, 2021 – Sept 6, 2031

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

CONTRACTOR: Oneida Technical Solutions, LLC (OTS)
2037 Dream Catcher Plaza
Oneida, New York 13421
Phone number: (315) 534-1086
Fax number: (315) 361-8621
E-Mail: joseph.cavano@onenterprises.com
Website: oneidatechnicalsolutions.com

CONTRACTOR’S ADMINISTRATION SOURCE: Joseph Cavano, Director of Business Affairs
2037 Dream Catcher Plaza
Oneida, New York 13421
Phone number: (315) 534-1086
Fax number: (315) 361-8621
E-Mail: joseph.cavano@onenterprises.com

BUSINESS SIZE: 8(a) Small Disadvantaged, Tribally-Owned

CUSTOMER INFORMATION:

1a. TABLE OF AWARDED MAS CATEGORIES/ SIN(s)

<table>
<thead>
<tr>
<th>SIN(s)</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES</td>
</tr>
<tr>
<td>54151HACS</td>
<td>HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)</td>
</tr>
</tbody>
</table>

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN:
(Government net price based on a unit of one, hourly rate)

54151S- Technical Writer $65.26

54151HACS- Cybersecurity Technician/Analyst $65.11
c. **HOURLY RATES (Services only):**

SIN(s) 54151S and 54151HACS

<table>
<thead>
<tr>
<th>Proposed Labor Category</th>
<th>APPROVED GSA PRICING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>54151S IT Professional Services</strong></td>
<td></td>
</tr>
<tr>
<td>IT Subject Matter Specialist</td>
<td>$143.60</td>
</tr>
<tr>
<td>Systems Engineer, Senior</td>
<td>$142.30</td>
</tr>
<tr>
<td>Project Manager, Senior</td>
<td>$129.46</td>
</tr>
<tr>
<td>Technician/Analyst</td>
<td>$70.33</td>
</tr>
<tr>
<td>Technical Writer</td>
<td>$65.26</td>
</tr>
<tr>
<td><strong>54151HACS HACS SIN</strong></td>
<td></td>
</tr>
<tr>
<td>IT Subject Matter Specialist, Cybersecurity</td>
<td>$140.71</td>
</tr>
<tr>
<td>Cybersecurity Engineer</td>
<td>$99.10</td>
</tr>
<tr>
<td>Cybersecurity Project Manager, Senior</td>
<td>$127.30</td>
</tr>
<tr>
<td>Cybersecurity Technician/Analyst</td>
<td>$65.11</td>
</tr>
<tr>
<td>Cybersecurity Documentation Specialist</td>
<td>$77.32</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**: Domestic and Overseas

5. **POINT(S) OF PRODUCTION**: N/A

6. **DISCOUNT FROM LIST PRICES**: GSA Net Prices are shown on the attached GSA Pricelist. Negotiated discount has been applied and the IFF has been added.

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

8. **PROMPT PAYMENT TERMS**: 0% Net 30

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**: 30 days ARO

11b. **EXPEDITED DELIVERY**: 30 days or less as discussed with the ordering activity

11c. **OVERNIGHT AND 2-DAY DELIVERY**: N/A
11d. **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.

12. **FOB POINT:** Destination

13a. **ORDERING ADDRESS:** 2037 Dream Catcher Plaza, Oneida, New York 13421

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).

14. **PAYMENT ADDRESS:** 2037 Dream Catcher Plaza, Oneida, New York 13421; ACH/EFT available, contact contractor for details.

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 required in performance of work at the Task Order level.

25. **DUNS NUMBER:** 079381098

26. **NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE:** Contractor has an Active Registration in the SAM database.
SIN 54151S – Capabilities

Oneida Technical Solutions (OTS) provides, but not limited to, the following IT Professional Services: IT infrastructure services, IT modernization project execution and technology upgrades, network engineering, IT and desktop management, data center operations, cloud migration, application programming, and data warehouse architecture and database support.

Please visit our website at https://www.oneidatechnicalsolutions.com/what-we-do for a more complete description of our services, capabilities and past performance information.

SIN 54151S Labor Category Descriptions

1. **IT Subject Matter Specialist**

   **Minimum/General Experience:** At least twelve years of related hands-on experience with specific Statement of Work or Performance Work Statement requirements.

   **Functional Responsibility:** Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that necessitate high-level knowledge of the subject matter for effective implementation. Participates as needed in all phases of IT infrastructure design or software development with emphasis on the planning, analysis, modeling, simulation, testing, integration, documentation and presentation phases.

