Tangent Technologies, LLC
7208 CAPITOL VIEW DR
MCLEAN, VA 22101-2618
Phone: 703-598-8086
Fax: 703-995-0736
http://www.tangentt.com/

CONTRACT NUMBER:  GS-35F-656GA

PERIOD COVERED BY CONTRACT:
September 7, 2017 through September 6, 2027

BUSINESS SIZE:
Service Disabled Veteran Owned Small Business (SDVOSB)
Women Owned Small Business (WOSB)

Price List current through modification PS-0012 effective June 24, 2022

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

1a. AUTHORIZED SPECIAL ITEM NUMBERS (SINs):

<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>Information Technology Professional Services</td>
</tr>
<tr>
<td>OLM</td>
<td>Order-Level Materials (OLM)</td>
</tr>
</tbody>
</table>

*Includes the following subcategories: High Value Asset (HVA) Assessments, Risk and Vulnerability Assessment (RVA), Penetration Testing, Incident Response, and Cyber Hunt

1b. Lowest Priced Model Number and Price for each SIN: See Price List

1c. SERVICES OFFERED: See Price List

2. MAXIMUM ORDER PER SIN:

<table>
<thead>
<tr>
<th>SIN</th>
<th>MAXIMUM ORDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>$500,000 per SIN/Order</td>
</tr>
<tr>
<td>54151S</td>
<td>$500,000 per SIN/Order</td>
</tr>
<tr>
<td>OLM</td>
<td>$250,000 per SIN/Order</td>
</tr>
</tbody>
</table>

3. MINIMUM ORDER LIMITATION: $100

4. GEOGRAPHIC COVERAGE (DELIVERY AREA): Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

5. POINT OF PRODUCTION: United States

6. BASIC DISCOUNT: Prices listed are net, discounts have been deducted and the industrial funding fee has been added.

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. FOREIGN ITEMS: None

10a. TIME OF DELIVERY: As negotiated with the Ordering Activity

10b. EXPEDITED DELIVERY: Contact Contractor

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

10d. URGENT REQUIREMENTS: Contact Contractor

11. F.O.B. POINT: Destination
12a. ORDERING ADDRESS: Tangent Technologies, LLC
7208 CAPITOL VIEW DR
MCLEAN, VA 22101-2618

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: Same as Ordering Address

14. WARRANTY PROVISION: Standard Commercial Warranty

15. EXPORT PACKING CHARGES: Not Applicable

16. TERMS AND CONDITIONS OF RENTAL: Not Applicable

17. TERMS AND CONDITIONS OF INSTALLATION: Not Applicable

18a. TERMS AND CONDITIONS OF REPAIR PARTS: Not Applicable

18b. TERMS AND CONDITIONS FOR ANY OTHER SERVICES: Not Applicable

19. LIST OF SERVICE AND DISTRIBUTION POINTS: Not Applicable

20. LIST OF PARTICIPATING DEALERS: Not Applicable

21. PREVENTIVE MAINTENANCE: Not Applicable

22a. SPECIAL ATTRIBUTES: Not Applicable

22b. SECTION 508 COMPLIANCE INFORMATION: Not Applicable

23. UNIQUE ENTITY IDENTIFIER (UEI) NUMBER: VGRPWZJMHN64

24. CONTRACTOR HAS 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)
- NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

1. SCOPE
a. The labor categories, prices, terms and conditions stated under Special Item Number 54151HACS 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, and may be quoted along with services to provide a total solution.

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

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

e. 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.

b) To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.
9. **INVOICES**

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

10. **RESUMES**

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

11. **APPROVAL OF SUBCONTRACTS**

The ordering activity may require that the Contractor receive, from the ordering activity'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**

Please refer to the labor category descriptions and pricing incorporated into this GSA Pricelist.
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S)

1. **SCOPE**
   a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Professional 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.

   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.
   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


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 (Dec
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 Professional Services.

9. INDEPENDENT CONTRACTOR

All IT Professional 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 Professional 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)

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.

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

Please refer to the labor category descriptions and pricing incorporated into this GSA Pricelist.
LABOR CATEGORY DESCRIPTIONS

Category/Title: Subject Matter Expert Senior
Education: Bachelors Degree
Years of Experience: 10+ years
Responsibilities: Subject Matter Expertise Senior in Information Technology, Information Security, or any other type of technology related to service area being supported. Must be capable of identifying issues and developing recommended courses of action based on experience and industry best practices. The SME Senior is a recognized expert in a given area of technology. In addition to providing significant technology support, the SME Senior is capable of directing teams engaged in large scale, complex projects.

