

GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE CATALOG/PRICE LIST



RIVERSTONE SOLUTIONS INC
109 Jefferson Street North
Suite 11
Huntsville, AL 35801
T: 256-716-8379
www.riverstonesolutions.com

Multiple Award Schedule (MAS)
Information Technology – IT Services

Special Item No. **54151S Information Technology Professional Services**

Special Item No. **518210C Cloud Professional Services**

Special Item No. **54151HACS Highly Adaptive Cybersecurity Services**

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 INTERNET address for **GSA Advantage!** is <http://www.gsaadvantage.gov>

SCHEDULE TITLE: Federal Supply Schedule 70 – General Purpose Commercial Information Technology Equipment, Software, and Services

CONTRACT NUMBER: 47QTCA20D006F

CONTRACT PERIOD: February 18, 2020 –February 17, 2025

For more information on ordering from Federal Supply go to this website: www.gsa.gov/schedules

CONTRACTOR’S ADMINISTRATION SOURCE:

Riverstone Solutions, Inc.
109 Jefferson Street N, Suite 11
Huntsville, AL 35801
(256) 769-8379
GSA@riverstonesolutions.com

BUSINESS SIZE: Small, Woman Owned Small Business, HUBZone Business

CUSTOMER INFORMATION:

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

SIN	DESCRIPTION
SIN 54151S	Information Technology Professional Services- IT Professional Services and/or labor categories for database planning and design; systems analysis, integration, and design; programming, conversion and implementation support; network services, data/records management, and testing.
SIN 518210C	Cloud and Cloud-Related IT Professional Services- IT professional services that are focused on providing the types of services that support the Government’s adoption of, migration to or governance/management of Cloud computing. Specific labor categories and/or fixed price solutions (e.g. migration services, etc.) that support activities associated with assessing Cloud solutions, refactoring workloads for Cloud solutions, migrating legacy or other systems to Cloud solutions, providing management/governance of Cloud solutions, DevOps, developing cloud native applications or other Cloud oriented activities.
SIN 54151HACS	Highly Adaptive Cybersecurity Services- Includes a wide range of fields such as the seven-step Risk Management Framework services, information assurance, virus detection, network management, situational awareness and incident response, secure web hosting, and backup, security services and, Security Operations Center (SOC) services. HACS vendors are cataloged under the 5 subcategories of High Value Asset Assessments; Risk and Vulnerability Assessments, Cyber Hunt, Incident Response, and Penetration Testing.

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN:
Not Applicable, Services Only

1c. HOURLY RATES (Services only):

Information Technology Professional Services	Labor Category	GSA Price 2/18/2020--2/17/2021
SIN 54151S	IT Support Specialist I	\$44.89
SIN 54151S	IT Support Specialist II	\$66.09
SIN 54151S	Systems Analyst III	\$80.59
SIN 54151S	Systems Engineer II	\$83.15
SIN 54151S	Technical Analyst II	\$89.77
SIN 54151S	Database Administrator II	\$122.17
SIN 54151S	Database Administrator III	\$134.20
SIN 54151S	Cyber Security Specialist IV	\$96.75
SIN 54151S	Cyber Security Specialist V	\$122.19
SIN 54151S	Enterprise Consultant	\$122.17
SIN 54151S	Senior Enterprise Consultant	\$136.83

Cloud and Cloud-Related IT Professional Services	Labor Category	GSA Price 2/18/2020 – 2/17/2021
SIN 518210C	Cloud Engineer I	\$89.77
SIN 518210C	Cloud Engineer II	\$99.54
SIN 518210C	Cloud System Analyst	\$110.69
SIN 518210C	Cloud Cyber Security Engineer II	\$123.19
SIN 518210C	Cloud Database Specialist II	\$125.86
SIN 518210C	Cloud Network Architect	\$132.95
SIN 518210C	Cloud Systems Administrator	\$137.46
SIN 518210C	Cloud Enterprise Architect	\$153.41

Highly Adaptive Cybersecurity Services	Labor Category	GSA Price 8/14/2020 – 8/13/2021
54151HACS	Cyber Security Specialist I	\$54.12
54151HACS	Cyber Systems Analyst III	\$79.37
54151HACS	Cyber Security Planner II	\$81.89
54151HACS	Cyber Security Specialist III	\$88.62
54151HACS	Cyber Security Specialist IV	\$97.24
54151HACS	Cyber Security Specialist V	\$122.82
54151HACS	Cyber Security SME	\$152.15
54151HACS	Senior Security Assessment Engineer	\$168.61

