



**GENERAL SERVICES ADMINISTRATION
FEDERAL ACQUISITION SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE CATALOG/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 is available through *GSA Advantage!*, a menu-driven database system. The website for *GSA Advantage!* is <https://www.gsaadvantage.gov>.

SCHEDULE TITLE: MAS – Multiple Award Schedule

CONTRACT NUMBER: 47QTCA19D004D

CONTRACT PERIOD: January 15, 2019 – January 14, 2024

For more information on ordering from Federal Supply Schedules, click on the GSA Schedules link at www.gsa.gov.

CONTRACTOR: Triple Point Security Incorporated
161 Fort Evans Road NE, Suite 325
Leesburg, VA 20176

CONTRACTOR’S ADMINISTRATION SOURCE: Carlo Espiritu
161 Fort Evans Road NE, Suite 325
Leesburg, VA 20176
Phone: 703-216-8650
Email: cespiritu@triplepointsecurity.com

BUSINESS SIZE: 8(a), Minority Owned, and HUBZone Certified Small Business

CUSTOMER INFORMATION:

1a. TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs)

SIN	DESCRIPTION
518210C	Cloud and Cloud-Related IT Professional Services
54151S	Information Technology Professional Services
54151HEAL	Health Information Technology Services

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

<u>SIN</u>	<u>Part #</u>	<u>Price</u>
518210C	CloudCheckr-7A	1.65% of the Cloud Spend
54151S	IT Security Analyst I	\$83.39

54151HEAL Health IT Security Analyst I \$83.39

- 1c. **HOURLY RATES:** See page 16 for Hourly Rates
2. **MAXIMUM ORDER*:** \$500,000
3. **MINIMUM ORDER:** \$100
4. **GEOGRAPHIC COVERAGE:** Domestic, 50 states, Washington, DC, Puerto Rico
5. **POINT(S) OF PRODUCTION:** N/A
6. **Discount from list prices or statement of net price:** All Prices offered are net.
7. **QUANTITY DISCOUNT(S):** 2.0% for any single purchase order over \$250,000
8. **PROMPT PAYMENT TERMS:** 1% 20 Days, Net 30
- 9.a **Government Purchase Cards must be accepted at or below the micro-purchase threshold.**
- 9.b **Government Purchase Cards are accepted above the micro-purchase threshold.**
10. **FOREIGN ITEMS:** None
- 11a. **TIME OF DELIVERY:** 30 Business Days
- 11b. **EXPEDITED DELIVERY:** Contact Contractor
- 11c. **OVERNIGHT AND 2-DAY DELIVERY:** Contact Contractor
- 11d. **URGENT REQUIRMENTS:** Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.
12. **FOB POINT:** Destination
- 13a. **ORDERING ADDRESS:** 161 Fort Evans Road NE, Suite 325, Leesburg, VA 20176
- 13b. **ORDERING PROCEDURES:** For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in FAR 8.405-3
14. **PAYMENT ADDRESS:** 161 Fort Evans Road NE, Suite 325, Leesburg, VA 20176
15. **WARRANTY PROVISION:** Standard Commercial Warranty

16. **EXPORT PACKING CHARGES:** N/A
17. **TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE:** Accepted above the micro-purchase level
18. **TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR (IF APPLICABLE):** N/A
19. **TERMS AND CONDITIONS OF INSTALLATION (IF APPLICABLE):** N/A
20. **TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE):**
N/A
- 20a. **TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE):**
N/A
21. **LIST OF SERVICE AND DISTRIBUTION POINTS (IF APPLICABLE):** N/A
22. **LIST OF PARTICIPATING DEALERS (IF APPLICABLE):** N/A
23. **PREVENTIVE MAINTENANCE (IF APPLICABLE):** N/A
- 24a. **SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants):** N/A
- 24b. **Section 508 Compliance for EIT:** as applicable
25. **DUNS NUMBER:** 967945531
26. **NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE:** Registration is valid

SIN 54151S Labor Category Descriptions

The labor categories below are further subdivided by knowledge/skill level. Definitions of these knowledge/skill levels are as follows:

Level I – Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with oversight from engagement program/project management or team leads. Contributes to deliverables and performance metrics.

Level II – Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads technology assignments. Evaluates performance results and recommends major changes affecting short-term engagement growth and success. Functions as a technical expert across multiple project assignments. Supports engagement management, business development, and staffing. Mentors team members.

