GENERAL SERVICES ADMINISTRATION

Federal Supply Service

Authorized Federal Supply Schedule Price List

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.

Multiple Award Schedule

FSC Group: Information Technology

FSC Class:

Contract number: 47QTCA22D00CB

Contract period: August 22, 2022 through August 21, 2027

Contractor's name,
3040 Williams Dr., Suite 150
Fairfax, VA 22031
202-903-5955

Contractor’s internet address/web site where schedule information can be found:
www.bulletproofsi.com

Contract administration source (if different from preceding entry).
Gus Fritschie
gus.fritschie@bulletproofsi.com
202-903-5955

Business size:
Small

For more information on ordering from Federal Supply Schedules go to the GSA Schedules page at GSA.gov.

Prices Shown Herein are Net (discount deducted)
CUSTOMER INFORMATION

1a. Table of awarded special item number(s) with appropriate cross-reference to item descriptions and awarded price(s).

<table>
<thead>
<tr>
<th>SINs</th>
<th>Recovery</th>
<th>SIN Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>54151SRC</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>54151HACS</td>
<td>54151HACSRC</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>541990RISK</td>
<td>541990RISKRC</td>
<td>Risk Assessment and Mitigation Services</td>
</tr>
<tr>
<td>OLM</td>
<td>OLMSTLOC OLMRC</td>
<td>Order-Level Materials (OLM’s)</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. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply. See Page 4

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate “Not applicable” for this item. See Page 4

2. Maximum order:

<table>
<thead>
<tr>
<th>SINs</th>
<th>Maximum Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>$500,000</td>
</tr>
<tr>
<td>54151HACS</td>
<td>$500,000</td>
</tr>
<tr>
<td>541990RISK</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>OLM</td>
<td>$250,000</td>
</tr>
</tbody>
</table>

3. Minimum order: $100

4. Geographic coverage (delivery area). Worldwide

5. Point(s) of production (city, county, and State or foreign country).
3040 Williams Dr., Suite 150, Fairfax, VA  22031

6. Discount from list prices or statement of net price. Government Net Prices (discounts already deducted.)

7. Quantity discounts.
05% for orders $150,000-$300,000
1% for orders over $300,000
8. Prompt payment terms. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions. Net 30 days

9. Foreign items. Not Applicable

10a. Time of delivery. To Be Determined at the Task Order level

10b. Expedited Delivery. Items available for expedited delivery are noted in this price list. To Be Determined at the Task Order level

10c. Overnight and 2-day delivery. To Be Determined at the Task Order level

10d. Urgent Requirements. To Be Determined at the Task Order level

11. F.O.B. point(s). Destination

12a. Ordering address.
3040 Williams Dr., Suite 150, Fairfax, VA 22031

12b. 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.

13. Payment address.
3040 Williams Dr., Suite 150, Fairfax, VA 22031

14. Warranty provision. Standard Commercial Warranty Terms & Conditions

15. Export packing charges, if applicable. Not Applicable

16. Terms and conditions of rental, maintenance, and repair (if applicable). Not Applicable

17. Terms and conditions of installation (if applicable). Not Applicable

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). Not Applicable

18b. Terms and conditions for any other services (if applicable). Not Applicable

19. List of service and distribution points (if applicable). Not Applicable

20. List of participating dealers (if applicable). Not Applicable

21. Preventive maintenance (if applicable). Not Applicable

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). Not Applicable
22b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor’s website or other location.) The EIT standards can be found at: www.Section508.gov.
Not Applicable

23. Unique Entity Identifier (UEI) number. CYXRLNTC81G7

24. Notification regarding registration in System for Award Management (SAM) database. Contractor registered and active in SAM