2. MAXIMUM ORDER*: \$ 500,000

NOTE TO ORDERING ACTIVITIES: *If the best value selection places your order over the Maximum Order identified in this catalog/pricelist, you have an opportunity to obtain a better schedule contract price. Before placing your order, contact the aforementioned contractor for a better price. The contractor may (1) offer a new price for this requirement (2) offer the lowest price

available under this contract or (3) decline the order. A delivery order that exceeds the maximum order may be placed under the schedule contract in accordance with FAR 8.404.

3. **MINIMUM ORDER:** \$100
4. **GEOGRAPHIC COVERAGE:** 48 contiguous states including the District of Columbia, Alaska, Puerto Rico, and Hawaii
5. **POINT(S) OF PRODUCTION:** N/A
6. **DISCOUNT FROM LIST PRICES:** GSA Net Prices are shown on the attached GSA Pricelist.
7. **QUANTITY DISCOUNT(S):** ½% order \$250,000 and over for SIN 518210C and SIN 54151S
8. **PROMPT PAYMENT TERMS:** 0%, 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. Contact contractor for limit.**
10. **FOREIGN ITEMS:** None
- 11a. **TIME OF DELIVERY:** Negotiated with Ordering Agency
- 11b. **EXPEDITED DELIVERY:** Negotiated with Ordering Agency
- 11c. **OVERNIGHT AND 2-DAY DELIVERY:** N/A
- 11d. **URGENT REQUIRMENTS:** N/A
12. **FOB POINT:** Destination
- 13a. **ORDERING ADDRESS:** Same as contractor
- 13b. **ORDERING PROCEDURES:** Ordering activities shall use the ordering procedures described in Federal Acquisition Regulation 8.405-3 when placing an order or establishing a BPA for supplies or services. The ordering procedures, information on Blanket Purchase Agreements (BPA's) and a sample BPA can be found at the GSA/FSS Schedule Homepage (fss.gsa.gov/schedules).
14. **PAYMENT ADDRESS:** Same as contractor
15. **WARRANTY PROVISION:** N/A for services
16. **EXPORT PACKING CHARGES:** Not applicable
17. **TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE:** N/A
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):** As applicable
- 24b. **Section 508 Compliance for Electronic and Information Technology (EIT):** As applicable
25. **DUNS NUMBER:** 933887031
26. **NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE:** Contractor has an Active Registration in the SAM database.
CAGE Code: 71WX3

27. LABOR CATEGORIES - IT Professional Services SIN 54151S

Commercial Job Title	Minimum/General Experience	Functional Responsibility
IT Support Specialist I	One (1) year of technical experience which applies to a variety of IT related tasks dealing with the design, implementation, maintenance and support for operating systems, hardware, software, applications and other equipment.	Works under supervision to implement solutions as architected and designed.
IT Support Specialist II	Three (3) years of technical experience which applies to a variety of IT related analysis tasks which are broad in nature, concerned with the design, analysis & implementation, including hardware, software & support facilities and/or equipment.	Under general supervision, creates and/or maintains and supports operating systems, IT applications, web-based applications, communications, software, databases, compilers, repositories and utility and dissembler programs. Analyzes and presents available DBMS products to support validated user requirements. Modifies existing software and develops special purpose software to ensure efficiency and integrity between systems and applications.
Systems Analyst III	Four (4) years of technical experience which applies to a variety of IT related analysis tasks which are specific in nature, concerned with the design, analysis & implementation, including personnel, hardware, software & support facilities and/or equipment.	Evaluates, reviews, analyzes and recommends system and data management products to support validated user requirements. Creates and/or maintains operating systems, IT applications, web-based applications, communications, software, databases, compilers, repositories and utility and dissembler programs. Modifies existing software and develops special-purpose software to ensure efficiency and integrity between systems and applications. Performs specific IT and readiness analysis tasks.

