AUSGAR Technologies, Inc.
10721 Treena Street
San Diego, CA 92131
(P) 855-428-7427 (F) 855-893-5489
www.ausgar.com

Contract Number: 47QTC20D002Q
Period Covered by Contract: November 26, 2019 to November 25, 2024

Business Size: Small Business

General Services Administration
Federal Acquisition Service

Pricelist current through PO-0001, dated November 26, 2019.

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

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov.
CUSTOMER INFORMATION:

1. **Awarded Special Item Number(s):**
   
<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>Professional Information Technology Services</td>
</tr>
</tbody>
</table>

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract: See page 12.

1c. Descriptions of all corresponding commercial job titles with experience, functional responsibility and education are provided beginning on page 13.

2. **Maximum Order:** $500,000

3. **Minimum Order:** $100

4. **Geographic Coverage:** Domestic only

5. **Point of Production:** N/A

6. **Prices Shown Herein are Net** (discount deducted)

7. **Quantity Discount:** None

8. **Prompt Payment Terms:** Net 30. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions

9. **a. Notification that Government purchase cards are accepted at or below the micro-purchase threshold:** Will be accepted at or below the micro-purchase threshold.
   
   **b. Notification whether Government purchase cards are accepted or not accepted above the micro-purchase threshold:** Will be accepted above the micro-purchase threshold.

10. **Foreign Items:** None

11. **Time of Delivery:** AUSGAR Technologies, Inc. shall deliver or perform services in accordance with the terms negotiated in an agency’s order.

11b. **Expedited Delivery:** Consult with Contractor

11c. **Overnight/2-Day Delivery:** Consult with Contractor

11d. **Urgent Requirements:** Consult with Contractor

12. **FOB Point:** Destination
13. **a. Ordering Address:** Contracts Department  
    ATTN: GSA Administrator  
    10721 Treena Street  
    San Diego, CA 92131  

   **b. Ordering Procedures** For supplies and services, the ordering procedures, information on  
   Blanket Purchase Agreements (BPA’s) are found in Federal Acquisition Regulation (FAR) 8.405-3.

14. **Payment Address:** Accounting Department  
    ATTN: Accounts Receivable  
    10721 Treena Street  
    San Diego, CA 92131

15. **Warranty Provisions:** Contractor’s Standard Warranty

16. **Export Packing charges:** Not applicable

17. **Terms and conditions of Government Purchase Card Acceptance:** Contact AUSGAR Technologies, Inc. for terms and conditions of Government Purchase Card acceptance.

18. **Terms and conditions of rental, maintenance, and repair:** Not applicable

19. **Terms and conditions of installation:** Not applicable

20. **Terms and conditions of repair parts:** Not applicable

20a. **Terms and conditions for any other services:** Not applicable

21. **List of service and distribution points:** Not applicable

22. **List of participating dealers:** Not applicable

23. **Preventive maintenance:** Not applicable

24a. **Environmental attributes**, e.g., recycled content, energy efficiency, and/or reduced pollutants:  
    Not applicable

24b. **AUSGAR Technologies, Inc.** for Section 508 compliance information. The EIT standards can be  
    found at: http://www.section508.gov

25. **DUNS Number:** 141809082

26. **AUSGAR Technologies, Inc.** is registered in the System for Award Management (SAM) database.
Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs 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-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memorandum M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- OMB Memorandum M-16-03 - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- OMB Memorandum M-16-04 – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- 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)
1. **SCOPE**
   a. The labor categories, prices, terms and conditions stated under Special Item Numbers 54151HACS High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Multiple Award Schedule.
   b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on Multiple Award Schedule (e.g. 511210 and 33411), and may be quoted along with services to provide a total solution.
   c. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.
   d. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.
   e. 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, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements 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**

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’s 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.

   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's 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.
1. SCOPE
   a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Services within the scope of this Multiple Award Schedule.
   b. 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. PERFORMANCE INCENTIVES
   a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract in accordance with this clause.
   b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
   c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity’s mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDER
   a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements 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.