<table>
<thead>
<tr>
<th>SIN</th>
<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>54151S</td>
<td>IT Program Manager</td>
<td>$207.96</td>
<td>$214.20</td>
<td>$220.62</td>
<td>$227.24</td>
<td>$234.06</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Project Manager</td>
<td>$188.61</td>
<td>$194.27</td>
<td>$200.10</td>
<td>$206.10</td>
<td>$212.29</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Subject Matter Expert</td>
<td>$242.30</td>
<td>$249.57</td>
<td>$257.05</td>
<td>$264.76</td>
<td>$272.71</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Lead Consultant</td>
<td>$169.27</td>
<td>$174.35</td>
<td>$179.58</td>
<td>$184.97</td>
<td>$190.51</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Senior Consultant</td>
<td>$145.09</td>
<td>$149.44</td>
<td>$153.92</td>
<td>$158.54</td>
<td>$163.30</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Consultant</td>
<td>$120.91</td>
<td>$124.53</td>
<td>$128.27</td>
<td>$132.12</td>
<td>$136.08</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Security Analyst I</td>
<td>$164.43</td>
<td>$169.37</td>
<td>$174.45</td>
<td>$179.68</td>
<td>$185.07</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Security Analyst II</td>
<td>$178.94</td>
<td>$184.31</td>
<td>$189.84</td>
<td>$195.53</td>
<td>$201.40</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Security Analyst III</td>
<td>$188.61</td>
<td>$194.27</td>
<td>$200.10</td>
<td>$206.10</td>
<td>$212.29</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Security Engineer I</td>
<td>$183.78</td>
<td>$189.29</td>
<td>$194.97</td>
<td>$200.82</td>
<td>$206.84</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Security Engineer II</td>
<td>$203.12</td>
<td>$209.22</td>
<td>$215.49</td>
<td>$221.96</td>
<td>$228.62</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Security Engineer III</td>
<td>$212.80</td>
<td>$219.18</td>
<td>$225.76</td>
<td>$232.53</td>
<td>$239.50</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Technical Writer</td>
<td>$111.23</td>
<td>$114.57</td>
<td>$118.01</td>
<td>$121.55</td>
<td>$125.20</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Analyst I</td>
<td>$164.43</td>
<td>$169.37</td>
<td>$174.45</td>
<td>$179.68</td>
<td>$185.07</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Analyst II</td>
<td>$178.94</td>
<td>$184.31</td>
<td>$189.84</td>
<td>$195.53</td>
<td>$201.40</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Analyst III</td>
<td>$188.61</td>
<td>$194.27</td>
<td>$200.10</td>
<td>$206.10</td>
<td>$212.29</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Engineer I</td>
<td>$183.78</td>
<td>$189.29</td>
<td>$194.97</td>
<td>$200.82</td>
<td>$206.84</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Engineer II</td>
<td>$203.12</td>
<td>$209.22</td>
<td>$215.49</td>
<td>$221.96</td>
<td>$228.62</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Engineer III</td>
<td>$212.80</td>
<td>$219.18</td>
<td>$225.76</td>
<td>$232.53</td>
<td>$239.50</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cloud Security Engineer</td>
<td>$183.78</td>
<td>$189.29</td>
<td>$194.97</td>
<td>$200.82</td>
<td>$206.84</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester</td>
<td>$149.92</td>
<td>$154.42</td>
<td>$159.05</td>
<td>$163.83</td>
<td>$168.74</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Senior Penetration Tester</td>
<td>$169.27</td>
<td>$174.35</td>
<td>$179.58</td>
<td>$184.97</td>
<td>$190.51</td>
</tr>
<tr>
<td>541990RISK</td>
<td>Risk Program Manager</td>
<td>$207.96</td>
<td>$214.20</td>
<td>$220.62</td>
<td>$227.24</td>
<td>$234.06</td>
</tr>
<tr>
<td>541990RISK</td>
<td>Risk Project Manager</td>
<td>$188.61</td>
<td>$194.27</td>
<td>$200.10</td>
<td>$206.10</td>
<td>$212.29</td>
</tr>
<tr>
<td>541990RISK</td>
<td>Risk Subject Matter Expert</td>
<td>$242.30</td>
<td>$249.57</td>
<td>$257.05</td>
<td>$264.76</td>
<td>$272.71</td>
</tr>
<tr>
<td>541990RISK</td>
<td>Risk Lead Consultant</td>
<td>$169.27</td>
<td>$174.35</td>
<td>$179.58</td>
<td>$184.97</td>
<td>$190.51</td>
</tr>
<tr>
<td>541990RISK</td>
<td>Risk Senior Consultant</td>
<td>$145.09</td>
<td>$149.44</td>
<td>$153.92</td>
<td>$158.54</td>
<td>$163.30</td>
</tr>
</tbody>
</table>
541990 RISK
Risk Consultant
$120.91 $124.53 $128.27 $132.12 $136.08
Risk Assessment and Mitigation Associate I
$111.23 $114.57 $118.01 $121.55 $125.20
Risk Assessment and Mitigation Associate II
$120.91 $124.53 $128.27 $132.12 $136.08
Risk Assessment and Mitigation Associate III
$138.32 $142.47 $146.74 $151.14 $155.68
Risk IT Technical Writer
$111.23 $114.57 $118.01 $121.55 $125.20