Systems Engineer II	Four (4) years of technical experience which applies to engineering work requiring judgment in the evaluation, selection, adaptation and/or modification of standard techniques, procedures and criteria. Experience developing new approaches to problem solving.	Independently performs assignments with instructions as to the general results expected. Receives technical guidance on unusual or complex problems and supervisor approval for all projects. Implement engineering principles, techniques and processes. Determine product specifications and evaluate technologies for implementation and integration within the customer parameters. Document the results of complex analysis and design tasks. Design moderate to complex systems; assist in developing standards and techniques. Also defines system architectures and infrastructures to provide required functionality. Coordinates the activities of Systems Engineers and Jr. Systems Engineers assigned to specific systems engineering projects.
Technical Analyst II	Four (4) years of technical experience which applies to a broad IT related skill set. Experience in IT product and system analysis with skills in identifying functional requirements to solve business problems using IT solutions and in transitioning strategic goals to operations.	Evaluates, reviews, analyzes information system technologies, technical requirements, integration strategies, and recommends technical additions and modifications in support of system design, solution design or technical writing tasks related to user or system documentation.
Database Administrator II	Two (2) years of technical experience which applies to one or more of the leading relational database management systems, such as Microsoft SQL Server, IBM DB2, MySQL and Oracle. General experience with non-relational data management.	Implement, support and manage the corporate database. Design and configure relational database objects. Maintain data integrity and availability. Ensure database security, including backups & disaster recovery. Plan and implement application and data provisioning.
Database Administrator III	Four (4) years of technical experience which applies to one or more of the leading database management systems, such as, Microsoft SQL Server, IBM DB2, MySQL and Oracle and non-relational data management systems.	Implement, support and manage the corporate database. Design and configure relational database objects. Maintain data integrity and availability. Design deploy and monitor database servers. Design data distribution and data archiving solutions. Ensure database security, including backups & disaster recovery. Plan and implement application and data provisioning. Produce entity relationship & data flow diagrams, database normalization schemata, logical to physical database maps, and data table parameters.
Cyber Security Specialist IV	Four (4) years of technical experience which applies to expert knowledge of and ability to apply advanced technical principles, theories, and concepts. Experience with computer forensic and intrusion support to high technology investigations in the form of computer evidence seizure, computer forensic analysis, data recovery, and network assessments, researching and maintaining proficiency in tools, techniques, countermeasures, and trends in computer network vulnerabilities, data hiding and network security and encryption.	Seasoned technical individual contributor possessing extensive expertise in technical domain area. Responsible for assessing or developing solutions to technical issues and problems that are undefined and complex. Assess or develop solutions to complex technical issues and problems that impact multiple area or disciplines. Regularly employs ingenuity and creativity to develop new technical solutions and systems in order to achieve functional objectives. Responsible for maintaining computer and information security incident, damage and threat assessment programs. Duties include investigating computer and information security incidents to determine extent of compromise to information and automated information systems

Cyber Security Specialist V	Six (6) years of technical experience which applies to technical principles, theories, concepts and their application across range of programs. Experience designing, developing or recommending integrated system solutions ensuring proprietary/confidential data and systems are protected, participating with the client in the strategic design process to translate security and business requirements into technical designs, and configuring and validating secure systems.	Individual contributor and recognized subject matter expert within technical IT and security domain areas. Resolves highly complex problems using significant application of technical knowledge, conceptualizing, reasoning and interpretation. Develops, implements or assesses solutions that are highly innovative and achieved through research and integration of best practices. Responsible for maintaining computer and information security incident, damage and threat assessment programs, investigating computer and information security incidents to determine extent of compromise to information and automated information systems, Providing computer forensic and intrusion support to high technology investigations in the form of computer evidence seizure, computer forensic analysis, data recovery, and network assessments, researching and maintaining proficiency in tools, techniques, countermeasures, and trends in computer network vulnerabilities, data hiding and network security and encryption.
Enterprise Consultant	Six (6) years of technical experience which applies to designing, deploying, maintaining and documenting enterprise management solutions for complex heterogeneous IT environments. Has a good understanding of complex, multi-platform information technology (IT) infrastructure operations, processes and tools.	Designs and Deploys architected solution and ability to solve unanticipated complications in the field. Also has a good understanding of both on-premise and cloud deployment models (Public, Private, Hybrid, Community), Cloud Delivery Services (Software as a Service [SAAS], Platform as a Service [PAAS] and Infrastructure as a Service [IAAS]), hypervisors and virtualization. Leads technical teams with diverse areas of specialization to implement multiple software management tools either sequentially or in parallel. May be responsible for planning transition/migration from an existing on-premise Data Center to a Cloud Computing Environment. Identifies and deploys enterprise-wide system management tools. Performs ongoing operation issues and has the capability to manage systems.
Senior Enterprise Consultant	Eight (8) years of technical experience which applies to designing, deploying, maintaining and documenting enterprise management solutions for complex heterogeneous IT environments. Has a good understanding of complex, multi-platform information technology (IT) infrastructure operations, processes and tools.	Technical subject matter expert for enterprise-wide system management tools and operations. Broad understanding of complex, multi-platform information technology (IT) infrastructure operations, hardware, software, processes and tools. Develops detailed design documents for multiple platform three-tiered client server environments including geospatial definition and design. Architect solutions for systems management tools and oversees project implementation. Also has a good understanding of Cloud Deployment Models, hypervisors and virtualization. Design and document enterprise management solutions for complex heterogeneous IT environments. Architect solutions that integrate systems, network and help desk tools into an integrated IT solution. Provide hardware and software tool selection analysis and recommendations. Manages technical teams with diverse areas of specialization to implement multiple software management tools either sequentially or in parallel.