Category/Title: Information Systems Security Officer (ISSO) Level 1
Education: Bachelors Degree
Years of Experience: 2 years
Responsibilities: Specialized in the analysis or application of system security practices within an organization/agency. Designs, develops and writes certification and accreditation (C&A) documentation packages included in the process of helping an organization/agency obtain an authority to operate (ATO) on its systems and/or environment. Follows National Institute of Standards and Technology (NIST) and/or Department of Defense IA Certification and Accreditation Process standards in performance of job functions. Performs Information Systems Security Officer (ISSO) services for an organization/agency. Familiar with commonly used concepts, practices, and procedures within a particular field. Works under general supervision. Relies on experience to plan and accomplish goals.

Category/Title: Cyber Security Analyst II
Education: Bachelors Degree
Years of Experience: 3+ years
Responsibilities: Assessing security controls in accordance with industry recognized security standards, frameworks, laws and policies. Conducting security control assessment interviews with information system security stakeholders, collect and review artifacts and evidence for compliance with security controls, and document assessment results in a security assessment report. Ensure the quality assurance of security assessment results in system security packages. Ensuring non-compliance of security control is remediated through the use of the Plan of Action & Milestones (POA&M) process. Review evidence of remediation of findings, providing guidance and expertise where necessary. Recommend closure of POA&Ms based on documented evidence and artifacts.

Category/Title: Cyber Security Analyst I
Education: High School Diploma
Years of Experience: 0+ years
Responsibilities: The Cyber Security Analyst I is responsible for maintaining appropriate levels of information security throughout the organization; ensure effective use of security measures and technical solutions to protect data. This person will develop and implement practical and achievable policies and practices for the protection of business information regardless of media or delivery mechanism. Will also ensure the company is compliant with regulatory requirements and security best practices as defined by industry experts and internal audit. This position is responsible for handling highly sensitive and confidential information.
**Category/Title: Subject Matter Expert**

**Education:** Bachelor’s Degree  
**Years of Experience:** 7 years  
**Responsibilities:** Applies an enterprise-wide set of disciplines for the planning, analysis, design and construction of information systems on an enterprise-wide basis or across a major sector of the enterprise. Develops analytical and computational techniques and methodologies for problem solutions. Performs enterprise wide strategic systems planning, business information planning, business and analysis. Performs process and data modeling in support of the planning and analysis efforts using both manual and automated tools. Applies reverse engineering and re-engineering disciplines to develop migration strategic and planning documents. Provides technical guidance in software engineering techniques and automated support tools.

**Category/Title: Subject Matter Expert Junior**

**Education:** Bachelor’s Degree  
**Years of Experience:** 5 years  
**Responsibilities:** Provides high-level subject matter expertise for work described in the task. Provides advanced technical knowledge and analysis of highly specialized applications and operational environment, high-level functional systems analysis, design, integration, documentation, training, and implementation advice on complex problems, which require doctorate level knowledge of the subject matter for effective implementation. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, training, and presentation phases. Applies principles, methods, and knowledge of specific functional areas of expertise to specific task order requirements.

**Category/Title: Principal Information Technology Consultant**

**Education:** Bachelor’s degree  
**Years of Experience:** 7 years  
**Responsibilities:** Specialized experience includes demonstrated experience in IT areas specifically relevant to task orders. Must have served as a team leader in directly related applied or analytical areas. Works with senior management level personnel from Government Agencies and Departments.

**Category/Title: Senior Information Technology Consultant**

**Education:** Bachelor’s degree  
**Years of Experience:** 5 years  
**Responsibilities:** Provide technical knowledge in their area of expertise, work individually and on teams to support the completion of project specific tasks within established milestones and budgetary constraints and interface with the client on a daily basis. In addition, senior consultants apply their specific expertise to the practical issues they identify or those presented to the client. They also assist in formulating solutions, preparation of reports, studies and documentation, and support presentations and client meetings.