   **Minimum Education:** A Bachelor’s degree in a relevant field of study

2. **Systems Engineer, Senior**

   **Minimum/General Experience:** At least ten years of related hands-on experience with specific Statement of Work or Performance Work Statement requirements.

   **Functional Responsibility:** Under general direction, manages the purchase, installation, and support of network communications, including LAN/WAN systems. Responsible for evaluating current systems. Works on complex problems where analysis of situation requires in-depth evaluation of various factors. Plans large-scale systems projects through vendor comparison and cost studies. Provides work leadership and training to lower level network engineers. Requires expert knowledge of LAN/WAN systems, networks, and applications.

   **Minimum Education:** A Bachelor’s degree in a relevant field of study

3. **Project Manager, Senior**

   **Minimum/General Experience:** At least ten years of related hands-on experience with specific Statement of Work or Performance Work Statement requirements.

   **Functional Responsibility:** Planning, directing, and managing complex IT projects and operations, such as software development using agile, waterfall or hybrid project management methodology; IT network upgrades and technology refreshes to include comprehensive planning of organization and end-user impacts to minimize downtime; IT hardware rollouts and complex projects integrating multiple disparate systems together with Commercial Off the Shelf (COTS) or Government Off the Shelf (GOTS) products; technical and management leadership of task compliance with industry accepted Government and civilian and user standards. Knowledge of configuration management and quality assurance concepts and guidelines for example, AGILE, Information Technology Infrastructure Library (ITIL), Institute of Electrical, and Electronic Engineers (IEEE), and Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI), Project Management Body of Knowledge (PMBOK). Project Management Professional (PMP) certification
required and/or commensurate work experience and education in managing large-scale IT projects.

**Minimum Education:** A Bachelor's degree in a relevant field of study

4. **Technician/Analyst**

**Minimum/General Experience:** At least four years of related hands-on experience with specific Statement of Work or Performance Work Statement requirements.

**Functional Responsibility:** Installs, tests and analyzes all elements of complex computer and network facilities (including power, software, communications devices, lines, modems, and terminals). Monitors and controls the performance and status of the network resources. Utilizes software and hardware tools and identifies and diagnoses complex problems and factors affecting network performance. Provides maintenance and break/fix repair of routers/switches or computer hardware and end user devices, such as computers, laptops, mobile devices, multi-function devices.

**Minimum Education:** An Associate's degree in a relevant field of study

5. **Technical Writer**

**Minimum/General Experience:** At least four years of related hands-on experience with specific Statement of Work or Performance Work Statement requirements.

**Functional Responsibility:** Researches, outlines and writes technical end-user documentation including user manuals, technical documents, online Help and infrastructure documentation for information technology computer systems, help desk procedures for troubleshooting and resolving customer requests for support, software programs and/or processes. Collects and organizes information required for preparation of user manuals, training materials, installation guides, proposals, and other deliverables. Drafts policy documents pertaining to information technology management, software/technical user manuals and standard operating procedures for a variety of information technology professional services.

**Minimum Education:** An Associate's degree in a relevant field of study

**Alternate Degree Experience Equivalency for 54151S Labor Categories:**

A higher degree than the minimum education required will substitute as credit for the corresponding years of experience as noted below:

<table>
<thead>
<tr>
<th>Degree</th>
<th>Experience Equivalence if higher degree than minimum education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate’s</td>
<td>N/A</td>
</tr>
<tr>
<td>Bachelor’s</td>
<td>2 years</td>
</tr>
<tr>
<td>Master’s</td>
<td>2 years</td>
</tr>
<tr>
<td>Doctorate</td>
<td>2 years</td>
</tr>
</tbody>
</table>
SIN 54151HACS – Capabilities

OTS is expert at providing HACS-related services, and currently supports highly complex, secure and regulated environments such as the Department of Defense.

The scope of the HACS SIN includes proactive and reactive cybersecurity services. Assessment services needed for systems categorized as High Value Assets (HVA) are also within scope of this SIN. It includes Risk and Vulnerability Assessments (RVA), Security Architecture Review (SAR), and Systems Security Engineering (SSE). Additionally, the scope of the SIN includes services for the seven step Risk Management Framework (RMF), and Security Operations Center (SOC) services.

- The seven-step RMF includes preparation, information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCMA) which evaluate organization-wide ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization’s incident management functions.
- SOC services are services such as: 24x7x365 monitoring and analysis, traffic analysis, incident response and coordination, penetration testing, anti-virus management, intrusion detection and prevention, and information sharing.