3% escalation rate

54151S
IT Program Manager
Manages contract support operations, involving multiple projects and groups of personnel at multiple locations. Manages corporate management structure to direct effective contract support activities. Can lead multiple projects that involve the successful management of teams composed of information system or information technology professionals who are responsible for analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunication systems. Must have demonstrated capability for oral and written communications with all levels of management. Must have a thorough knowledge of the capabilities of applicable computer and communications configurations. Meets with customer and contractor personnel to formulate and review task plans and deliverable items. Ensures conformance with task schedules and costs.
Minimum Experience: Minimum of 10 years of IT experience, including at least 5 years of IT project or program management experience. Advanced degree can substitute for years of experience.
Minimum Education: Bachelor's degree in relevant IT or business discipline.

IT Project Manager
Manages projects that involve teams of information system or information technology professionals who are responsible for analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunication systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. Organizes, directs, and coordinates the planning and production of all activities associated with assigned delivery order projects. Must have demonstrated capability for oral and written communications.
Minimum Experience: Minimum of 3 years of IT or telecommunications project management experience. Advanced degree may substitute for years of experience.
Minimum Education: Bachelor's degree in relevant IT or business discipline.

IT Subject Matter Expert
Has expert understanding of complex IT environments. Deploys solutions and provides expert advisory in areas of IT, security and risk. May initiate, supervise, or develop requirements from a project's inception to conclusion for complex programs. Provides strategic advice, technical guidance and expertise to program and project staff. Provides analysis, evaluation and recommendations for improvements, optimization development, or maintenance efforts for client-specific or critical challenges/issues. Assists and guides project team members and delivers presentations to client executives.
Minimum Experience: Minimum of 5 years specialized experience, including specialized experience in cyber, risk, or IT fields.
Minimum Education: Bachelor's degree in relevant IT or business discipline.

IT Lead Consultant
Assists in the assessment, development, implementation and maintenance of enterprise IT, Cybersecurity and Risk programs. Consults on and develops solutions to enable adoption of standards, policy and procedures, as well as measure performance and compliance. Develops policy, procedures, and best practices. Devises solutions for networks, applications, information and business processes. Conducts system reviews and analyses, performs security and risk assessments, consults on integration of new solutions, and ensures IT and security controls are in place and operating effectively. Prepares presentations, papers and other materials to support program managers, CIOs, and CISOs. Prepares and provides management and project reports.
Minimum Experience: Minimum of 5 years of experience supporting IT, cybersecurity, risk and related projects.
Minimum Education: Bachelor's degree in computer sciences, information systems, business administration or other related technical or scientific discipline.