28. LABOR CATEGORIES – Cloud Professional Services SIN 518210C

Commercial Job Title	Minimum/General Experience	Functional Responsibility
Cloud Engineer I	One (1) year of technical experience which applies to an understanding of network concepts, protocols, operating systems security configuration, applications, network scanning, security configuration and compliance in a cloud environment.	Implement or assess with authorization, cloud based operating systems, applications, tools and other enterprise functional service areas in support of technology and compliance activities.
Cloud Engineer II	Two (2) years of technical experience which applies to an understanding of network concepts, protocols, operating systems security configuration, applications, network scanning, security configuration and compliance in a cloud environment.	Performs cloud provisioning, operating, and maintaining systems running on a cloud environment. Ability to identify and gather requirements to define a solution to be built and operated in the cloud. Capabilities to provide cloud operations and deployment guidance and best practices throughout the lifecycle of a project. Implement and support cloud foundational components like databases, logic apps, application gateways, compute, network, storage, backup, disaster recovery.
Cloud System Analyst	Four (4) years of technical experience which applies to the support of various cloud platforms and infrastructure, implementation of cloud security related products	Implements, install, configures, automates, and monitors various cloud services. Perform operational engineering for activities which include platform upgrades, server patching, monitoring, configuration, and troubleshooting. Provide periodic off-hours on-call support for production and development environments. Work closely with a team of architects, engineers, and developers to create functional design specifications and assist with other project deliverables as needed. Employee is considered a user with privileged or administrator access to systems, logs and/or assets aligning with least privilege access necessary for support of functional business areas and IT systems.
Cloud Cyber Security Engineer II	Four (4) years of technical experience which applies to experience in assessing or maintaining cloud-based computer and information security incident, damage and threat assessment programs.	Responsible for developing solutions to technical security issues and problems that are undefined and complex. Develops solutions to complex technical issues and problems that impact multiple area or disciplines. Duties include investigating computer and information security incidents in the cloud to determine extent of compromise to information and automated information systems. Provide cloud compute forensic and intrusion support to high technology investigations in the form of computer evidence seizure, computer forensic analysis, data recovery, and network assessments, researching and maintaining proficiency in tools, techniques, countermeasures, and trends in computer network vulnerabilities, data hiding and network security and encryption.
Cloud Database Specialist II	Four (4) years of technical experience which applies to complex, multi-platform information technology (IT) infrastructure and database related operations, processes and tools	Deploys enterprise-wide system and data management tools. Performs ongoing operation and management of cloud-based data systems. Designs and Deploys architected solutions and has ability to solve unanticipated complications in the field. Has a good understanding of Cloud Deployment Models (Public, Private, Hybrid, Community), Cloud Delivery Services (Software as a Service [SAAS], Platform as a Service [PAAS] and Infrastructure as a Service [IAAS]), hypervisors and virtualization. Deploys and documents enterprise data management solutions for complex