**Category/Title: Information Technology Consultant**

**Education:** Bachelor’s Degree  
**Years of Experience:** 3 years  
**Responsibilities:** Interface with the client on a daily basis, assist in identifying problems, perform technical analysis and develop solutions, support the completion of project specific tasks within set milestones and budgetary constraints, and support presentations and client meetings.
Category/Title: Program Manager
Education: Bachelor’s Degree
Years of Experience: 10 years. Background demonstrates progressive experience in leading project, demonstrated ability to provide guidance and direction for specific projects or sub-tasks and a capability to manage multi-task projects of high complexity for clients.
Responsibilities: Program Managers have taken on increasing responsibility in the design, implementation, and management of projects. They interface with the clients on project specific issues, direct the completion of projects within established milestones and budgetary constraints, coordinate project specific entities, and review work products for completeness and adherence to applicable regulations and customer requirements.

Category/Title: Project Manager/Task Order Manager II
Education: Bachelor’s Degree
Years of Experience: 6 years
Responsibilities: Accountable for all aspects of project or task order performance. Provides overall direction to all project level activity and personnel interfaces with client personnel. Ensures schedules are met. Monitors performance indicators such as cost, timing and manpower loading. Keeps management informed of project status and deviations. Demonstrates strong oral and written communication skills. Typically reports to the Program Manager or other senior management.

Category/Title: Project Manager/Task Order Manager I
Education: Bachelor’s Degree
Years of Experience: 4 years
Responsibilities: Accountable for all aspects of project or task order performance. Provides overall direction to all project level activity and personnel interfaces with client personnel. Ensures schedules are met. Monitors performance indicators such as cost, timing and manpower loading. Keeps management informed of project status and deviations. Demonstrates strong oral and written communication skills. Typically reports to the Program Manager or other senior management.

Category/Title: Project Coordinator I
Education: Bachelor’s Degree
Years of Experience: 2 years
Responsibilities: The Project Coordinator is responsible for providing administrative and functional support for program operations. These tasks include but are not limited to interacting with DHS personnel, and subcontractors for the collection of all project deliverables. In addition, the Project Coordinator will maintain a project database that contains all deliverables tracking information and will also schedule and track jobs. Additionally, the individual will provide support for the functioning of all interfaces used by/within the organization, through technical/application troubleshooting and quality assurance activities, consistent with applicable regulations and established protocols.

Category/Title: Senior Business Analyst
Education: Bachelor’s Degree
Years of Experience: 10 years
Responsibilities: Provides up-to-date expertise in Information Systems and apply this to the development, execution and improvement of action plans by providing advice and guidance to others in the application of information and best practices. Possesses the ability to stay current with customer needs and strategies; utilizing formal and informal written communication methods (example: emails, newsletters, PowerPoint presentations, executive updates, and task lists) to communicate updates and findings; and facilitate project meetings and presentations to all types of diverse audiences (example: senior management, Customers, technical staff) Work with a Program or Project Manager to lead or participate in multiple projects by completing and updating project documentation; managing project scope; adjusting schedules when necessary; determining daily priorities; ensuring efficient and on-time delivery of project tasks and milestones; following proper escalation paths; and managing customer and supplier relationships.

Category/Title: Business Analyst
Education: Bachelor’s Degree
Years of Experience: 4 years
Responsibilities: Provides up-to-date expertise in Information Systems and apply this to the development, execution and improvement of action plans by providing advice and guidance to others in the application of information and best practices. Possesses the ability to stay current with customer needs and strategies; utilizing formal and informal written communication methods (example: emails, newsletters, PowerPoint presentations, executive updates, and task lists) to communicate updates and findings; and facilitate project meetings and presentations to all types of diverse audiences (example: senior management, Customers, technical staff) Work with a Program or Project Manager to participate in multiple projects by completing and updating project documentation; managing project scope; adjusting schedules when necessary; determining daily priorities; ensuring efficient and on-time delivery of project tasks and milestones; following proper escalation paths; and managing customer and supplier relationships.

Category/Title: Information Systems Security Officer (ISSO) Principal
Education: Bachelor’s Degree
Years of Experience: 10 years
Responsibilities: Specialized in the analysis and application of system security practices within an organization/agency. Designs, develops and writes continuous authorization (C&A) documentation packages included in the process of helping an organization/agency obtain an authority to operate (ATO) on its IT systems. Follows National Institute of Standards and Technology (NIST), FISMA and/or Department of Defense IA Certification and Accreditation Process standards in performance of job functions. Performs Information Systems Security Officer (ISSO), business continuity planning, and IT disaster recovery planning and security risk assessment services for an organization/agency. Demonstrates expertise in common concepts, practices, and procedures within Information Security and may provide consultation on complex IT projects and is considered to be an expert in the field. Relies on extensive experience and judgment to plan and accomplish goals. Demonstrates the ability to lead other ISSOs as a technical expert.