IT Senior Consultant
Assists in the assessment, development, implementation and maintenance of enterprise IT, Cybersecurity and Risk programs. Consults on and develops solutions to enable adoption of standards, policy and procedures, as well as measure performance and compliance. Develops policy, procedures, and best practices. Devises solutions for networks, applications, information and business processes. Conducts system reviews and analyses, performs security and risk assessments, consults on integration of new solutions, and ensures IT and security controls are in place and operating effectively. Prepares
presentations, papers and other materials to support program managers, CIOs, and CISOs. Prepares and provides management and project reports. Provides technical leadership and direction in support of project manager. **Minimum Experience:** Minimum of 3 years of experience supporting IT, cybersecurity, risk and related projects. **Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**IT Consultant**
Assists in the assessment, development, implementation and maintenance of enterprise IT, Cybersecurity and Risk programs. Consults on and develops solutions to enable adoption of standards, policy and procedures, as well as measure performance and compliance. Develops policy, procedures, and best practices. Devises solutions for networks, applications, information and business processes. Conducts system reviews and analyses, performs security and risk assessments, consults on integration of new solutions, and ensures IT and security controls are in place and operating effectively. **Minimum Experience:** Up to 3 years of experience supporting IT, cybersecurity, risk and related projects. **Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**IT Security Analyst I**
Analyzes, defines, and recommends IT security requirements. Verifies whether IT system protections meet designated certification and accreditation criteria. Plans, implements, upgrades, or monitors IT security measures for the protection of computer networks and information. May ensure appropriate IT security controls are in place that will safeguard digital assets and infrastructure. May perform monitoring and analysis of various IT security solutions and, including SIEM solutions, to detect the presence of unknown or suspected cyber threats. May actively monitor IT security threats and risks, provide in-depth incident analysis, evaluate IT security incidents, and provide proactive threat research. May provide first tier response to IT security incidents and coordinate with threat operations team to resolve high severity level incidents. May track investigation results and reports on findings. **Minimum Experience:** Up to 3 years of experience providing analytical support to IT, cyber, risk and assessment projects. **Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**IT Security Analyst II**
Analyzes, defines, and recommends IT security requirements. Verifies whether IT system protections meet designated certification and accreditation criteria. Plans, implements, upgrades, or monitors IT security measures for the protection of computer networks and information. May ensure appropriate IT security controls are in place that will safeguard digital assets and infrastructure. May perform monitoring and analysis of various IT security solutions and, including SIEM solutions, to detect the presence of unknown or suspected cyber threats. May actively monitor IT security threats and risks, provide in-depth incident analysis, evaluate IT security incidents, and provide proactive threat research. May provide second tier response to IT security incidents and coordinate with threat operations team to resolve high severity level incidents. May track investigation results and reports on findings. **Required Experience:** Minimum of 3 years of experience providing analytical support to IT, cyber, risk and assessment projects. **Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**IT Security Analyst III**
Analyzes, defines, and recommends IT security requirements. Verifies whether IT system protections meet designated certification and accreditation criteria. Plans, implements, upgrades, or monitors IT security measures for the protection of computer networks and information. May ensure appropriate IT security controls are in place that will safeguard digital assets and infrastructure. May perform monitoring and analysis of various IT security solutions and, including SIEM solutions, to detect the presence of unknown or suspected cyber threats. May actively monitor IT security threats and risks, provide in-depth incident analysis, evaluate IT security incidents, and provide proactive threat research. May provide third tier response to IT security incidents and coordinate with threat operations team to resolve high severity level incidents. May track investigation results and reports on findings. **Required Experience:** Minimum of 5 years of experience providing analytical support to IT, cyber, risk and assessment projects. **Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**IT Security Engineer I**
Provides IT security architecture, policy, and design guidance for IT systems and networks. Provides technical expertise in IT security. Gathers, organizes and analyzes technical information about an organization's goals, needs and strategy, existing IT and security products, and ongoing IT and security programs. Designs, develops, engineers, and implements IT solutions to IT security requirements and is responsible for the implementation and development of IT security. Reports orally and in writing to the Program Manager, Project Manager, contractor management, and government representatives. **Required Experience:** Up to 3 years of technical experience in defining IT security requirements for high level applications, evaluation of approved IT security product capabilities, and developing IT solutions to multilevel IT security problems. **Required Education:** Bachelor's degree in relevant IT or business discipline.

**IT Security Engineer II**
Functional Responsibility: Provides IT security architecture, policy, and design guidance for IT systems and networks. Serves as the senior technical expert on complex and challenging IT/security system projects. May be assigned as team leader on tasks of various technical disciplines or may work alone or as part of a team of Information Technology Security Engineers. Provides highly technical expertise in multilevel IT security. Gathers and organizes technical information about an organization’s goals and needs, existing IT and security products, and ongoing IT and security programs in the multilevel security arena. Designs, develops, engineers, and implements IT solutions to multilevel IT security requirements and is responsible for the implementation and development of multilevel IT security. Reports orally and in writing to the Program Manager, Project Manager, contractor management, and government representatives. May serve as the Contractor's authorized interface with the Contracting Officer's Representative/Technical Representative (COR/COTR).

Required Experience: Minimum 5 years of increasing responsibility and specialized experience in defining computer security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to multilevel security problems.

Required Education: Bachelor's degree in relevant IT or business discipline.