		heterogeneous IT environments. May be responsible for designing new Cloud Computing and data related environments and/or planning transition and data migration from an existing Data Center to a Cloud Computing Environment.
Cloud Network Architect	Four (4) years of technical experience which applies to cloud-based network design and implementation.	Design cloud-based computer networks. Manage software-based routers, switches, modems and firewalls. Research and implement network software, such as network drivers and monitoring applications. Work closely with the CTO or ISSO and other executives to align network design with organizational goals. Supervise network engineers, network admins and other workers in network setup & configuration. Continuously evaluate emerging network technologies to maximize performance, security & efficiency.
Cloud Systems Administrator	Four (4) years of technical experience which applies to the design and implementation of various cloud platforms and infrastructure of cloud security related products	Design and implement public cloud and on-premises platforms. Install, configure, automate, and monitor various cloud services. Implement cloud security related products. Perform operational engineering for activities which include platform upgrades, server patching, monitoring, configuration, and troubleshooting. Provide periodic off-hours on-call support for production and development environments. Work closely with a team of architects, engineers, and developers to create functional design specifications and assist with other project deliverables as needed. Employee is considered a user with privileged or administrator access to systems, logs and/or assets aligning with least privilege access necessary for support of functional business areas and IT systems.
Cloud Enterprise Architect	Six (6) years of technical experience which applies to multiple operating systems such as Linux, Unix, Solaris, Ubuntu, Windows. Good understanding of networking. Detailed experience in designing and long-term IT strategy and planning for complex IT infrastructures and platforms.	Responsible for converting the technical requirements of an enterprise cloud related project into the architecture and design that will guide the final product. Also responsible for bridging the gaps between complex business problems and solutions in the cloud. Work closely with other members of technical team, including DevOps engineers and developers, to ensure that the right technology or technologies are being built. Design, build and implement enterprise-class cloud systems for a production environment. Align standards, frameworks and security with overall business and technology strategy. Identify security design gaps in existing and proposed architectures and recommend changes or enhancements.

29. LABOR CATEGORIES - Highly Adaptive Cybersecurity Services SIN 54151HACS

Commercial Job Title	Minimum/General Experience	Functional Responsibility
Cyber Security Specialist I	One (1) years of technical experience which applies to ability to apply principles, theories, and concepts of narrow technical domain related to information and cyber security.	Individual contributor representing the most common entry point for technical employees; works under direct supervision. Resolves technical problems that are typically not difficult or complex. Works under supervision on less complex projects/ assignments. Responsible for assessing or maintaining computer and information security incident, damage and threat assessment programs.
Cyber Systems Analyst III	Two (2) years of technical experience which applies to ability to information technology and computer systems analysis.	Evaluates, reviews, and analyzes cyber systems, solutions and products to support validated user requirements. Evaluates operating systems, IT applications, web-based applications, communications, software, databases, compilers, repositories to establish and maintain cyber secure systems. Works independently, establishing or assessing procedures to maintain secure personnel, hardware, software and support facilities and/or equipment. Assesses threats and vulnerabilities. Basic understanding of Risk Management Framework, Cyber Hunt and Penetration Testing activities.
Cyber Security Planner II	Two (2) years of technical experience which applies to the ability to Conduct IT engineering work requiring judgment in the evaluation, selection, adaptation and/or modification of standard techniques, procedures and criteria in designing, assessing or maintaining secure information technology systems.	Evaluation and planning to determine configurations, policies and procedures, countermeasures in operational and non-operational situations. Independently performs assignments with instructions as to the general results expected. Receives technical guidance on unusual or complex problems and supervisor approval for all projects. Determine product specifications and evaluate technologies for implementation and integration within the customer parameters. Document the results of complex analysis and design tasks. Design moderate to complex systems; assist in developing standards and techniques. Formulate and document alternative methodologies for achieving customer objectives. Coordinates the activities of Jr. Analysts assigned to specific systems engineering projects.
Cyber Security Specialist III	Four (4) years of technical experience which applies to ability to Design, develop, recommend or evaluate integrated system solutions ensuring proprietary/confidential data and systems are protected.	Detailed understanding of network concepts, protocols, operating systems security configuration, applications, network scanning, security configuration and compliance. Assess and or Audit with authorization operating systems, applications, tools and other enterprise functional service areas in support of compliance activities. Responsible for maintaining computer and information security incident, damage and threat assessment programs. Investigate computer and information security incidents to determine extent of compromise to information and automated information systems Providing computer forensic and intrusion support to high technology investigations in the form of computer evidence seizure, computer forensic analysis, data recovery, and network assessments, researching and maintaining proficiency in tools, techniques, countermeasures, and trends in computer network vulnerabilities, data hiding and