Category/Title: Information Systems Security Officer (ISSO) Level 3
Education: Bachelor’s Degree
Years of Experience: 6 years
Responsibilities: Specialized in the analysis and application of system security practices within an organization/agency. Designs, develops and writes continuous authorization (C&A) documentation packages included in the process of helping an organization/agency obtain an authority to operate (ATO) on its IT systems. Follows National Institute of Standards and Technology (NIST), FISMA and/or Department of Defense IA Certification and Accreditation Process standards in performance of job functions.
functions. Performs Information Systems Security Officer (ISSO), business continuity planning, and IT disaster recovery planning and security risk assessment services for an organization/agency. Demonstrates expertise in common concepts, practices, and procedures within Information Security and may provide consultation on complex IT projects and is considered to be an expert in the field. Relies on extensive experience and judgment to plan and accomplish goals. Demonstrates the ability to lead other ISSOs as a technical expert.

**Category/Title: Information Systems Security Officer (ISSO) Level 2**

**Education:** Bachelor’s Degree  
**Years of Experience:** 4 years  
**Responsibilities:** Specialized in the analysis and application of system security practices within an organization/agency. Designs, develops and writes continuous authorization (C&A) documentation packages included in the process of helping an organization/agency obtain an authority to operate (ATO) on its IT systems. Follows National Institute of Standards and Technology (NIST), FISMA and/or Department of Defense IA Certification and Accreditation Process standards in performance of job functions. Performs Information Systems Security Officer (ISSO), business continuity planning, and IT disaster recovery planning and security risk assessment services for an organization/agency. Demonstrates expertise in common concepts, practices, and procedures within Information Security and may provide consultation on complex IT projects and is considered to be proficient in the field.

**Category/Title: IT Security Specialist IV**

**Education:** Bachelor’s Degree  
**Years of Experience:** 7 years  
**Responsibilities:** Performs and evaluates information risk assessments. Designs, develops, and implements information security and disaster recovery programs in accordance with organizational information security standards. Ensures that all information systems are functional and secure. The Level IV IT Security Specialist is a recognized expert in the area of information technology security. In addition to providing information technology assessments and analysis, the Level IV IT Security Specialist is capable of directing teams engaged in large scale, complex projects.

**Category/Title: IT Security Specialist III**

**Education:** Bachelor’s Degree  
**Years of Experience:** 3 years  
**Responsibilities:** Responsible for providing customer support in solving all phases of complex information security related technical problems. Reviews and recommends information security solutions to customer problems based on an understanding of products/systems test results. Conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, software engineering, program design, configuration management, integration, and testing of information security products and techniques. Solutions are based on a firm understanding of government/industry policy, practices, procedures, and customer requirements. Particular attention placed on Guard, Firewall, Intrusion Detection Systems, Security Event and Information Management Systems (SIEM), and emerging security technologies and future trends in support of information system and network security. Insures that solutions are fully compatible with or engineered into the customer’s network design. Provides work direction and guidance to other personnel, ensures accuracy of the work of other personnel, operates under deadlines, and is able to work on multiple tasks.

**Category/Title: Cyber Security Analyst IV**

**Education:** Bachelor’s Degree  
**Years of Experience:** 10 years
**Responsibilities:** Monitors IT assets using logs from firewalls, servers, workstations, and other input points to assess overall security risks and possible exposure. Design and implement standards, practices, metrics, and reporting. Direct efforts to prioritize and mitigate department level audit findings or inquiries and emerging environmental threats.

**Category/Title:** Cyber Security Analyst III  
**Education:** Bachelor’s Degree  
**Years of Experience:** 6 years  
**Responsibilities:** Monitors IT assets using logs from firewalls, servers, workstations, and other input points to assess overall security risks and possible exposure. Design and implement standards, practices, metrics, and reporting. Direct efforts to prioritize and mitigate department level audit findings or inquiries and emerging environmental threats.

