GENERAL SERVICES ADMINISTRATION

Federal Supply Service

Authorized Federal Supply Schedule Price List

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

Multiple Award Schedule

FSC Group: Information Technology FSC Class:
Contract number: 47QTCA18D00G0
Contract period: July 9, 2018 Through July 8, 2023

Markesman LLC dba Markesman Group

11817 CANON BLVD
NEWPORT NEWS, VA 23606-2569
757-932-1369
Charlene Polk
Charlene.Polk@markesman.com
http://www.markesman.com

Business size: Small Business
Veteran Owned Small Business
SBA Certified HUBZone Firm

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

Price list current as of Modification #PS-0005 effective March 21, 2022

Prices Shown Herein are Net (discount deducted)

CUSTOMER INFORMATION

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

SINs	SIN Title
54151S	Information Technology Professional Services
54151HACS	Highly Adaptive Cybersecurity Services (HACS)
OLM	Order-Level Materials (OLM's)

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply. See Page 35

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

SIN 54151S:

LABOR CATEGORIES

We have five hierarchical levels within each labor category. Each level entails several factors, including the candidate's education, experience, interpersonal skills and managerial aptitude. The descriptions provided herein cover typical duties and responsibilities expected of a candidate at a specific level. We have also described standard education and professional experience typical for the level under consideration.

We show below the experience and education requirements for each hierarchical level. When appropriate, we will substitute a candidate's professional experience for his or her academic credentials — and vice versa. The table below highlights the metrics we use while substituting experience for education, or the inverse.

Academic Degree	Degree Substitution	Experience Substitution
Associate's	2 years	2 years
Bachelor's	Associate's + 2 years	4 years
Master's	Bachelor's + 2 years	6 years

Doctorate	Master's + 4 years	10 years

Markesman Group offers an unparalleled value proposal that combines competitive rates, competent staff and operational flexibility. Our rates are market-driven, competitive and in line with the latest figures published by the U.S. Department of Labor's Bureau of Labor Statistics.

When performing tasks at a client's site, our personnel will — in agreement with the client and in compliance with contractual terms — have access to basic operational tools, including office space, supplies, reproduction, telephone service, as well as laboratory and automated data processing facilities.

Experience Levels

Level 1 Technical Experience

Minimum/General Experience – We assess relevant experience based on factors such as project deliverables, candidate profile, team structure and client requirements. Generally, this level requires one to three years of general experience in information systems, including specialized experience in providing state-of-the art solutions in information systems technology (or, if the area of expertise is new state-of-the-art technology, the specialized experience may be less than four years and more consistent with the age of the technology). The incumbent performs highly specialized and technical tasks associated with the most current and cutting-edge technologies. A Level 1 staff member may serve as a technical consultant on a project or a number of projects covering his/her area of technical expertise. Level 1 personnel are generally recognized as professionals possessing limited technical expertise, and are sought out by others in their area of expertise for advice and guidance.

Minimum Education: Associate's degree or equivalent

Functional Responsibility – A Level 1 staff member

- Provides expert, independent services and leadership in specialized analytic of technical areas
- Interacts with team members, supporting senior coworkers on project assignments when necessary
- Provides expertise in areas falling within his/her knowledge realm
- Gives expert advice and assistance in state-of-the-art software/hardware
- Coordinates with contractor management and support personnel to ensure problem definition, resolution and post-implementation follow-up, in compliance with the organization's procedures, requirements and internal controls

Level 2 Technical Experience

Minimum/General Experience – We evaluate relevant experience depending on factors such as project deliverables, candidate profile, team structure and client requirements. A Level 2 staff position generally requires three to six years of general experience in information systems, including specialized experience providing state-of-the-art solutions in information systems technology (or, if the particular area of expertise is new state-of-the-art technology, the specialized experience may be less than six years and more consistent with the age of the technology). Level 2 personnel possess appropriate expertise in the function performed or technology being addressed, and are able to provide subject matter expertise when necessary.