		<p>network security and encryption. Participating with the client in the strategic design process to translate security and business requirements into technical designs, and configuring and validating secure systems; Testing security products/systems to detect computer and information security weakness. Develop plans to safeguard computer files against unauthorized modification, destruction or disclosure.</p>
Cyber Security Specialist IV	<p>Five (5) years of technical experience which applies to Design, develop, recommend or assess integrated system solutions ensuring proprietary/confidential data and systems are protected.</p>	<p>Seasoned technical individual contributor possessing extensive expertise in technical domain area. Responsible for developing solutions to technical issues and problems that are undefined and complex. Develops solutions to complex technical issues and problems that impact multiple area or disciplines. Assess and or Audit with authorization operating systems, applications, tools and other enterprise functional service areas in support of compliance activities. Responsible for maintaining computer and information security incident, damage and threat assessment programs. Investigate computer and information security incidents to determine extent of compromise to information and automated information systems Providing computer forensic and intrusion support to high technology investigations in the form of computer evidence seizure, computer forensic analysis, data recovery, and network assessments, researching and maintaining proficiency in tools, techniques, countermeasures, and trends in computer network vulnerabilities, data hiding and network security and encryption. Participating with the client in the strategic design process to translate security and business requirements into technical designs, and configuring and validating secure systems; Testing security products/systems to detect computer and information security weakness. Develop plans to safeguard computer files against unauthorized modification, destruction or disclosure.</p>
Cyber Security Specialist V	<p>Six (6) years of technical experience which applies to Design, develop, recommend or assess integrated system solutions ensuring proprietary/confidential data and systems are protected.</p>	<p>Individual contributor and recognized subject matter expert within technical domain area. Involves mastery of a specialized domain and thorough understanding of advanced technical principles, theories, and concepts obtained through advanced education. Resolves highly complex problems using significant application of technical knowledge, conceptualizing, reasoning and interpretation. Develops solutions that are highly innovative and achieved through research and integration of best practices. Has in-depth understanding of technical principles, theories, concepts and their application across range of programs. Responsible for maintaining computer and information security incident, damage and threat assessment programs, investigating computer and information security incidents to determine extent of compromise to information and automated information systems, Providing computer forensic and intrusion support to high technology investigations in the form of computer evidence seizure, computer forensic analysis, data recovery, and network assessments, researching and</p>

		maintaining proficiency in tools, techniques, countermeasures, and trends in computer network vulnerabilities, data hiding and network security and encryption. Performs activities to respond to potential and active cybersecurity threats.
Cyber Security Subject Matter Expert (SME)	Six (6) years of technical experience which applies to Design, develop, recommend or assess integrated system solutions ensuring proprietary/confidential data and systems are protected.	Individual contributor and widely recognized thought leader in technical domain area; contributes to the body of knowledge within technical domain. Develops cutting-edge solutions that display ingenuity and are achieved through collaboration and dialogue with other experts in the field. Mentors and coaches junior technical staff. Resolves undefined, highly complex and multi-dimensional problems that require significant technical depth, conceptualization and interpretation. Requires highest knowledge and mastery of highly advanced technologies, scientific principles, theories and concepts. Viewed as the leading expert and/or resource within the field by peers within and outside the organization. Responsible for maintaining computer and information security incident, damage and threat assessment programs. Duties include investigating computer and information security incidents to determine extent of compromise to information and automated information systems, Providing computer forensic and intrusion support to high technology investigations in the form of computer evidence seizure, computer forensic analysis, data recovery, and network assessments, researching and maintaining proficiency in tools, techniques, countermeasures, and trends in computer network vulnerabilities, data hiding and network security and encryption. In addition, duties may include designing, developing or recommending integrated system solutions ensuring proprietary/confidential data and systems are protected. Participating with the client in the strategic design process to translate security and business requirements into technical designs and configuring and validating secure systems.
Senior Security Assessment Engineer	Eight (8) years of technical experience which applies to Design, develop, recommend or assess integrated system solutions ensuring proprietary/confidential data and systems are protected.	Working as an expert within an Information Security team, works in identification, assessment, prioritization and remediation processes of cyber security risks and vulnerabilities. Evaluate cyber security threats, risk, vulnerabilities and processes to determine relative risk to the product, system and organization. In depth understanding of PCI, SOX, SOC1 and/or SOC2 with demonstrated ability to support cyber security related audit/compliance functions. May Perform penetration testing, code reviews, and design/architecture reviews Works closely with development teams to mitigate or remediate security vulnerabilities. In depth understanding of FedRAMP requirements and assessments.