4. PERFORMANCE OF SERVICES
   a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
   b. The Contractor agrees to render services only 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 IT 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.

5. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

   (1) Cancel the stop-work order; or

   (2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

   (1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

   (2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6. INSPECTION OF SERVICES

The Inspection of Services–Fixed Price (AUG 1996) (Deviation – May 2003) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection–Time-and-Materials and Labor-Hour (JAN 1986) (Deviation – May 2003) clause at FAR 52.246-6 applies to time-and-materials and labor-hour orders placed under this contract.
7. 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 (Deviation – May 2003) Rights in Data – General, may apply.

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

9. INDEPENDENT CONTRACTOR
All IT 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.

10. 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.

11. INVOICES
The Contractor, upon completion of the work ordered, shall submit invoices for IT 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.
12. PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIAION I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIAION I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

(b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—

   (1) The offeror;
   
   (2) Subcontractors; and/or
   
   (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES

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

14. INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.
<table>
<thead>
<tr>
<th>Labor Category</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Analyst/Engineer I</td>
<td>$69.64</td>
<td>$71.38</td>
<td>$73.17</td>
<td>$74.99</td>
<td>$76.87</td>
</tr>
<tr>
<td>IT Analyst/Engineer II</td>
<td>$87.37</td>
<td>$89.56</td>
<td>$91.79</td>
<td>$94.09</td>
<td>$96.44</td>
</tr>
<tr>
<td>IT Analyst/Engineer III</td>
<td>$103.38</td>
<td>$105.97</td>
<td>$108.62</td>
<td>$111.33</td>
<td>$114.12</td>
</tr>
<tr>
<td>IT Analyst/Engineer IV</td>
<td>$126.66</td>
<td>$129.82</td>
<td>$133.07</td>
<td>$136.40</td>
<td>$139.81</td>
</tr>
<tr>
<td>IT Analyst/Engineer V</td>
<td>$155.96</td>
<td>$159.86</td>
<td>$163.86</td>
<td>$167.95</td>
<td>$172.15</td>
</tr>
<tr>
<td>IT Program Manager II</td>
<td>$143.43</td>
<td>$147.01</td>
<td>$150.69</td>
<td>$154.45</td>
<td>$158.32</td>
</tr>
<tr>
<td>IT Program Manager III</td>
<td>$117.56</td>
<td>$120.50</td>
<td>$123.51</td>
<td>$126.60</td>
<td>$129.76</td>
</tr>
<tr>
<td>IT Program Support Specialist I</td>
<td>$118.40</td>
<td>$121.36</td>
<td>$124.40</td>
<td>$127.51</td>
<td>$130.70</td>
</tr>
<tr>
<td>IT Program Support Specialist II</td>
<td>$144.42</td>
<td>$148.03</td>
<td>$151.73</td>
<td>$155.52</td>
<td>$159.41</td>
</tr>
<tr>
<td>IT Program Support Specialist III</td>
<td>$161.97</td>
<td>$166.02</td>
<td>$170.17</td>
<td>$174.43</td>
<td>$178.79</td>
</tr>
<tr>
<td>IT Program Support Specialist IV</td>
<td>$196.47</td>
<td>$201.39</td>
<td>$206.42</td>
<td>$211.58</td>
<td>$216.87</td>
</tr>
<tr>
<td>IT Subject Matter Expert I</td>
<td>$77.32</td>
<td>$79.26</td>
<td>$81.24</td>
<td>$83.27</td>
<td>$85.35</td>
</tr>
<tr>
<td>IT Subject Matter Expert II</td>
<td>$93.03</td>
<td>$95.36</td>
<td>$97.74</td>
<td>$100.18</td>
<td>$102.69</td>
</tr>
<tr>
<td>IT Subject Matter Expert III</td>
<td>$111.21</td>
<td>$113.99</td>
<td>$116.84</td>
<td>$119.77</td>
<td>$122.76</td>
</tr>
<tr>
<td>IT Subject Matter Expert IV</td>
<td>$139.01</td>
<td>$142.49</td>
<td>$146.05</td>
<td>$149.70</td>
<td>$153.45</td>
</tr>
<tr>
<td>CyberSecurity Analyst/Engineer I</td>
<td>$173.84</td>
<td>$178.19</td>
<td>$182.64</td>
<td>$187.21</td>
<td>$191.89</td>
</tr>
<tr>
<td>CyberSecurity Analyst/Engineer II</td>
<td>$143.43</td>
<td>$147.01</td>
<td>$150.69</td>
<td>$154.45</td>
<td>$158.32</td>
</tr>
<tr>
<td>CyberSecurity Analyst/Engineer III</td>
<td>$173.84</td>
<td>$178.19</td>
<td>$182.64</td>
<td>$187.21</td>
<td>$191.89</td>
</tr>
<tr>
<td>CyberSecurity Analyst/Engineer IV</td>
<td>$118.40</td>
<td>$121.36</td>
<td>$124.40</td>
<td>$127.51</td>
<td>$130.70</td>
</tr>
<tr>
<td>CyberSecurity Analyst/Engineer V</td>
<td>$144.42</td>
<td>$148.03</td>
<td>$151.73</td>
<td>$155.52</td>
<td>$159.41</td>
</tr>
<tr>
<td>CyberSecurity Program Manager II</td>
<td>$161.97</td>
<td>$166.02</td>
<td>$170.17</td>
<td>$174.43</td>
<td>$178.79</td>
</tr>
<tr>
<td>CyberSecurity Program Manager III</td>
<td>$196.47</td>
<td>$201.39</td>
<td>$206.42</td>
<td>$211.58</td>
<td>$216.87</td>
</tr>
<tr>
<td>CyberSecurity Subject Matter Expert I</td>
<td>$69.64</td>
<td>$71.38</td>
<td>$73.17</td>
<td>$74.99</td>
<td>$76.87</td>
</tr>
<tr>
<td>CyberSecurity Subject Matter Expert II</td>
<td>$87.37</td>
<td>$89.56</td>
<td>$91.79</td>
<td>$94.09</td>
<td>$96.44</td>
</tr>
<tr>
<td>CyberSecurity Subject Matter Expert III</td>
<td>$103.38</td>
<td>$105.97</td>
<td>$108.62</td>
<td>$111.33</td>
<td>$114.12</td>
</tr>
<tr>
<td>CyberSecurity Subject Matter Expert IV</td>
<td>$126.66</td>
<td>$129.82</td>
<td>$133.07</td>
<td>$136.40</td>
<td>$139.81</td>
</tr>
</tbody>
</table>
CyberSecurity Analyst/Engineer I