Minimum Education: Bachelor's Degree or equivalent

Functional Responsibility – A Level 2 staff member

- Provides expert, independent services and leadership in specialized analytic or technical areas
- Shares expertise on an as-needed basis to all task assignments
- Provides expert advice and assistance in state-of-the-art software/hardware
- Analyzes current work streams and expected deliverables in order to recommend, when possible, enhancements and improvements that add value to the team's work or the entire project
- Coordinates with contractor management and support personnel to ensure problem definition, resolution and post-implementation follow-up

Level 3 Technical Experience

Minimum/General Experience: We appraise professional experience based on factors such as project deliverables, candidate profile, team structure and client requirements. Generally, this position entails six to nine years of general experience in analytic or information systems, including considerable specialized experience providing state-of-the-art solutions in analytic and information systems technology (or, if the particular area of expertise is new state-of-the-art technology, the specialized experience may be consistent with the age of the technology). Level 3 personnel possess considerable expertise in the function performed or technology being addressed.)

Minimum Education: Bachelor's Degree or equivalent

Functional Responsibility – A Level 3 staff member

- Provide expert, independent services and leadership in specialized analytic or technical areas
- Builds and manages strong working relationships through excellent communication, customer service, and work product delivery
- Improves existing programs by reviewing objectives and specifications; evaluating proposed changes; recommending changes; making modifications
- Creates an environment that breeds trust and collaboration with others; exhibits a strategic business focus with a customer-focused perspective
- Provides expertise on an as-needed basis to all task assignments
- Evaluates system potential by testing compatibility of new programs with existing programs
- Recommends, when necessary, enhancements to work streams and non-IT processes affecting the IT value chain
- Provides expert advice and assistance in state-of-the-art software/hardware
- Coordinates with contractor management and support personnel to ensure that the problem has been properly defined and that the solution will satisfy the organization's requirement

Level 4 Technical Experience

Minimum/General Experience: We assess pertinent experience based on factors such as project deliverables, candidate profile, team structure and client requirements. Generally, this position requires

nine to twelve years of general experience in analytic or information systems, including specialized experience providing state-of-the-art solutions in analytic or information systems technology (or, if the particular area of expertise is new state-of-the-art technology, the specialized experience may consistent with the age of the technology).

Minimum Education: Bachelor's Degree or equivalent

Functional Responsibility – A Level 4 staff member

- Guides program and project managers through the project management framework, thus enabling the successful execution of projects carried out from the project management lifecycle
- Shares expert, independent services and leadership in specialized analytic or technical areas
- Leads the evaluation, planning and execution of large , strategic programs across multiple work streams
- Supports and drives program success by supporting alignment with strategic priorities, sequencing with other large, strategic initiatives and ensuring program management excellence
- Supports team in distributing project portfolio information to executive management, and key stakeholders
- Provides expertise, when necessary, to all task assignments
- Shares expert advice and assistance in state-of-the-art software/hardware
- Coordinates with contractor management and support personnel to identify problems, fix inefficiencies and solve deficiencies in compliance with the organization's requirement

Level 5 Technical Experience

Minimum/General Experience: We evaluate relevant experience based on factors such as project deliverables, candidate profile, team structure and client requirements. Generally, this position requires twelve or more years of general experience in information systems, including specialized experience providing state-of-the-art solutions in analytic or information systems technology (or, if the particular area of expertise in new state-of-the-art technology, the specialized experience may be consistent with the age of the technology). Personnel at this level are recognized experts in the technology being addressed.