IT Security Engineer III

Functional Responsibility: Serves as the senior technical expert on complex and challenging IT system projects. May be assigned as team leader on tasks of various technical disciplines or may work alone or as part of a team of Information Technology Security Engineers. Provides highly technical expertise in multilevel IT security. Gathers and organizes technical information about an organization’s goals and needs, existing IT and security products, and ongoing IT and security programs in the multilevel security arena. Designs, develops, engineers, and implements IT solutions to multilevel IT security requirements and is responsible for the implementation and development of multilevel IT security. Reports orally and in writing to the Program Manager, Project Manager, contractor management, and government representatives. May serve as the Contractor's authorized interface with the Contracting Officer's Representative/Technical Representative (COR/COTR), government management personnel, and agency representatives.

Required Experience: Minimum 5 years of increasing responsibility and specialized experience in defining computer security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to multilevel security problems.

Required Education: Bachelor's degree in relevant IT or business discipline.

IT Technical Writer

Functional Responsibility: Develops, writes, and edits functional descriptions, system specifications, user's manuals, special reports, or any other deliverables and documents. Observes production and experimental activities to determine operating procedure and detail. Interviews production and engineering personnel, researches other material to become familiar with product technologies and production methods, reviews manufacturer’s and trade catalogs, drawings and other data relative to operation, maintenance, and service of equipment. Organizes material and completes writing assignment according to set standards regarding order, clarity, conciseness, style, and terminology and recommends revisions or changes in scope, format, content, and methods of reproduction and binding. Maintains records and files of work and revisions, selects photographs, drawings, sketches, diagrams, and charts to illustrate material, edits, standardizes, or changes material prepared by other writers or technical personnel. Reports orally and in writing to the Program Manager, Project Manager, contractor management, and government representatives.

Required Experience: Up to 3 years of technical experience in collecting and organizing information required for preparation of user’s manuals, training materials, installation guides, proposals, reports, and other systems/applications documentation. Required Education: Bachelor’s degree in relevant IT or business discipline. Experience may be substituted at the rate of two years of directly related experience for each year of education.

Security Analyst I

Analyzes, defines, and recommends security requirements. Verifies whether system protections meet designated certification and accreditation criteria. Plans, implements, upgrades, or monitors security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital assets and infrastructure. May perform monitoring and analysis of various security solutions and, including SIEM solutions, to detect the presence of unknown or suspected cyber threats. May actively monitor security threats and risks, provide in-depth incident analysis, evaluate security incidents, and provide proactive threat research. May provide first tier response to security incidents and coordinate with threat operations team to resolve high severity level incidents. May track investigation results and reports on findings.

Minimum Experience: Up to 3 years of experience providing analytical support to IT, cyber, risk and assessment projects.

Minimum Education: Bachelor’s degree in relevant IT or business discipline.

Security Analyst II

Analyzes, defines, and recommends security requirements. Verifies whether system protections meet designated certification and accreditation criteria. Plans, implements, upgrades, or monitors security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital assets and infrastructure. May perform monitoring and analysis of various security solutions and, including SIEM solutions, to detect the presence of unknown or suspected cyber threats. May actively monitor security threats and risks, provide in-depth incident analysis, evaluate security incidents, and provide proactive threat research. May provide first tier response to security incidents and coordinate with threat operations team to resolve high severity level incidents. May track investigation results and reports on findings.

Minimum Experience: Up to 3 years of experience providing analytical support to IT, cyber, risk and assessment projects.

Minimum Education: Bachelor’s degree in relevant IT or business discipline.
unknown or suspected cyber threats. May actively monitor security threats and risks, provide in-depth incident analysis, evaluate security incidents, and provide proactive threat research. May provide second tier response to security incidents and coordinate with threat operations team to resolve high severity level incidents. May track investigation results and reports on findings.

**Required Experience:** Minimum of 3 years of experience providing analytical support to IT, cyber, risk and assessment projects.

**Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**Security Analyst III**

Analyzes, defines, and recommends security requirements. Verifies whether system protections meet designated certification and accreditation criteria. Plans, implements, upgrades, or monitors security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital assets and infrastructure. May perform monitoring and analysis of various security solutions and, including SIEM solutions, to detect the presence of unknown or suspected cyber threats. May actively monitor security threats and risks, provide in-depth incident analysis, evaluate security incidents, and provide proactive threat research. May provide third tier response to security incidents and coordinate with threat operations team to resolve high severity level incidents. May track investigation results and reports on findings.

**Required Experience:** Minimum of 3 years of experience providing analytical support to IT, cyber, risk and assessment projects.

**Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**Security Engineer I**

Provides security architecture, policy, and design guidance for systems and networks. Provides technical expertise in security. Gathers, organizes and analyzes technical information about an organization's goals, needs and strategy, existing IT and security products, and ongoing IT and security programs. Designs, develops, engineers, and implements solutions to security requirements and is responsible for the implementation and development of security. Reports orally and in writing to the Program Manager, Project Manager, contractor management, and government representatives.

**Required Experience:** Up to 3 years of technical experience in defining computer security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to multilevel security problems.

**Required Education:** Bachelor's degree in relevant IT or business discipline.

**Security Engineer II**

**Functional Responsibility:** Provides security architecture, policy, and design guidance for systems and networks. Serves as the senior technical expert on complex and challenging IT/security system projects. Gathers, organizes and analyzes technical information about an organization's goals, needs and strategy, existing IT and security products, and ongoing IT and security programs. Designs, develops, engineers, and implements solutions to security requirements and is responsible for the implementation and development of security. Reports orally and in writing to the Program Manager, Project Manager, contractor management, and government representatives. May serve as the Contractor's authorized interface with the Contracting Officer's Representative/Technical Representative (COR/COTR), government management personnel, and agency representatives.

**Required Experience:** Minimum 3 years of increasing responsibility and specialized experience in defining computer security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to multilevel security problems.

**Required Education:** Bachelor's degree in relevant IT or business discipline.

**Security Engineer III**

**Functional Responsibility:** Serves as the senior technical expert on complex and challenging IT system projects. May be assigned as team leader on tasks of various technical disciplines or may work alone or as part of a team of Information Security Engineers. Provides highly technical expertise in multilevel security. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the multilevel security arena. Designs, develops, engineers, and implements solutions to multilevel security requirements and is responsible for the implementation and development of multilevel security. Reports orally and in writing to the Program Manager, Project Manager, contractor management, and government representatives. May serve as the Contractor's authorized interface with the Contracting Officer's Representative/Technical Representative (COR/COTR), government management personnel, and agency representatives.

**Required Experience:** Minimum 5 years of increasing responsibility and specialized experience in defining computer security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to multilevel security problems.

**Required Education:** Bachelor’s degree in Computer Science, Information Systems, Engineering, Math, Business or other related scientific or technical discipline.

**Cloud Security Engineer**
**Functional Responsibility**: Provides expertise in defining security requirements and developing security solutions that ensure mitigation of risk identified in cloud based solutions. Defines and develops security policies and processes related to the protection of sensitive or classified information. Plans, implements, upgrades and monitors security controls for the protection of cloud based networks and information systems. Provides technical assistance in the selection, configuration, and maintenance of cloud security devices/systems including, but not limited to, firewalls, IPS/IDS, SIEM, WAF, Network-based Malware detection and related platforms as well as software-defined systems. Designs, develops, engineers and implements solutions to protection of sensitive or classified information. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solutions. Analyzes general information assurance and cyber security-related technical problems and provides basic engineering and technical support in solving these problems. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle. This will require practical use and understanding of advanced security protocols and standards, and solid knowledge of information security principles and practices as well as latest scalable technologies.

**Minimum Experience**: Minimum 1 year of experience. Experience in systems analysis and programming preferred.

**Minimum Education**: Bachelor's degree in relevant IT or business discipline.

---

**Penetration Tester**

**Functional Responsibility**: Performs authorized penetration testing activities on enterprise network assets to uncover vulnerabilities across platforms. Emulates adversarial cyber activities to identify weaknesses, enumerate vulnerabilities and assess the overall security posture of customer networks and information systems. Analyzes policies and configurations and evaluates compliance with regulations, enterprise directives and best practices. Assesses threats to the environment via penetration testing, risk assessments, and other assessments. Provides input on the adequacy of security designs and architectures. Scopes assessments, develops penetration test plans, identifies and exploits vulnerabilities, drafts reports and communicates results to key stakeholders.

**Minimum Experience**: Up to 3 years of experience supporting ethical hacking and related projects.

**Minimum Education**: Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT, CEH, CISSP or other Penetration Testing certification.

---

**Senior Penetration Tester**

**Functional Responsibility**: Performs authorized penetration testing activities on enterprise network assets to uncover vulnerabilities across platforms. Emulates adversarial cyber activities to identify weaknesses, enumerate vulnerabilities and assess the overall security posture of customer networks and information systems. Analyzes policies and configurations and evaluates compliance with regulations, enterprise directives and best practices. Assesses threats to the environment via penetration testing, risk assessments, and other assessments. Provides input on the adequacy of security designs and architectures. Scopes assessments, develops penetration test plans, identifies and exploits vulnerabilities, drafts reports and communicates results to key stakeholders.