Functional Responsibilities: The CyberSecurity/Engineer I assists in implementing and remediating complex system-wide cyber security requirements based upon analysis of user and system policies, governing directives and instructions, and resource demands and availability. Supports customers with implementation of doctrine and policies. Provides support in coordinating with organizational stakeholders and leadership to establish and define programs, resources, risks, and mitigations. Provides some degree of knowledge and experience for government and commercial cyber and information systems, such as dedicated special purpose systems requiring specialized security features and procedures; to include computing networks and transports. Possesses the ability for, contribution to, and deciphering of, complex technical documentation for system and architecture diagrams or drawings. Capable of operating computing network defense applications and tools for monitoring and safeguarding. This is an entry-level position that works under immediate supervision.

Minimum Education: Bachelor’s in IT, Telecommunications, or other related field

Minimum Experience: 1 year

CyberSecurity Analyst/Engineer II

Functional Responsibilities: The CyberSecurity Analyst/Engineer II assists in designing, implementing, and remediating complex system-wide cyber security requirements based upon analysis of user and system policies, governing directives and instructions, and resource demands and availability. Assists customers with implementation of doctrine and policies. Provides support in coordinating and communicating with organizational stakeholders and leadership to establish and define programs, resources, risks, and mitigations. Provides knowledge and experience of government and commercial cyber and information systems, such as dedicated special purpose systems requiring specialized security features and procedures; to include computing networks and transports. Possesses the ability for, contribution to, generation and deciphering of complex technical documentation for system and architecture diagrams or drawings. Capable of installing, configuring, and operating computing network defense applications and tools for monitoring and safeguarding. Works under general supervision.