**Category/Title:** Penetration Tester II  
**Education:** Bachelor’s Degree  
**Years of Experience:** 5 years  
**Responsibilities:** The Penetration Tester II identifies, investigates, analyzes, and remediates information security events to ensure enterprise integrity against technical and physical risks. Conducts quality management reviews to evaluate the effectiveness of security controls. This position reports on the controls effectiveness for mitigating exposure to identified risks. Communicates security issues and control gaps through security governance processes. This position implements and integrates risk management procedures across the enterprise. Participates in the development and maintenance of business continuity planning, data, systems, and network security for systems & controls related to their job duties.

**Category/Title:** Penetration Tester I  
**Education:** Bachelor’s Degree  
**Years of Experience:** 2 years  
**Responsibilities:** Perform Security Penetration Assessments exploiting and compromising defined targets in a global enterprise environment ranging from web applications to handheld systems. Identify and exploit vulnerabilities in web and mobile applications, OS, hardware, databases, wired and wireless networks, etc. Document technical and logical security findings identified during the security assessments and providing security recommendations for enterprise executives, developers, web/system and database administrators.

**Category/Title:** System Administrator Senior  
**Education:** Bachelor’s Degree  
**Years of Experience:** 7 years  
**Responsibilities:** Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).

**Category/Title:** Network Operations Specialist Intermediate  
**Education:** Bachelor’s Degree  
**Years of Experience:** 4 years  
**Responsibilities:** Plans, implements, and operates network services/systems, to include hardware and virtual environments.
Category/Title: Cyber Defense Infrastructure Support Specialist Intermediate
Education: Bachelor’s Degree
Years of Experience: 4
Responsibilities: Tests, implements, deploys, maintains, and administers the dedicated cyber defense hardware and software. Performs system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration. Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).