Minimum Education: Master's Degree or equivalent

Functional Responsibility – A Level 5 staff member

- Formulates a plan that aligns with key stakeholders across brands, regions, functions, and steering committees to monitor the health of each initiative and advocate for the project through its lifecycle
- Support team in facilitating feedback between governance committees, corporate PMOs, and other departments throughout the organization striving for continuous process improvement
- Maintains and facilitates the alignment, prioritization, and pacing of projects, including enabling and timely resolution identification of cross-functional risks to major initiatives
- Drives project management and financial rigor across relevant work streams to ensure planning is realistic while also supporting strategic objectives and timing during the strategic planning processes

- Provides expert, independent services and leadership in specialized analytic or technical areas
- Provides guidance and recommendations to program and project managers and business stakeholders based upon feasibility, benefit, risk, and resource capability
- Requires a big-picture focus, broad business process experience, relationship building, and client management skills

GENERAL LABOR CATEGORY DESCRIPTIONS

Subject Matter Expert

Primary Responsibilities:

- Performs as a consultant in a highly specialized, leading edge information technologies and methodologies. Performs elaborate analysis and studies
- Provides highly technical and specialized guidance concerning automated solutions to complex information processing problems
- Prepares reports, gives presentations & works independently or as a member of a team
- Recognizes areas for internal improvement and developing plans for implementing them
- May serve as a Contractor Task Order Project Manager
- Understands, articulates and implements best practices related to their area of expertise
- May lead or be an active participant of a work-group with the need for specialized knowledge
- Provides guidance on how their area of capability can resolve an organizational need and actively participates in all phases of the Software and Hardware development life cycle

Additional Responsibilities:

- Cultivates and maintains effective working relationships with a variety of stakeholders, including end users, project managers, engineers and senior staff members
- Participates in multiple work-groups at one time, and disseminating information across all levels of the organization
- Is articulate and communicates effectively to diverse audiences; translates subject matter terminology into business terms and recommends alternatives to both senior management and end users.

System Administrator

Primary Responsibilities:

- Relies on extensive experience and judgment to plan and accomplish goals
- Is responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software and related infrastructure
- Participates in technical research and development to enable continuing innovation within the infrastructure
- Ensures that system hardware, operating systems, software systems, and related procedures adhere to organizational values, enabling staff, volunteers, and Partners

- Acts as the communications conduit to executive sponsor; conducts periodic briefings/status updates

Additional Responsibilities:

- Assists project teams with technical issues in the Initiation and Planning phases of our standard Project Management Methodology
- Takes part in the definition of needs, benefits, and technical strategy; research & development within the project life-cycle; technical analysis and design; and support of operations staff in executing, testing and rolling-out the solutions
- Participates in projects to streamline the transition of projects from development staff to production staff by performing operations activities within the project life-cycle

Software Developer

Primary Responsibilities:

- Specializes in software development using a particular language or development tool. Prepares detailed specifications from which programs will be written
- May be involved in related activities such as research and development and evaluation of commercial off-the-shelf (COTS) products
- Operates in advanced technical environments such as Visual Basic, C, C++, C#, Java, XML, Cold Fusion and ASP

Additional Responsibilities:

- Performs coding, debugging and testing to define the integration between proposed development projects and existing systems
- Considers and researches emerging technologies to improve current applications, architectures and processes
- Designs, develops, and implements customized solutions for various systems
- Provides post-deployment support for all custom applications and implementations provided to the government

IT Analyst

Primary Responsibilities:

- Provides highly technical and specialized solutions to complex IT problems
- Supports the Lead IT Manager and extends technical support to the Manufacturing client
- Manages network groups and folder permissions
- Tracks user help desk tickets, diagnoses issues and resolves on front-end support
- Maintains user accounts and hardware inventory
- Is involved in the design, operation and maintenance of technology products

Additional Responsibilities:

- Communicates project status with clients and management
- Performs backups and changes as per company directives

- Administers and troubleshoots Windows servers, LAN and components
- Handles daily server backups, anti-virus protection, performance tuning and security changes
- May design systems and assess the effectiveness of technology resources already in use or new systems that are being implemented
- Determines the practicality of changes and modification of systems
- Works with external partners, including consultants, agencies and vendors, to arrive at the most appropriate system or integration of multiple systems

IT Engineer

Primary Responsibilities:

- Responsible for solving engineering problems relating to resources and facilities management, database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, data/records management, and other computer related services
- Determines program objectives and requirements and develops standards and guides for diverse engineering and scientific activities
- Guides the successful completion of major programs and may function in a project leadership role
- Serves as the prime technical contact on contracts and projects

Additional Responsibilities:

- Interacts with customers on significant technical matters
- Responsible for network management, software development and database administration
- Provide technical support to a business or an organization's employees and train non-technical workers on the business's information systems

SIN 54151HACS:

Labor Category Name	Labor Category Description	Min Years' Experience	Min Education
Subject Matter Expert 1	The Subject Matter Expert 1 has industry experience in the relevant subject matter. This individual will use information technology expertise and/or industry focus expertise in fulfilling the interpreted customer specification. The Subject Matter 1 is highly experienced in the industry regarding information technology. The Subject Matter Expert 1 provides thought leadership related to current and future customer plans in relation to the state information technology.	10	Bachelor's
Subject Matter Expert 2	The Subject Matter Expert 2 has industry experience in the relevant subject matter. this individual will use information technology expertise and/or industry focus expertise in	12	Bachelor's

	fulfilling the interpreted customer specification. The Subject Matter Expert 2 is highly experienced in the industry regarding information technology. The Subject Matter Expert 2 provides thought leadership related to current and future customer plans regarding the stated information technology.		
Subject Matter Expert 3	The Subject Matter Expert 3 has industry experience in the relevant subject matter. This individual will use information technology expertise and/or industry focus expertise in fulfilling the interpreted customer specification. The Subject Matter Expert 3 is highly experienced in the industry regarding the stated information technology. The Subject Matter Expert3 provides thought leadership related to current and future customer plans regarding the stated information technology.	15	Bachelor's
Subject Matter Expert 4	The Subject Matter Expert 4 has industry experience in the relevant subject matter. This individual will use information technology expertise and/or industry focus expertise in fulfilling the interpreted customer specification. The Subject Matter Expert 4 is highly experienced in the industry regarding the stated information technology. The Subject Matter Expert3 provides thought leadership related to current and future customer plans regarding the stated information technology.	20	Masters
Incident Response Analyst 1	Contributes to generating response to crisis or urgent situations to mitigate immediate or potential threats. The Incident Response Analyst 1 uses mitigation, preparedness, and response and recovery approaches, as needed, to ensure proper information security. The individual handles and responds to cyber security incidents through coordination with stakeholders such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement, and privacy offices. The Incident Response Analyst 1 conducts intake incident reporting, ticket updates, and notifies stakeholders of cybersecurity incidents and forensic investigations in relation to computer security incidents and escalates when necessary, as well as coordinates response to computer security incidents. The Incident	2	High School / GED

	Response Analyst provides recommendations as to a course of action on each incident and creates, manages, and records all actions taken and serves as the initial POC for Events of Interest reported both internally and externally.		
Incident Response Analyst 2	Contributes to generating responses to crisis or urgent situations to mitigate immediate and / or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to ensure proper information security. The Incident Response Analyst 2 provides oversight for incident data flow and response, content, and remediation. Partners with other incident response centers in maintaining anunderstanding of threats, vulnerabilities, and exploits that could impact networks and assets Performs real-time proactive event investigation on various security enforcement systems, such as SIEM, Anti-virus, Internet content filtering/reporting, malicious code prevention, Firewalls, IDS & IPS, Web security, anti- spam, etc. The individual performs the role of Incident Coordinator for IT Security events requiring focused response, containment, investigation, and remediation and performs forensic analysis on hosts supporting investigations. The Incident Response Analyst 2 conducts both static and dynamic malware analysis in customer and external environments.	2	Bachelor's
Incident Response Analyst 3	Contributes to generating responses to crisis or urgent situations to mitigate immediate and / or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. The Incident Response Analyst 3 will lead shifts and functional IR teams, providing oversight for incident data flow and response, content, and remediation, and partners with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets. The individual performs real-time proactive event investigation on various security enforcement systems, such as SIEM, Anti-Virus, Internet content filtering/reporting, malicious code identification, Firewalls, IDS & IPS, Web Security, anti-spam, etc. The Incident Response Analyst 3 also performs the role of Incident Coordinator for IT Security events requiring focused response, containment, investigation, and remediation, forensic analysis on hosts supporting	5	Bachelors