Minimum Education: Bachelor’s in IT, Telecommunications, or other related field

Minimum Experience: 4 years
CyberSecurity Analyst/Engineer III

Functional Responsibilities: The CyberSecurity Analyst/Engineer III designs, implements, and remediates complex system-wide cyber security requirements based upon the analysis of user and system policies, governing directives, and instructions, and resource demands and availability. Supports customers at the highest levels in the development and implementation of doctrine and policies. Coordinates the development, design, and application of solutions implemented by more junior staff members. Applies expertise to government and commercial cyber systems, such as dedicated special purpose systems requiring specialized security features and procedures; to include computing networks and transports. Provides guidance and direction to other professionals, acts in an advisory capacity, coordinates resolution of highly complex problems and tasks. Possesses the ability to generate and decipher complex technical documentation for system and architecture diagrams or drawings. Capable of installing, configuring, and operating computing network defense applications and tools for monitoring and safeguarding. Able to analyze and communicate computing network defense applications and tools outputs to customers and junior staff members. Works independently. May oversee and lead other employees assigned to the task(s).

Minimum Education: Bachelor’s in IT, Telecommunications, or other related field

Minimum Experience: 6 years

CyberSecurity Analyst/Engineer IV

Functional Responsibilities: The CyberSecurity Analyst/Engineer IV provides expert technical analysis, guidance, and direction of cyber security, to include applications, operating systems, physical security, networks, risk assessment, critical infrastructure continuity and contingency planning, emergency preparedness, security awareness, and training. Provides analysis of existing system’s vulnerability to possible intrusions, resource manipulation, resource denial, and destruction of resources. Provides adept technical expertise and analysis of document creation and review, and supports policy and procedures preparation and implementation. Provides expert technical knowledge and analysis of governing directives and instructions. Oversees, leads, and supervises other employees assigned to the task(s).

Minimum Education: Bachelor’s in IT, Telecommunications, or other related field

Minimum Experience: 8 years
CyberSecurity Analyst/Engineer V

**Functional Responsibilities:** The CyberSecurity Analyst/Engineer V establishes and satisfies complex system-wide cyber security requirements based upon the analysis of user and system policies, governing directives and instructions, and resource demands and availability. Supports customers at the highest levels in the development and implementation of doctrine and policies. Provides leadership and guidance in the development, design, and application of solutions implemented by staff members. Coordinates with senior representatives within the customer organization to establish and define programs, resources, and risks. Applies expertise of government and commercial cyber systems, such as dedicated special purpose systems requiring specialized security features and procedures; to include computing networks and transports. Provides guidance and direction to other professionals; acts in a consulting and/or advisory capacity; coordinates resolution of highly complex problems and tasks; and possesses the ability to meet and operate under deadlines. Subject Matter Expert (SME) in a given operating system or computing environment. A SME of computer network defense operations, incident reporting, and governing directives and instructions. Oversees all engineering requirements and personnel as assigned.

**Minimum Education:** Master’s in IT, Telecommunications, or other related field

**Minimum Experience:** 15 years

CyberSecurity Program Manager II

**Functional Responsibilities:** The Program Manager II provides leadership and overall direction of all phases of multiple cyber security programs from inception through completion including overall cost, schedule & performance; formulates and enforces work standards; and solves complex technical, administrative, and management problems. Serves as the single authorized cyber security interface with Government management personnel. Participates in customer cyber security program reviews, identifies cyber security problems, and obtains cyber security solutions. Provides verbal and written skills required to maintain complete cyber security program control.

**Minimum Education:** Bachelor’s in IT, Telecommunications, or other related field

**Minimum Experience:** 10 years

CyberSecurity Program Manager III

**Functional Responsibilities:** The Program Manager III provides top-level leadership and generally supervises two (2) or more cyber security programs/projects at multiple geographic sites. Formulates and enforces work standards; and solves complex technical, administrative, financial, and management problems. Serves as top-level cyber security interface with Government management personnel as well as company senior management. Provides verbal and written skills at all management levels to maintain complete cyber security program control.