**Minimum Experience**: Minimum of 3 years of experience supporting ethical hacking and related projects.

**Minimum Education**: Must have one of the following certifications: OSCP, GIAC GPEN, GWAPT, CEH, CISSP or other Penetration Testing certification.

---

**Risk Program Manager**

Manages risk contract support operations, involving multiple projects and groups of personnel at multiple locations. Manages corporate management structure to direct effective contract support activities. Can lead multiple projects that involve the successful management of teams composed of information system or information technology professionals who are responsible for analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunication systems. Must have demonstrated capability for oral and written communications with all levels of management. Must have a thorough knowledge of the capabilities of applicable computer and communications configurations. Meets with customer and contractor personnel to formulate and review task plans and deliverable items. Ensures conformance with task schedules and costs.

**Minimum Experience**: Minimum of 10 years of IT experience, including at least 5 years of IT project or program management experience. Advanced degree can substitute for years of experience.

**Minimum Education**: Bachelor's degree in relevant IT or business discipline.

---

**Risk Project Manager**

Manages risk projects that involve teams of information system or information technology professionals who are responsible for analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunication systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. Organizes, directs, and coordinates the planning and production of all activities associated with assigned delivery order projects. Must have demonstrated capability for oral and written communications.

**Minimum Experience**: Minimum of 3 years of IT or telecommunications project management experience. Advanced degree may substitute for years of experience.

**Minimum Education**: Bachelor's degree in relevant IT or business discipline.

---

**Risk Subject Matter Expert**
Has expert understanding of complex risk IT environments. Deploys solutions and provides expert advisory in areas of IT, security and risk. May initiate, supervise, or develop requirements from a project’s inception to conclusion for complex programs. Provides strategic advice, technical guidance and expertise to program and project staff. Provides analysis, evaluation and recommendations for improvements, optimization development, or maintenance efforts for client-specific or critical challenges/issues. Assists and guides project team members and delivers presentations to client executives.

**Minimum Experience:** Minimum of 5 years specialized experience, including specialized experience in cyber, risk, or IT fields.

**Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**Risk Lead Consultant**
Assists in the assessment, development, implementation and maintenance of risk enterprise IT, Cybersecurity and Risk programs. Consults on and develops solutions to enable adoption of standards, policy and procedures, as well as measure performance and compliance. Develops policy, procedures, and best practices. Devises solutions for networks, applications, information and business processes. Conducts system reviews and analyses, performs security and risk assessments, consults on integration of new solutions, and ensures IT and security controls are in place and operating effectively. Prepares presentations, papers and other materials to support program managers, CIOs, and CISOs. Prepares and provides management and project reports.

**Minimum Experience:** Minimum of 5 years of experience supporting IT, cybersecurity, risk and related projects.

**Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**Risk Senior Consultant**
Assists in the assessment, development, implementation and maintenance of risk enterprise IT, Cybersecurity and Risk programs. Consults on and develops solutions to enable adoption of standards, policy and procedures, as well as measure performance and compliance. Develops policy, procedures, and best practices. Devises solutions for networks, applications, information and business processes. Conducts system reviews and analyses, performs security and risk assessments, consults on integration of new solutions, and ensures IT and security controls are in place and operating effectively. Prepares presentations, papers and other materials to support program managers, CIOs, and CISOs. Prepares and provides management and project reports. Provides technical leadership and direction in support of project manager.

**Minimum Experience:** Minimum of 3 years of experience supporting IT, cybersecurity, risk and related projects.

**Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**Risk Consultant**
Assists in the assessment, development, implementation and maintenance of risk enterprise IT, Cybersecurity and Risk programs. Consults on and develops solutions to enable adoption of standards, policy and procedures, as well as measure performance and compliance. Develops policy, procedures, and best practices. Devises solutions for networks, applications, information and business processes. Conducts system reviews and analyses, performs security and risk assessments, consults on integration of new solutions, and ensures IT and security controls are in place and operating effectively.