Level III – Provides technical and management leadership on major tasks or technology assignments. Establishes goals and plans that meet long-term engagement objectives. Possesses domain and expert technical knowledge. Directly supports and interfaces with the client, helps manage engagement finances, develops service delivery methodologies, and support engagement staffing (recruiting, hiring, and retaining) to ensure that technical requirements are met. Interactions involve business development, client negotiations, and interfacing with client senior management. Decision-making and domain knowledge may have a critical impact on overall engagement implementation. Mentors team members.

IT CLOUD SECURITY – SUBJECT MATTER EXPERT

Functional Responsibilities:

- Provide technical subject matter expertise on cloud computing security service management practices, cloud service design and implementation, and process development and improvement
- Advise and implement innovative cloud security tools, tenant management practices, and cloud service provider (CSP) processes and procedures
- Develop proof-of-concept (PoC) solutions and provision CSP-based development, test, and production environments based on client requirements
- Integrate several CSP services and develop potential solutions to complex challenges
- Establish service and workload operations and maintenance (O&M) framework
- Automate technical and administrative processes and procedures
- Stay abreast of cloud computing, cloud computing security, and IT security industry standards, tools/technologies, and practices
- Manage tenant and operations activities per security and compliance requirements
- Analyze tactical to strategic challenges and identify opportunities for improvement
- Support complex system development initiatives
- Educate clients on industry and CSP products and practices

Minimum Years of Experience:

Level I – 3 to 5
Level II – 6 to 9
Level III – 10 to 12+

Minimum Education/degree requirements:

Level I – Bachelor’s degree
Level II – Master’s degree (or bachelor’s degree +2 years of relevant experience)
Level III – Master’s degree (or bachelor’s degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Cloud service provider (CSP) or vendor-agnostic cloud computing security training and industry-recognized IT security certifications
Level II – Industry-recognized CSP or vendor-agnostic cloud computing security certifications
Level III – Industry-recognized CSP or vendor-agnostic cloud computing security advanced certifications

IT CLOUD SECURITY ENGINEER

Functional Responsibilities:

- Design and implement cloud services solutions utilizing cloud service provider (CSP) services and tools/technologies based on client requirements
- Operate security tools and technologies to maintain the security posture of a cloud-based system or application
- Integrate innovative IT security solutions with cloud-based environments for vulnerability management, threat management, configuration management, and tenant monitoring
- Support system and application migrations from on-premise to cloud-based environments
- Analyze anomalous events and responds to potential threats to the environment
- Support proof-of-concept (PoC) system and application implementations based on business and security requirements
- Configure CSP tenants based on industry practices and business requirements
- Develop processes and procedures to establish and maintain the security of a cloud-based environment
- Apply IT security concepts and principles to CSP environments
- Support implementation and assessment security and compliance requirements

Minimum Years of Experience:

Level I – 0 to 3
Level II – 4 to 6
Level III – 7 to 9+

Minimum Education/degree requirements:

Level I – Associate’s degree in relevant field of study

Level II – Bachelor’s degree

Level III – Master’s degree (or bachelor’s degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Cloud service provider (CSP) or vendor-agnostic cloud computing security training and industry-recognized IT security certifications

Level II – Industry-recognized CSP or vendor-agnostic cloud computing security certifications

Level III – Industry-recognized CSP or vendor-agnostic cloud computing security advanced certifications

IT SECURITY ANALYST

Functional Responsibilities:

- Provide risk management services that support client infrastructure and system security
- Conduct security assessments and support system security authorization activities
- Evaluate systems and applications for compliance with various security and business requirements
- Participates with the client in the system and application design process to translate security and business requirements into technical implementations
- Configure and validate logical and physical security controls and tests security products and systems to detect security weaknesses
- Support clients in the areas of, but not limited to, IT security engineering, change management, configuration management, and contingency planning
- Participate in risk assessments to identify threats to client organizations’ environment
- Review and provide feedback on the adequacy of overall security design, architecture, and operations
- Conduct routine technical IT security tasks in support of operations and maintenance (O&M) activities such as vulnerability and patch management
- Support information security program metrics gathering and reporting
- Prepare for and conduct IT security readiness inspections, self-inspections, and audit activities
- Develop requisite assessment reports and present findings to clients

Minimum Years of Experience:

Level I – 0 to 3

Level II – 4 to 6

Level III – 7 to 9+

Minimum Education/degree requirements:

Level I – Associate’s degree in relevant field of study

Level II – Bachelor’s degree

Level III – Master’s degree (or bachelor’s degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Industry-recognized IT security or risk management training