**Minimum Education:** Bachelor’s in IT, Telecommunications, or other related field

**Minimum Experience:** 15 years
CyberSecurity Subject Matter Expert I

Functional Responsibilities: The CyberSecurity Subject Matter Expert I provides analytical expertise; applies advanced comprehensive knowledge of cyber security methodologies, theoretical concepts, principles, and practices in specific professional, scientific, or technical disciplines; conducts and directs complex cyber security projects; and performs in a professional position requiring an in-depth knowledge of cyber security. Responsible for ensuring compliance with cyber security technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions.

Minimum Education: Bachelor’s in IT, Telecommunications, or other related field

Minimum Experience: 5 years

CyberSecurity Subject Matter Expert II

Functional Responsibilities: The CyberSecurity SME II provides analytical expertise; applies advanced comprehensive knowledge of cyber security methodologies, theoretical concepts, principles, and practices in specific professional, scientific, or technical disciplines; conducts and directs complex cyber security projects; and performs in a professional position requiring an in-depth knowledge of cyber security. Responsible for ensuring compliance with cyber security technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions.

Minimum Education: Bachelor’s in IT, Telecommunications, or other related field

Minimum Experience: 8 years

CyberSecurity Subject Matter Expert III

Functional Responsibilities: The CyberSecurity SME III provides analytical expertise; applies advanced comprehensive knowledge of cyber security methodologies, theoretical concepts, principles, and practices in specific professional, scientific, or technical disciplines; conducts and directs complex cyber security projects; and performs in a professional position requiring an in-depth knowledge of cyber security. Responsible for ensuring compliance with cyber security technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions.

Minimum Education: Bachelor’s in IT, Telecommunications, or other related field

Minimum Experience: 10 years
CyberSecurity Subject Matter Expert IV

Functional Responsibilities: The CyberSecurity SME IV provides analytical expertise; applies advanced comprehensive knowledge of cyber security methodologies, theoretical concepts, principles, and practices in specific professional, scientific, or technical disciplines; conducts and directs complex cyber security projects; and performs in a professional position requiring an in-depth knowledge of cyber security. Responsible for ensuring compliance with cyber security technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions.

Minimum Education: Bachelor’s in IT, Telecommunications, or other related field

Minimum Experience: 12 years

Experience & Degree Substitution Equivalencies
Experience exceeding the minimum shown may be substituted for education. Likewise, education exceeding the minimum shown may be substituted for experience.

<table>
<thead>
<tr>
<th>Equivalent Degree</th>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate’s</td>
<td>High School or equivalent plus 2 years relevant experience</td>
</tr>
<tr>
<td>Bachelor’s</td>
<td>Associate’s degree + 2 years relevant experience or 4 years relevant experience</td>
</tr>
<tr>
<td>Master’s</td>
<td>Bachelor’s plus 2 years relevant experience or Associate’s degree + 4 years relevant experience</td>
</tr>
<tr>
<td>PhD</td>
<td>Master’s + 2 years relevant experience, or Bachelor’s + 4 years relevant experience or Associate’s + 6 years relevant experience</td>
</tr>
</tbody>
</table>
IT Analyst/Engineer I

**Functional Responsibilities:** The IT Analyst/Engineer I performs as a Junior IT Analyst/Engineer. Applies newly developed skills and knowledge of techniques in a specific technical area. Analyzes, evaluates, and makes IT recommendations as part of a team or under supervision of senior personnel. Performs installations, basic IT troubleshooting, and support functions. May assist with presentations, task planning, resource coordination, and/or budget development as they relate to information technology. Performs in a junior professional level under close supervision and within well-defined guidelines. This is an entry level position that works under immediate supervision.