**Minimum Experience:** Up to 3 years of experience supporting IT, cybersecurity, risk and related projects.

**Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**Risk Assessment and Mitigation Associate I**
**Functional Responsibility:** Assists in evaluating cybersecurity risks, testing controls designed to mitigate risk, and communicating issues and findings to management. Performs audits and assessments focused on evaluating the effectiveness of security governance, tools and operations. Evaluates the design, effectiveness and efficiency of information technology and security processes, procedures, and technical controls including solution/system implementations, identify and address gaps in cybersecurity risk management. Provides detailed risk assessments, risk explanations and mitigation recommendations. Designs and develops new business processes, procedures and policies in response to risk assessments, and ensures compliance with governance and regulatory requirements.

**Minimum Experience:** Up to 3 years of experience participating in projects as a team member, with specific experience in one or more key project areas.

**Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**Risk Assessment and Mitigation Associate II**
**Functional Responsibility:** Assists in evaluating cybersecurity risks, testing controls designed to mitigate risk, and communicating issues and findings to management. Performs audits and assessments focused on evaluating the effectiveness of security governance, tools and operations. Evaluates the design, effectiveness and efficiency of information technology and security processes, procedures, and technical controls including solution/system implementations, identify and address gaps in cybersecurity risk management. Provides detailed risk assessments, risk explanations and mitigation recommendations. Designs and develops new business processes, procedures and policies in response to risk assessments, and ensures compliance with governance and regulatory requirements. Tasks may also include breach mitigation and analysis and forensic services.

**Minimum Experience:** Minimum 3 years of experience participating in projects as a team member, with specific experience in one or more key project areas.
one or more key project areas.

**Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**Risk Assessment and Mitigation Associate III**

**Functional Responsibility:** Assists in evaluating cybersecurity risks, testing controls designed to mitigate risk, and communicating issues and findings to management. Performs audits and assessments focused on evaluating the effectiveness of security governance, tools and operations. Evaluates the design, effectiveness and efficiency of information technology and security processes, procedures, and technical controls including solution/system implementations, identify and address gaps in cybersecurity risk management. Provides detailed risk assessments, risk explanations and mitigation recommendations. Designs and develops new business processes, procedures and policies in response to risk assessments, and ensures compliance with governance and regulatory requirements. Tasks may also include breach mitigation and analysis and forensic services.

**Minimum Experience:** Minimum 5 years of experience participating in projects as a team member, with specific experience in one or more key project areas.

**Minimum Education:** Bachelor's degree in relevant IT or business discipline.

**Risk IT Technical Writer**

**Functional Responsibility:** Develops, writes, and edits functional risk descriptions, system specifications, user's manuals, special reports, or any other deliverables and documents related to risk. Observes production and experimental activities to determine operating procedure and detail, interviews production and engineering personnel, researches other material to become familiar with product technologies and production methods, reviews manufacturer's and trade catalogs, drawings and other data relative to operation, maintenance, and service of equipment. Organizes material and completes writing assignment according to set standards regarding order, clarity, conciseness, style, and terminology and recommends revisions or changes in scope, format, content, and methods of reproduction and binding. Maintains records and files of work and revisions, selects photographs, drawings, sketches, diagrams, and charts to illustrate material, edits, standardizes, or changes material prepared by other writers or technical personnel. Reports orally and in writing to the Program Manager, Project Manager, contractor management, and government representatives.

**Required Experience:** Up to 3 years of technical experience in collecting and organizing information required for preparation of user's manuals, training materials, installation guides, proposals, reports, and other systems/applications documentation.

**Required Education:** Bachelor's degree in relevant IT or business discipline. Experience may be substituted at the rate of two years of directly related experience for each year of education.

**Service Contract Labor Standards:** The Service Contract Labor Standards (SCLS), formerly known as the Service Contract Act (SCA), is applicable to this contract as it applies to the entire Multiple Award Schedule (MAS) and all services provided. While no specific labor categories have been identified as being subject to SCLS/SCA due to exemptions for professional employees (FAR 22.1101, 22.1102 and 29 CFR 541.300), this contract still maintains the provisions and protections for SCLS/SCA eligible labor categories. If and / or when the contractor adds SCLS/SCA labor categories to the contract through the modification process, the contractor must inform the Contracting Officer and establish a SCLS/SCA matrix identifying the GSA labor category titles, the occupational code, SCLS/SCA labor category titles and the applicable WD number. Failure to do so may result in cancellation of the contract.