Level II – Industry-recognized IT security or risk management certification

Level III – Industry-recognized IT security or risk management advanced certification

IT SECURITY ENGINEER

Functional Responsibilities:

- Help prevent IT security attacks through technical expertise and knowledge of networks, endpoints, databases, security tools/technologies, and understanding of threat landscape
- Assess security posture of a client’s environment and develop remediation/mitigation strategies to reduce risks while enhancing system and application security
- Provide technical input to information security policies, processes, and awareness training
- Develop standard operating procedures (SOPs) for security operations and security tools/technologies
- Respond to potential threats and conduct investigations to validate compromises
- Conduct security testing to identify weaknesses and to determine the depth and breadth the weaknesses introduce
- Perform system and application investigations that may include host-based and network-based data to determine activities as well as software and code analysis
- Support removal of malicious software and systems from clients’ environments and development of after actions and lessons-learned for prevention
- Implement and integrate standard and innovative IT security tools/technologies into client environments
- Operate, manage, and maintain hardware and software of IT security tools/technologies
- Review innovative technologies to help ensure that they conform to security policies, computer infrastructure, and business requirements

Minimum Years of Experience:

Level I – 0 to 3

Level II – 4 to 6

Level III – 7 to 9+

Minimum Education/degree requirements:

Level I – Associate’s degree in relevant field of study

Level II – Bachelor’s degree

Level III – Master’s degree (or bachelor’s degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Industry-recognized IT security vendor or vendor agnostic technical training

Level II – Industry-recognized IT security vendor or vendor agnostic technical certification

Level III – Industry-recognized IT security vendor or vendor agnostic advanced technical certification

IT SECURITY – SUBJECT MATTER EXPERT

Functional Responsibilities:

- Provide technical subject matter expertise on multiple IT security domains across client engagements and initiatives
- Support information technology (IT) governance and drive security architecture and business requirements during engagement delivery
- Recommend improvements in IT security implementation and design while leveraging the use of existing solutions and investments
- Responsible for managing the collaboration of key security and risk stakeholders to develop and review enterprise IT security and risk strategies
- Develop solutions and direct technical teams in the investigation and resolution of complex IT security issues and initiatives
- Assist in drafting and proposing organization-wide IT security and action plans based on security risk and analysis based on potential and emerging threats to the client's environment
- Recommend and implement IT security strategies and actions in support of client organizations' wider risk management program
- Develop short and long-term security initiatives that align with client executives' goals and business plans
- Manage technologies that support information systems and IT security requirements throughout the system development life cycle
- Support management of multiple project timelines, deliverables, and information requests of IT security initiatives and engagements
- Play a lead role in technology and security exercises related to architecture and participate in platform audits of both business process and technology

Minimum Years of Experience:

Level I – 3 to 5
Level II – 6 to 9
Level III – 10 to 12+

Minimum Education/degree requirements:

Level I – Bachelor's degree
Level II – Master's degree (or bachelor's degree +2 years of relevant experience)
Level III – Master's degree (or bachelor's degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Industry recognized IT security vendor or vendor-agnostic certification
Level II – Multiple industry recognized IT security vendor or vendor-agnostic certifications
Level III – Industry recognized IT security vendor or vendor-agnostic advanced certification

IT PROGRAM MANAGER

Functional Responsibilities:

- Organize, direct, and manage engagement operations involving multiple, complex and interrelated project tasks areas
- Monitor engagement performance through metrics and reporting
- Conduct quality control activities to monitor deliverable and service quality
- Manage teams of engagement support personnel at multiple locations
- Maintain and manage client relationships at senior levels of the client organization
- Meets with clients and engagement personnel to formulate and review task plans and deliverables
- Participate in the development of short and long-term security initiatives that align with client executives' goals and business plans
- Proactively identify potential issues and support the issue resolution process
- Determine engagement resource requirements and identify appropriate service delivery staff and tools/technologies
- Drive conformance with program task schedules and costs
- Lead periodic program reviews and status meetings and present content in a clear and concise manner

Minimum Years of Experience:

Level I – 3 to 5

Level II – 6 to 9

Level III – 10 to 12+

Minimum Education/degree requirements:

Level I – Bachelor's degree

Level II – Master's degree (or bachelor's degree +2 years of relevant experience)

Level III – Master's degree (or bachelor's degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Project Management Professional (PMP) training or Program Management Professional (PgMP) training

Level II – PMP certification and PgMP training

Level III – PMP and PgMP certification

SIN 54151HEAL Labor Category Descriptions

The labor categories below are further subdivided by knowledge/skill level. Definitions of these knowledge/skill levels are as follows:

Level I – Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with oversight from engagement program/project management or team leads. Contributes to deliverables and performance metrics.