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field in IT, Telecommunications or other related field

**Minimum Experience:** 1 year

---

IT Analyst/Engineer II

**Functional Responsibilities:** The IT Analyst/Engineer II performs as a Mid-Level IT Analyst/Engineer. Applies newly developed skills and knowledge of techniques in a specific professional, scientific/engineering, or technical area. Analyzes, evaluates, and makes IT recommendations as part of a team or under supervision of senior personnel. Performs installations, basic IT troubleshooting, and support functions. May assist with presentations, task planning, resource coordination, and/or budget development as they relate to information technology. Works under general supervision.

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 4 years

---

IT Analyst/Engineer III

**Functional Responsibilities:** The IT Analyst/Engineer III performs as a Mid-Level IT Analyst/Engineer. Applies newly developed skills and knowledge of techniques in a specific professional, scientific/engineering, or technical area. Analyzes, evaluates, and makes IT recommendations as part of a team or under supervision of senior personnel. Performs installations, basic IT troubleshooting, and support functions. May assist with presentations, task planning, resource coordination, and/or budget development as they relate to information technology. Works under general supervision.

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 6 years
IT Analyst/Engineer IV

**Functional Responsibilities:** The IT Analyst/Engineer IV performs as a Principal IT Analyst/Engineer. Applies advanced comprehensive knowledge of IT methodologies, theoretical concepts, principles, and practices in technical disciplines; conducts and directs complex projects; and performs in a professional position requiring an in-depth knowledge of information technology. Responsible for ensuring compliance with technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions. May oversee and lead other employees assigned to the task(s).

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 8 years

IT Analyst/Engineer V

**Functional Responsibilities:** The IT Analyst/Engineer V provides the highest level of analytical expertise; applies advanced comprehensive knowledge of IT methodologies, theoretical concepts, principles, and practices in specific professional, scientific, or technical disciplines; conducts and directs complex projects; and performs in a professional position requiring an in-depth knowledge of information technology. Responsible for ensuring compliance with technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions. Oversees all engineering requirements and personnel as assigned.

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 15 years

IT Program Manager II

**Functional Responsibilities:** The IT Program Manager II provides leadership and overall direction of all phases of multiple IT programs from inception through completion including overall cost, schedule & performance; formulates and enforces work standards; and solves complex technical, administrative, and management problems as they relate to information technology. Serves as the single authorized interface with Government management personnel. Participates in customer IT program reviews, identifies technical problems, and obtains solutions. Provides verbal and written skills required to maintain complete IT program control.

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 10 years
**IT Program Manager III**

**Functional Responsibilities:** The IT Program Manager III provides top-level leadership and generally supervises two (2) or more IT programs/projects at multiple geographic sites. Formulates and enforces work standards; and solves complex technical, administrative, financial, and management problems as they relate to information technology. Serves as top-level interface with Government management personnel as well as company senior management. Provides verbal and written skills at all management levels to maintain complete program control.

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 15 years

---

**IT Program Support Specialist I**

**Functional Responsibilities:** The IT Program Support Specialist I performs as Junior Support Specialist. Assists in monitoring financial and/or administrative aspects of assigned contracts and deliverables. May also be asked to provide documentation planning and support, project administration, general office support, and executive secretarial support as needed. This is an entry level position that works under immediate supervision.

**Minimum Education:** Associate’s in IT, Telecommunications or other related field

**Minimum Experience:** 1 year

---

**IT Program Support Specialist II**

**Functional Responsibilities:** The IT Program Support Specialist II performs as Support Specialist. Monitors financial and/or administrative aspects of assigned IT contracts and deliverables as follows: Tracks and validates all client financial information; establishes and maintains master contract files; prepares and monitors status of all deliverables; tracks the value of contracts; and reports payment of government fees as they relate to information technology. Updates IT task reports with funding information and prepares revenue projections for all active contract TOs. May also provide IT documentation planning and support, general office support, and executive secretarial support. May use automated systems to track IT deliverables, financial transactions, and management information. Works under general supervision.