There are five subcategories under the HACS SIN. Vendors listed within each subcategory in GSA eLibrary have passed a technical evaluation for that specific subcategory:

- **High Value Asset Assessments** – include Risk and Vulnerability Assessment (RVA) 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. See the section below on RVA for details on those services. Security Architecture Review (SAR) 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. Systems Security Engineering (SSE) 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.

- **Risk and Vulnerability Assessment** – 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.

- **Cyber Hunt** – 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.

- **Incident Response** – 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.

- **Penetration Testing** – is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.
SIN 54151HACS – Labor Category Descriptions

1. **IT Subject Matter Specialist, Cybersecurity**

   **Minimum/General Experience:** At least twelve years of related hands-on experience with specific Statement of Work or Performance Work Statement requirements.

   **Functional Responsibility:** Provides extremely high-level subject matter proficiency for work described in the task. Provides advanced technical knowledge and analysis of highly specialized applications and operational environment, high-level functional systems analysis, design, integration, documentation, training, and implementation advice on complex problems that require doctorate level knowledge of the subject matter for effective implementation. Deep expertise in relevant subject matter specific to cybersecurity; used for niche projects or analysis that require focused expertise in a particular security domain or response. Specializes in information security protocols and practices in accordance with NIST and the DoD Risk Management Framework.

   **Minimum Education:** A Bachelor’s degree in a relevant field of study

2. **Cybersecurity Engineer**

   **Minimum/General Experience:** At least five years of related hands-on experience with specific Statement of Work or Performance Work Statement requirements.

   **Functional Responsibility:** Under general direction, manages the purchase, installation, and support of network communications and/or information security systems. Responsible for evaluating current systems. Works on complex problems where analysis of situation requires in-depth evaluation of various factors. Plans large-scale systems projects through vendor comparison and cost studies. Provides work leadership and training to lower level engineers or technicians. Requires expert knowledge of systems, networks, and applications. Establishes and satisfies complex system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands.

   **Minimum Education:** A Bachelor’s degree in a relevant field of study

3. **Cybersecurity Project Manager, Senior**

   **Minimum/General Experience:** At least ten years of related hands-on experience with specific Statement of Work or Performance Work Statement requirements.

   **Functional Responsibility:** Planning, directing, and managing complex IT projects and operations; Technical and management leadership of task compliance with industry accepted Government and civilian and user standards. Knowledge of configuration management and quality assurance concepts and guidelines for example, AGILE, Information Technology Infrastructure Library (ITIL), Institute of Electrical, and Electronic Engineers (IEEE), and Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI), Project Management Body of Knowledge (PMBOK).

   **Minimum Education:** A Bachelor’s degree in a relevant field of study

4. **Cybersecurity Technician/Analyst**

   **Minimum/General Experience:** At least two years of related hands-on experience with specific Statement of
Work or Performance Work Statement requirements.

**Functional Responsibility:** Installs, tests and analyzes all elements of complex computer and network facilities (including power, software, communications devices, lines, modems, and terminals). Monitors and controls the performance and status of the network resources. Utilizes software and hardware tools and identifies and diagnoses complex problems and factors affecting network performance. Provides maintenance and break/fix repair of routers/switches or computer hardware and end user devices, such as computers, laptops, mobile devices, multi-function devices.

**Minimum Education:** A Bachelor’s degree in a relevant field of study

5. **Cybersecurity Documentation Specialist**

**Minimum/General Experience:** At least two years of related hands-on experience with specific Statement of Work or Performance Work Statement requirements.

**Functional Responsibility:** Researches, outlines and writes technical end-user documentation including user manuals, technical documents, online Help and infrastructure documentation for information technology computer systems, help desk procedures for troubleshooting and resolving customer requests for support, software programs and/or processes. Collects and organizes information required for preparation of user manuals, training materials, installation guides, proposals, and other deliverables. Documents artifacts for cybersecurity compliance in accordance with Risk Management Framework; drafts policy documents pertaining to information security and standard operating procedures. Generates technical documentation related to findings and remediation in accordance with DISA STIG. Prepares artifacts for use in eMass or other similar tool.

**Minimum Education:** A Bachelor’s degree in a relevant field of study

**Alternate Degree Experience Equivalency for 54151HACS Labor Categories:**

A higher degree than the minimum education required will substitute as credit for the corresponding years of experience as noted below:

<table>
<thead>
<tr>
<th>Degree</th>
<th>Experience Equivalence if higher degree than minimum education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate’s</td>
<td>N/A</td>
</tr>
<tr>
<td>Bachelor’s</td>
<td>2 years</td>
</tr>
<tr>
<td>Master’s</td>
<td>2 years</td>
</tr>
<tr>
<td>Doctorate</td>
<td>2 years</td>
</tr>
</tbody>
</table>