* Years of experience can be substituted for education requirements at a rate of 2 years experience for 1 year of education (i.e. eight years of experience can be substituted for a four-year bachelor's degree.)
<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category Description</th>
<th>9/7/2021 – 9/6/2022</th>
<th>9/7/2022 – 9/6/2023</th>
<th>9/7/2023 – 9/6/2024</th>
<th>9/7/2024 – 9/6/2025</th>
<th>9/7/2025 – 9/6/2026</th>
<th>9/7/2026 – 9/6/2027</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Subject Matter Expert Senior</td>
<td>$167.35</td>
<td>$170.70</td>
<td>$174.12</td>
<td>$177.60</td>
<td>$181.15</td>
<td>$184.77</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Information Systems Security Officer (ISSO) Level 1</td>
<td>$74.50</td>
<td>$75.99</td>
<td>$77.51</td>
<td>$79.06</td>
<td>$80.64</td>
<td>$82.25</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Analyst II</td>
<td>$89.82</td>
<td>$91.62</td>
<td>$93.45</td>
<td>$95.32</td>
<td>$97.22</td>
<td>$99.17</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Analyst I</td>
<td>$44.97</td>
<td>$45.87</td>
<td>$46.79</td>
<td>$47.72</td>
<td>$48.68</td>
<td>$49.65</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert</td>
<td>$140.10</td>
<td>$142.90</td>
<td>$145.76</td>
<td>$148.68</td>
<td>$151.65</td>
<td>$154.68</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert Junior</td>
<td>$108.97</td>
<td>$111.15</td>
<td>$113.37</td>
<td>$115.64</td>
<td>$117.95</td>
<td>$120.31</td>
</tr>
<tr>
<td>54151S</td>
<td>Principal Information Technology Consultant</td>
<td>$181.61</td>
<td>$185.24</td>
<td>$188.95</td>
<td>$192.73</td>
<td>$196.58</td>
<td>$200.50</td>
</tr>
<tr>
<td>54151S</td>
<td>Senior Information Technology Consultant</td>
<td>$155.67</td>
<td>$158.78</td>
<td>$161.96</td>
<td>$165.19</td>
<td>$168.50</td>
<td>$171.87</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Technology Consultant</td>
<td>$140.10</td>
<td>$142.90</td>
<td>$145.76</td>
<td>$148.68</td>
<td>$151.65</td>
<td>$154.68</td>
</tr>
<tr>
<td>54151S</td>
<td>Program Manager</td>
<td>$166.04</td>
<td>$169.37</td>
<td>$172.76</td>
<td>$176.21</td>
<td>$179.73</td>
<td>$183.33</td>
</tr>
<tr>
<td>54151S</td>
<td>Project Manager/Task Order Manager II</td>
<td>$134.91</td>
<td>$137.61</td>
<td>$140.36</td>
<td>$143.17</td>
<td>$146.03</td>
<td>$148.95</td>
</tr>
<tr>
<td>54151S</td>
<td>Project Manager/Task Order Manager I</td>
<td>$122.46</td>
<td>$124.91</td>
<td>$127.41</td>
<td>$129.95</td>
<td>$132.55</td>
<td>$135.20</td>
</tr>
<tr>
<td>54151S</td>
<td>Project Coordinator I</td>
<td>$93.40</td>
<td>$95.27</td>
<td>$97.17</td>
<td>$99.12</td>
<td>$101.10</td>
<td>$103.12</td>
</tr>
<tr>
<td>54151S</td>
<td>Senior Business Analyst</td>
<td>$108.97</td>
<td>$111.15</td>
<td>$113.37</td>
<td>$115.64</td>
<td>$117.95</td>
<td>$120.31</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Analyst</td>
<td>$89.25</td>
<td>$91.03</td>
<td>$92.86</td>
<td>$94.71</td>
<td>$96.61</td>
<td>$98.54</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Information Systems Security Officer (ISSO) Principle</td>
<td>$166.04</td>
<td>$169.37</td>
<td>$172.75</td>
<td>$176.21</td>
<td>$179.73</td>
<td>$183.33</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Information Systems Security Officer (ISSO) Level 3</td>
<td>$150.48</td>
<td>$153.49</td>
<td>$156.56</td>
<td>$159.69</td>
<td>$162.88</td>
<td>$166.14</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Information Systems Security Officer (ISSO) Level 2</td>
<td>$134.91</td>
<td>$137.61</td>
<td>$140.36</td>
<td>$143.17</td>
<td>$146.03</td>
<td>$148.95</td>
</tr>
<tr>
<td>54151HACS</td>
<td>IT Security Specialist IV</td>
<td>$129.72</td>
<td>$132.32</td>
<td>$134.96</td>
<td>$137.66</td>
<td>$140.42</td>
<td>$143.22</td>
</tr>
<tr>
<td>54151HACS</td>
<td>IT Security Specialist III</td>
<td>$98.59</td>
<td>$100.56</td>
<td>$102.57</td>
<td>$104.62</td>
<td>$106.72</td>
<td>$108.85</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Analyst IV</td>
<td>$124.53</td>
<td>$127.02</td>
<td>$129.56</td>
<td>$132.16</td>
<td>$134.80</td>
<td>$137.50</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Analyst III</td>
<td>$114.16</td>
<td>$116.44</td>
<td>$118.77</td>
<td>$121.14</td>
<td>$123.57</td>
<td>$126.04</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester II</td>
<td>$181.61</td>
<td>$185.24</td>
<td>$188.95</td>
<td>$192.73</td>
<td>$196.58</td>
<td>$200.51</td>
</tr>
<tr>
<td>SIN</td>
<td>Labor Category Description</td>
<td>9/7/2021 – 9/6/2022</td>
<td>9/7/2022 – 9/6/2023</td>
<td>9/7/2023 – 9/6/2024</td>
<td>9/7/2024 – 9/6/2025</td>
<td>9/7/2025 – 9/6/2026</td>
<td>9/7/2026 – 9/6/2027</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester I</td>
<td>$160.86</td>
<td>$164.07</td>
<td>$167.36</td>
<td>$170.70</td>
<td>$174.12</td>
<td>$177.60</td>
</tr>
<tr>
<td>54151HACS</td>
<td>System Administrator Senior</td>
<td>$111.10</td>
<td>$113.32</td>
<td>$115.59</td>
<td>$117.90</td>
<td>$120.26</td>
<td>$122.66</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Network Operations Specialist Intermediate</td>
<td>$111.77</td>
<td>$114.00</td>
<td>$116.28</td>
<td>$118.61</td>
<td>$120.98</td>
<td>$123.40</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Defense Infrastructure Support Specialist</td>
<td>$157.02</td>
<td>$160.16</td>
<td>$163.37</td>
<td>$166.63</td>
<td>$169.97</td>
<td>$173.37</td>
</tr>
</tbody>
</table>