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 3 years
IT Program Support Specialist III

**Functional Responsibilities:** The IT Program Support Specialist III performs as Senior Support Specialist. Works with Program Management to implement financial and/or administrative aspects of assigned IT contracts and deliverables as follows: Tracks and validates all client financial information; establishes and maintains master contract files; prepares and monitors status of all deliverables; tracks the value of contracts; and reports payment of government fees as they relate to information technology. Interfaces with Program Management and government customers with regards to revenue projections for all active IT contract TOs. May also provide IT documentation development, planning, and support to Program Management and executive secretarial support. Uses automated systems to track IT deliverables, financial transactions, and management information. May oversee and lead other employees assigned to the task(s).

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 8 years

IT Program Support Specialist IV

**Functional Responsibilities:** The IT Program Support Specialist IV performs as Senior Support Specialist. Works with Program Management to implement financial and/or administrative aspects of assigned IT contracts and deliverables as follows: Tracks and validates all client financial information; establishes and maintains master contract files; prepares and monitors status of all deliverables; tracks the value of contracts; and reports payment of government fees as they relate to information technology. Interfaces with Program Management and government customers with regards to revenue projections for all active IT contract TOs. May also provide IT documentation development, planning, and support to Program Management and executive secretarial support. Uses automated systems to track IT deliverables, financial transactions, and management information. May oversee and lead other employees assigned to the task(s). May oversee and lead other employees assigned to the task(s).

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 12 years

IT Subject Matter Expert I

**Functional Responsibilities:** The IT Subject Matter Expert (SME) I provides analytical expertise; applies advanced comprehensive knowledge of IT methodologies, theoretical concepts, principles, and practices in specific technical disciplines; conducts and directs complex IT related projects; and performs in a professional position requiring an in-depth knowledge of information technology. Responsible for ensuring compliance with technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions.

**Minimum Education:** Bachelor’s in IT, Telecommunications or other related field

**Minimum Experience:** 5 years
IT Subject Matter Expert II

Functional Responsibilities: The IT SME II provides analytical expertise; applies advanced comprehensive knowledge of IT methodologies, theoretical concepts, principles, and practices in specific professional, scientific, or technical disciplines; conducts and directs complex IT related projects; and performs in a professional position requiring an in-depth knowledge of information technology. Responsible for ensuring compliance with technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions.

Minimum Education: Bachelor’s in IT, Telecommunications or other related field

Minimum Experience: 8 years

IT Subject Matter Expert III

Functional Responsibilities: The IT SME III provides analytical expertise; applies advanced comprehensive knowledge of IT methodologies, theoretical concepts, principles, and practices in specific professional, scientific, or technical disciplines; conducts and directs complex IT related projects; and performs in a professional position requiring an in-depth knowledge of information technology. Responsible for ensuring compliance with technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions.

Minimum Education: Bachelor’s in IT, Telecommunications or other related field

Minimum Experience: 10 years

IT Subject Matter Expert IV

Functional Responsibilities: The IT SME IV provides analytical expertise; applies advanced comprehensive knowledge of IT methodologies, theoretical concepts, principles, and practices in specific professional, scientific, or technical disciplines; conducts and directs complex IT related projects; and performs in a professional position requiring an in-depth knowledge of information technology. Responsible for ensuring compliance with technological standards throughout the project and operates with considerable latitude for un-reviewed actions or decisions.

Minimum Education: Bachelor’s in IT, Telecommunications or other related field

Minimum Experience: 12 years
Experience & Degree Substitution Equivalencies
Experience exceeding the minimum shown may be substituted for education. Likewise, education exceeding the minimum shown may be substituted for experience.

<table>
<thead>
<tr>
<th>Equivalent Degree</th>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate’s</td>
<td>High School or equivalent plus 2 years relevant experience</td>
</tr>
<tr>
<td>Bachelor’s</td>
<td>Associate’s degree + 2 years relevant experience or 4 years relevant experience</td>
</tr>
<tr>
<td>Master’s</td>
<td>Bachelor’s plus 2 years relevant experience or Associate’s degree + 4 years relevant experience</td>
</tr>
<tr>
<td>PhD</td>
<td>Master’s + 2 years relevant experience, or Bachelor’s + 4 years relevant experience or Associate’s + 6 years relevant experience or 8 years relevant experience</td>
</tr>
</tbody>
</table>