Level II – Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads technology assignments. Evaluates performance results and recommends major changes affecting short-term engagement growth and success. Functions as a technical expert across multiple project assignments. Supports engagement management, business development, and staffing. Mentors team members.

Level III – Provides technical and management leadership on major tasks or technology assignments. Establishes goals and plans that meet long-term engagement objectives. Possesses domain and expert technical knowledge. Directly supports and interfaces with the client, helps manage engagement finances, develops service delivery methodologies, and support engagement staffing (recruiting, hiring, and retaining) to ensure that technical requirements are met. Interactions involve business development, client negotiations, and interfacing with client senior management. Decision-making and domain knowledge may have a critical impact on overall engagement implementation. Mentors team members.

HEALTH IT CLOUD SECURITY – SUBJECT MATTER EXPERT

Functional Responsibilities:

- Provide technical subject matter expertise on cloud computing security service management practices, cloud service design and implementation, and process development and improvement
- Advise and implement innovative cloud security tools, tenant management practices, and cloud service provider (CSP) processes and procedures
- Develop proof-of-concept (PoC) solutions and provision CSP-based development, test, and production environments based on client requirements
- Integrate several CSP services and develop potential solutions to complex challenges
- Establish service and workload operations and maintenance (O&M) framework
- Automate technical and administrative processes and procedures
- Stay abreast of cloud computing, cloud computing security, and IT security industry standards, tools/technologies, and practices
- Manage tenant and operations activities per security and compliance requirements
- Analyze tactical to strategic challenges and identify opportunities for improvement
- Support complex system development initiatives
- Educate clients on industry and CSP products and practices

Minimum Years of Experience:

Level I – 3 to 5
Level II – 6 to 9
Level III – 10 to 12+

Minimum Education/degree requirements:

Level I – Bachelor’s degree
Level II – Master’s degree (or bachelor’s degree +2 years of relevant experience)
Level III – Master’s degree (or bachelor’s degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Cloud service provider (CSP) or vendor-agnostic cloud computing security training and industry-recognized IT security certifications
Level II – Industry-recognized CSP or vendor-agnostic cloud computing security certifications
Level III – Industry-recognized CSP or vendor-agnostic cloud computing security advanced certifications

HEALTH IT CLOUD SECURITY ENGINEER

Functional Responsibilities:

- Design and implement cloud services solutions utilizing cloud service provider (CSP) services and tools/technologies based on client requirements
- Operate security tools and technologies to maintain the security posture of a cloud-based system or application
- Integrate innovative IT security solutions with cloud-based environments for vulnerability management, threat management, configuration management, and tenant monitoring
- Support system and application migrations from on-premise to cloud-based environments
- Analyze anomalous events and responds to potential threats to the environment
- Support proof-of-concept (PoC) system and application implementations based on business and security requirements
- Configure CSP tenants based on industry practices and business requirements
- Develop processes and procedures to establish and maintain the security of a cloud-based environment
- Apply IT security concepts and principles to CSP environments
- Support implementation and assessment security and compliance requirements

Minimum Years of Experience:

Level I – 0 to 3
Level II – 4 to 6
Level III – 7 to 9+

Minimum Education/degree requirements:

Level I – Associate’s degree in relevant field of study

Level II – Bachelor’s degree

Level III – Master’s degree (or bachelor’s degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Cloud service provider (CSP) or vendor-agnostic cloud computing security training and industry-recognized IT security certifications

Level II – Industry-recognized CSP or vendor-agnostic cloud computing security certifications

Level III – Industry-recognized CSP or vendor-agnostic cloud computing security advanced certifications

HEALTH IT SECURITY ANALYST

Functional Responsibilities:

- Provide risk management services that support client infrastructure and system security
- Conduct security assessments and support system security authorization activities
- Evaluate systems and applications for compliance with various security and business requirements
- Participates with the client in the system and application design process to translate security and business requirements into technical implementations
- Configure and validate logical and physical security controls and tests security products and systems to detect security weaknesses
- Support clients in the areas of, but not limited to, IT security engineering, change management, configuration management, and contingency planning
- Participate in risk assessments to identify threats to client organizations’ environment
- Review and provide feedback on the adequacy of overall security design, architecture, and operations
- Conduct routine technical IT security tasks in support of operations and maintenance (O&M) activities such as vulnerability and patch management
- Support information security program metrics gathering and reporting
- Prepare for and conduct IT security readiness inspections, self-inspections, and audit activities
- Develop requisite assessment reports and present findings to clients

