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 for GSA Advantage!® is: GSAAdvantage.gov.

DSB Management Consultants, LLC

HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)
SPECIAL ITEM NUMBER (SIN) 54151HACS

Solicitation Number: 47QSMD20R0001
Refresh Number: 0004

Final SF30 Multiple Award Schedule (MAS) Consolidation
<Contract 47QTCA19D00JM> (A812)
04/13/2020

Contract Period: **August 23, 2019 – August 22, 2024**

DSB Management Consultants, LLC
7402 Valleycrest Boulevard
Annandale, VA 22003
Phone: 703-698-0150
Mobile: 571-221-7840
www.dsbmgt.com

Contract Administrators:
Donna S. Brown, President & CEO, 703-698-0150, dbrown@dsbmgt.com
William A. Brown, Cybersecurity Senior Manager, 703-867-6745, wbrown@dsbmgt.com
1a. Awarded SINs:

<table>
<thead>
<tr>
<th>Special Item Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS Highly Adaptive Cybersecurity Services (HACS)</td>
<td>SUBJECT TO COOPERATIVE PURCHASING - includes proactive and reactive cybersecurity services that improve the customer’s enterprise-level security posture. The scope of this category encompasses a wide range of fields that include, but are not limited to, Risk Management Framework (RMF) services, information assurance (IA), virus detection, network management, situational awareness and incident response, secure web hosting, and backup and security 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. The scope of this category also includes Security Operations Center (SOC) services. The SOC scope includes 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. HACS vendors are able to identify and protect a customer’s information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge.</td>
</tr>
</tbody>
</table>

1b. See the Labor Category Descriptions section for descriptions of all corresponding job titles, experience, functional responsibility and education for the services offered.

2. Maximum order - The maximum order value for this contract is $500,000

3. Minimum order - The minimum order to be issued is $100.00.

4. Geographic coverage: Worldwide

5. Points of Production: DSB Management Consultants, LLC Offices and Government Furnished Offices and Equipment

6. Basic Discount Terms SIN 54151HACS: 8% for GSA, USA Government

7. Quantity/Volume Discount: 1% for orders over $100,00- $249,999

8. Prompt Payment terms: 2%, Net 10 days; Net 30 days.

9a. Government purchase cards are accepted for payments equal to or less than the micro purchase threshold.
9b. Government purchase cards are not accepted for payment above the micro-purchase threshold.

10. Foreign items are not available on this contract.

11a. Time of delivery: DSB Management Consultants, LLC will deliver services as negotiated between DSB and the Ordering Agency.

11b. URGENT REQUIREMENTS: When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering agency, agencies are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within three workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering agency, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

12. FOB Point: Destination

13a. Ordering address: DSB Management Consultants, LLC
7402 Valleycrest Boulevard
Annandale, VA 22003

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: DSB Management Consultants, LLC
7402 Valleycrest Boulevard
Annandale, VA 22003

15. Warranty Provision – N/A

16. Export packing charges – N/A

17. DSB accepts the Government Purchase Card for purchases equal to or less than the micro-purchase threshold.

18. Terms and conditions of rental, maintenance, and repair: N/A

19. Terms and conditions of installation: N/A

20. Terms and conditions of repair parts: N/A

21. List of service and distribution points: N/A

22. List of participating dealers: N/A

23. Preventive maintenance: N/A

24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants): N/A

24b. If applicable, Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services. The EIT standards can be found at: www.Section508.gov/.
25. Data Universal Number System (DUNS) number: 00-347-7485


TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (SPECIAL ITEM NUMBERS 54151HACS)

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SIN must 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 800-160 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

● NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

1. SCOPE
   a. The labor categories, prices, terms and conditions stated under Special Item Number 54151HACS Highly Adaptive Cybersecurity Services (HACS) apply exclusively to Highly Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.

b. Services under this SIN are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on MAS Schedule SIN 54151HACS and may be quoted along with services to provide a total solution.

c. This SIN provides ordering activities with access to Highly Adaptive Cybersecurity services only.

d. Highly Adaptive Cybersecurity Services provided under this SIN shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

e. SCOPE:

54151HACS Highly Adaptive Cybersecurity Services (HACS) - SUBJECT TO COOPERATIVE PURCHASING - includes proactive and reactive cybersecurity services that improve the customer’s enterprise-level security posture.

● High Value Asset (HVA) Assessments includes the following:

   1. **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. 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.

   2. **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.

   3. **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.

● 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.

f. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.
2. ORDER
a. Agencies may use written orders, Electronic Data Interchange (EDI) orders, Blanket Purchase Agreements (BPAs), individual purchase orders, or task orders for ordering services under this contract. BPAs shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

3. PERFORMANCE OF SERVICES
a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.
b. The Contractor agrees to render services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor’s travel.