Minimum Years of Experience:

Level I – 0 to 3

Level II – 4 to 6

Level III – 7 to 9+

Minimum Education/degree requirements:

Level I – Associate’s degree in relevant field of study

Level II – Bachelor’s degree

Level III – Master’s degree (or bachelor’s degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Industry-recognized IT security or risk management training

Level II – Industry-recognized IT security or risk management certification

Level III – Industry-recognized IT security or risk management advanced certification

HEALTH IT SECURITY ENGINEER

Functional Responsibilities:

- Help prevent IT security attacks through technical expertise and knowledge of networks, endpoints, databases, security tools/technologies, and understanding of threat landscape
- Assess security posture of a client’s environment and develop remediation/mitigation strategies to reduce risks while enhancing system and application security
- Provide technical input to information security policies, processes, and awareness training
- Develop standard operating procedures (SOPs) for security operations and security tools/technologies
- Respond to potential threats and conduct investigations to validate compromises
- Conduct security testing to identify weaknesses and to determine the depth and breadth the weaknesses introduce
- Perform system and application investigations that may include host-based and network-based data to determine activities as well as software and code analysis
- Support removal of malicious software and systems from clients’ environments and development of after actions and lessons-learned for prevention
- Implement and integrate standard and innovative IT security tools/technologies into client environments
- Operate, manage, and maintain hardware and software of IT security tools/technologies
- Review innovative technologies to help ensure that they conform to security policies, computer infrastructure, and business requirements

Minimum Years of Experience:

Level I – 0 to 3

Level II – 4 to 6

Level III – 7 to 9+

Minimum Education/degree requirements:

Level I – Associate’s degree in relevant field of study

Level II – Bachelor’s degree

Level III – Master’s degree (or bachelor’s degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Industry-recognized IT security vendor or vendor agnostic technical training

Level II – Industry-recognized IT security vendor or vendor agnostic technical certification

Level III – Industry-recognized IT security vendor or vendor agnostic advanced technical certification

HEALTH IT SECURITY – SUBJECT MATTER EXPERT

Functional Responsibilities:

- Provide technical subject matter expertise on multiple IT security domains across client engagements and initiatives
- Support information technology (IT) governance and drive security architecture and business requirements during engagement delivery
- Recommend improvements in IT security implementation and design while leveraging the use of existing solutions and investments
- Responsible for managing the collaboration of key security and risk stakeholders to develop and review enterprise IT security and risk strategies
- Develop solutions and direct technical teams in the investigation and resolution of complex IT security issues and initiatives
- Assist in drafting and proposing organization-wide IT security and action plans based on security risk and analysis based on potential and emerging threats to the client's environment
- Recommend and implement IT security strategies and actions in support of client organizations' wider risk management program
- Develop short and long-term security initiatives that align with client executives' goals and business plans
- Manage technologies that support information systems and IT security requirements throughout the system development life cycle
- Support management of multiple project timelines, deliverables, and information requests of IT security initiatives and engagements
- Play a lead role in technology and security exercises related to architecture and participate in platform audits of both business process and technology

Minimum Years of Experience:

Level I – 3 to 5

Level II – 6 to 9

Level III – 10 to 12+

Minimum Education/degree requirements:

Level I – Bachelor's degree

Level II – Master's degree (or bachelor's degree +2 years of relevant experience)

Level III – Master's degree (or bachelor's degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Industry recognized IT security vendor or vendor-agnostic certification

Level II – Multiple industry recognized IT security vendor or vendor-agnostic certifications

Level III – Industry recognized IT security vendor or vendor-agnostic advanced certification

HEALTH IT PROGRAM MANAGER

Functional Responsibilities:

- Organize, direct, and manage engagement operations involving multiple, complex and interrelated project tasks areas
- Monitor engagement performance through metrics and reporting
- Conduct quality control activities to monitor deliverable and service quality
- Manage teams of engagement support personnel at multiple locations
- Maintain and manage client relationships at senior levels of the client organization
- Meets with clients and engagement personnel to formulate and review task plans and deliverables
- Participate in the development of short and long-term security initiatives that align with client executives' goals and business plans
- Proactively identify potential issues and support the issue resolution process
- Determine engagement resource requirements and identify appropriate service delivery staff and tools/technologies
- Drive conformance with program task schedules and costs
- Lead periodic program reviews and status meetings and present content in a clear and concise manner

Minimum Years of Experience:

Level I – 3 to 5

Level II – 6 to 9

Level III – 10 to 12+

Minimum Education/degree requirements:

Level I – Bachelor's degree

Level II – Master's degree (or bachelor's degree +2 years of relevant experience)

Level III – Master's degree (or bachelor's degree +2 years of relevant experience)

Any applicable training or certification requirement (or comparable):

Level I – Project Management Professional (PMP) training or Program Management Professional (PgMP) training

Level II – PMP certification and PgMP training

Level III – PMP and PgMP certification

SIN 518210C GSA PRICE LIST

Manufacturer	Part #	Description	UOI	Price
CloudCheckr	CCRES-01	CloudCheckr ResTier1 \$0- \$600,000	Month	2.39% of the Cloud Spend
CloudCheckr	CCRES-02	CloudCheckr ResTier2 \$600,001 - \$1,200,000	Month	2.29% of the Cloud Spend
CloudCheckr	CCRES-03	CloudCheckr ResTier3 \$1,200,001 - \$4,800,000	Month	2.19% of the Cloud Spend
CloudCheckr	CCRES-04	CloudCheckr ResTier4 \$4,800,001 - \$9,600,000	Month	2.09% of the Cloud Spend
CloudCheckr	CCRES-05	CloudCheckr ResTier5 \$9,600,001 - \$18,000,000	Month	1.99% of the Cloud Spend
CloudCheckr	CCRES-06	CloudCheckr ResTier6 \$18,000,001 - \$24,000,000	Month	1.90% of the Cloud Spend
CloudCheckr	CCRES-07	CloudCheckr ResTier7 \$24,000,001+	Month	1.65% of the Cloud Spend

SIN 54151S GSA PRICE LIST

Labor Category	Year 1 Hourly Rate	Year 2 Hourly Rate	Year 3 Hourly Rate	Year 4 Hourly Rate	Year 5 Hourly Rate
IT Cloud Security SME II		\$163.25	\$167.33	\$171.51	\$175.80
IT Cloud Security Engineer III		\$153.36	\$157.20	\$161.13	\$165.15
IT Cloud Security Engineer I		\$122.69	\$125.76	\$128.90	\$132.12
IT Security Analyst I		\$85.47	\$87.61	\$89.80	\$92.05
IT Security Engineer III		\$192.61	\$197.43	\$202.36	\$207.42
IT Security Engineer II		\$153.62	\$157.46	\$161.40	\$165.43
IT Security Engineer I		\$117.48	\$120.41	\$123.42	\$126.51
IT Security SME III		\$184.04	\$188.64	\$193.35	\$198.19
IT Security SME II		\$165.04	\$169.16	\$173.39	\$177.73
IT Security SME I		\$149.28	\$153.02	\$156.84	\$160.76
IT Program Manager		\$137.89	\$141.34	\$144.87	\$148.50



SIN 54151HEAL GSA PRICE LIST

Labor Category	Year 1 Hourly Rate	Year 2 Hourly Rate	Year 3 Hourly Rate	Year 4 Hourly Rate	Year 5 Hourly Rate
Health IT Cloud Security SME II	\$159.27	\$163.25	\$167.33	\$171.51	\$175.80
Health IT Cloud Security Engineer III	\$149.62	\$153.36	\$157.20	\$161.13	\$165.15
Health IT Cloud Security Engineer I	\$119.70	\$122.69	\$125.76	\$128.90	\$132.12
Health IT Security Analyst I	\$83.39	\$85.47	\$87.61	\$89.80	\$92.05
Health IT Security Engineer III	\$187.92	\$192.61	\$197.43	\$202.36	\$207.42
Health IT Security Engineer II	\$149.87	\$153.62	\$157.46	\$161.40	\$165.43
Health IT Security Engineer I	\$114.61	\$117.48	\$120.41	\$123.42	\$126.51
Health IT Security SME III	\$179.55	\$184.04	\$188.64	\$193.35	\$198.19
Health IT Security SME II	\$161.01	\$165.04	\$169.16	\$173.39	\$177.73
Health IT Security SME I	\$145.64	\$149.28	\$153.02	\$156.84	\$160.76
Health IT Program Manager	\$134.53	\$137.89	\$141.34	\$144.87	\$148.50