4. INSPECTION OF SERVICES
Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS (Jan 2017) & (ALTERNATE I-Jan 2017) for Time-and-Materials and Labor-Hour orders placed under this contract.

5. RESPONSIBILITIES OF THE CONTRACTOR
The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (May 2014) Rights in Data – General, may apply.

The Contractor shall comply with contract clause (52.204-21) to the Federal Acquisition Regulation (FAR) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY
Subject to the ordering activity security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.

7. INDEPENDENT CONTRACTOR
All Highly Adaptive Cybersecurity 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.
8. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

“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.

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.

9. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for Highly Adaptive Cybersecurity Services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

10. RESUMES

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

11. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Number 54151HACS for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.
## Labor Categories

**SIN 54151HACS Highly Adaptive Cybersecurity Services (HACS)**

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>Minimum/General Experience and Years of Experience</th>
<th>Functionality Responsibility (Summary)</th>
<th>Educational Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS Cybersecurity Senior Manager</td>
<td>Ten or more years of experience</td>
<td>A Cybersecurity Senior Manager (CSM) is an experienced leader of cybersecurity engagement work-streams that designs and implements solutions. A CSM leads a team of IT cybersecurity professionals. A CSM conducts engagement planning, supervises staff, reviews and completes work products. A CSM determines objectives, and executes engagements. A CSM assesses the effectiveness of IT security controls for design, implementation, and operating effectiveness. A CSM assesses IT systems strengths, vulnerabilities, risks, and threats; makes recommendations for improvement of those IT systems, operations, policies, and procedures for our clients.</td>
<td>Master’s degree in a related management and technical field and appropriate certification (CompTIA, ISACA, ISC2, SANS, etc.).</td>
</tr>
<tr>
<td>54151HACS Cybersecurity Manager</td>
<td>Seven to nine years of experience</td>
<td>A Cybersecurity Manager (CM) is an emerging leader of cybersecurity engagement work-streams that designs and implements solutions. A CM leads a team of IT cybersecurity professionals. A CM conducts engagement planning, supervises staff, reviews and completes work products. A CM confirms objectives, and executes engagements. A CM assesses the effectiveness of IT security controls for design, implementation, and operating effectiveness; develops recommendations for improvement of those IT systems, operations, policies, and procedures for our CSMs.</td>
<td>Master’s degree in a related management and technical field or appropriate certification (CompTIA, ISACA, ISC2, SANS, etc.)</td>
</tr>
<tr>
<td>54151HACS Cybersecurity Senior Associate III</td>
<td>Five to seven years of experience</td>
<td>A Cybersecurity Senior Associate III (CSA-III) demonstrates advanced knowledge and experience in IT program management, development operations, and security management, or related technology advisory engagements. A CSA-III leads and supports tasks, including deliverable development, on IT engagements related, but not limited to: vulnerability and risk assessment, IT audit, technology strategy; IT security architecture and services management; data analytics and visualization; infrastructure/network design and management; and cloud computing services. A CSA-III is highly proficient in the use of management and technology tools and supports the overall objectives and goals of the engagement. Demonstrates proficiency by performing engagement tasks; producing engagement deliverables and status reports; verifying and validating work plan completeness; setting an efficient and effective example for junior team members.</td>
<td>Bachelor’s degree in a related management and technical field and appropriate certification (CompTIA, ISACA, ISC2, SANS, etc.)</td>
</tr>
<tr>
<td>Labor Category</td>
<td>Minimum/General Experience and Years of Experience</td>
<td>Functionality Responsibility (Summary)</td>
<td>Educational Responsibility</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>54151 HACS Cybersecurity Senior Associate II</td>
<td>Four to Five years of experience</td>
<td>A Cybersecurity Senior Associate II (CSA-II) demonstrates requisite knowledge and experience in IT program management, development operations, and security management, or related technology advisory engagements. A CSA-II assists with leading and supporting tasks, including deliverable development, on IT engagements related, but not limited to: vulnerability and risk assessment, IT audit, technology strategy; IT security architecture and services management; data analytics and visualization; infrastructure/network design and management; and cloud computing services. A CSA-II is proficient in the use of management and technology tools and assist with supporting the overall objectives and goals of the engagement. Demonstrates proficiency by performing engagement tasks, producing assigned portions of engagement deliverables, and verifying and validating task assignment accuracy and completeness.</td>
<td>Bachelor’s degree in a related management and technical field and appropriate certification (CompTIA, ISACA, ISC2, SANS, etc.)</td>
</tr>
<tr>
<td>54151 HACS Cybersecurity Senior Associate I</td>
<td>Three to Four years of experience</td>
<td>A Cybersecurity Senior Associate I (CSA-I) demonstrates emerging knowledge and experience in IT program management, development operations, and security management, or related technology advisory engagements. A CSA-I performs supporting tasks, prepares deliverables on IT engagements related, but not limited to: vulnerability and risk assessment, IT audit, technology strategy; IT security architecture and services management; data analytics and visualization; infrastructure/network design and management; and cloud computing services. A CSA-I is progressing in the use of management and technology tools and supports their assigned objectives and tasks on the engagement. Demonstrates progressive development by performing assigned tasks; producing assigned deliverables; seeking and addressing feedback and review comments; seeking verification and validation of assignment completeness.</td>
<td>Bachelor’s degree in a related management and technical field or appropriate certification (CompTIA, ISACA, ISC2, SANS, etc.)</td>
</tr>
<tr>
<td>54151 HACS Cybersecurity Associate II</td>
<td>Two to three years of experience</td>
<td>A Cybersecurity Associate II (CA-II) has prior experience working on a Cybersecurity engagement. A CA-II is expected to perform a greater portion of the duties during a cybersecurity engagement, a vulnerability assessment, and/or an IT audit. A CA-II has IT and management skills, and will assist in the installation, configuration, and operation of cybersecurity tools. Possesses auditing and assessment skills and perform controls testing or conducts interviews with security control stakeholders. A CA-II prepares deliverables, which are reviewed by a Senior, Manager, and/or Senior Manager. A CA-II works and takes on greater responsibility under the guidance of a Manager or Senior, as part of a cybersecurity engagement team.</td>
<td>Associate’s degree in a related management and technical field and appropriate certification (CompTIA, ISACA, ISC2, SANS, etc.)</td>
</tr>
<tr>
<td>Labor Category</td>
<td>Minimum/General Experience and Years of Experience</td>
<td>Functionality Responsibility (Summary)</td>
<td>Educational Responsibility</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>54151HACS Cybersecurity Associate I</td>
<td>One to two years of experience</td>
<td>A Cybersecurity Associate I (CA-I) may have prior experience working on a Cybersecurity engagement. A CA-I is expected to perform a portion of the duties during a cybersecurity engagement, a vulnerability assessment, and/or an IT audit. A CA-I will typically have IT and management skills, and may assist in the installation, configuration, and operation of cybersecurity tools. May have auditing and assessment skills and perform some controls testing or participate in interviews with security control stakeholders. A CA-I prepares deliverables, which are reviewed by a Senior, Manager, and/or Senior Manager. A CA-I works under the guidance of a Manager or Senior, as part of a cybersecurity engagement team.</td>
<td>Associate’s degree in a related management and technical field or appropriate certification (CompTIA, ISACA, ISC2, SANS, etc.)</td>
</tr>
</tbody>
</table>

**Education and Experience Equivalency Policy**

DSB Management Consultants LLC reserves the right to make the following substitutions in the education and/or experience requirements for any labor category:

1. One year of experience is the equivalent of one year of education.
2. One year of education is the equivalent of one year of experience.
3. Certification related to the technology is equivalent to two years of the experience or education requirement.
## GSA Rates Excluding and Including the IFF for the Contract Base Period of 8/23/2019-8/22/2024

<table>
<thead>
<tr>
<th>#</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>UNIT OF ISSUE (e.g. Hour, Task, Sq ft)</th>
<th>PRICE OFFERED TO GSA (excluding IFF)</th>
<th>PRICE OFFERED TO GSA (including IFF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>54151HACS Cybersecurity Senior Manager</td>
<td>Hour</td>
<td>$197.80</td>
<td>$199.28</td>
</tr>
<tr>
<td>2</td>
<td>54151HACS Cybersecurity Manager</td>
<td>Hour</td>
<td>$179.86</td>
<td>$181.21</td>
</tr>
<tr>
<td>3</td>
<td>54151HACS Cybersecurity Senior Associate III</td>
<td>Hour</td>
<td>$144.90</td>
<td>$145.99</td>
</tr>
<tr>
<td>4</td>
<td>54151HACS Cybersecurity Senior Associate II</td>
<td>Hour</td>
<td>$133.40</td>
<td>$134.40</td>
</tr>
<tr>
<td>5</td>
<td>54151HACS Cybersecurity Senior Associate I</td>
<td>Hour</td>
<td>$120.06</td>
<td>$120.96</td>
</tr>
<tr>
<td>6</td>
<td>54151HACS Cybersecurity Associate II</td>
<td>Hour</td>
<td>$105.80</td>
<td>$106.59</td>
</tr>
<tr>
<td>7</td>
<td>54151HACS Cybersecurity Associate I</td>
<td>Hour</td>
<td>$ 87.86</td>
<td>$ 88.52</td>
</tr>
</tbody>
</table>