	investigations conducts both static and dynamic malware analysis in customer and external environments. The individual coordinates response action to identify threats and incidents, analyzes operational anomalies, network behavior and performs mitigation actions derived from cyber threat monitoring and anomaly analysis, and actively monitors the networks for cybersecurity threats and vulnerabilities. The Incident Response Analyst 3 provides oversight and performs quality assurance on Incident Closures and assists with knowledge management Standard Operating Procedures and procedural support data.		
Incident Response Analyst 4	Contributes to generating responses to crisis or urgent situations to mitigate immediate and / or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. The Incident Response Analyst 4 leads one or more functional security teams (Incident response, forensics, cyber intelligence, etc.), support the development of staff schedules and staffing forecast for approval, ensures shift members follow the appropriate incident escalation and reporting procedures, provides support promptly and efficiently through front-line telephone and email communications, ingest, triage, prioritize, assign, track, document, and manage incidents and results. The individual will correlate, map, and fuse any and all incident information for the development and distribution of cyber alerts and notices, or other products as required, document technical details of current or potential intruder threats consistent with environment, coordinate, communicate, share information, and work closely with organizational stakeholders. The Incident Response Analyst 4 will be responsible for knowledge management of operational procedures and support documentation.	7	Bachelor's
Cyber Security Engineer 1	Participate in special projects or investigations into specific technology or solution issues and research and piloting of new technologies. Serve as point of contact for engineering efforts while assisting in maintaining compliance with the customer's policies and guidelines. Duties may include providing administrative support to enterprise security devices, providing support in various applications and implement security standards, assist with configuration, validate secure complex systems, and test security	0	Bachelor's

	products and systems to detect security weakness.		
Cyber Security Engineer 2	The Cyber Security Engineer 2 participates in special projects or investigations specific technology or solution issues and research and piloting of new technologies. Serves as point of contact for engineering efforts and assisting in maintaining compliance with the customer's policies and guidelines. Duties may include assisting with assessing, designing, developing, and recommending integrated security system solutions that ensure proprietary and confidential data and systems are protected, providing assistance with technical engineering services for the support of integrated security systems and solutions, interface with the client in the strategic design process to translate security and business requirements into technical designs and assist with configuration, validate secure complex systems, and test security products and systems to detect security weakness.	3	Bachelor's
Cyber Security Engineer 3	The Cyber Security Engineer 3 participates in special projects or investigations specific technology or solution issues and research and piloting of new technologies. Serves as point of contact for engineering efforts and assists in maintaining compliance with the customer's policies and guidelines. Duties may include configuring and maintaining policies, maintaining documentation for exceptions to standards, providing timely and adequate responses to threats/alerts, assessing security events to drive to a resolution, providing timely and sufficient response to security incidents and assessment services, promotes security awareness.	6	Bachelor's
Cyber Security Engineer 4	The Cyber Security Engineer 4 participates in special projects or investigations specific technology or solution issues and research and piloting of new technologies. Serves as point of contact for engineering efforts and assists in maintaining compliance with the customer's policies and guidelines. Duties may include lead team of security engineers, manage large scale deployment, assessment, and O&M projects, validate and verify system security requirements definitions and analysis and establish system	8	Bachelor's

	security designs, design, develop, implement and/or integrate IA and security systems and system components including those for networking, computing, and enclave environments, build IA into systems deployed to operational environments		
Cyber Security Architect 1	The Cyber Security Architect 1 provides thought leadership related to current and future customer plans regarding protecting customer information technology from cyber threats. This individual possesses knowledge of the future direction and trends associated with the stated information technology and is up to date with current threats associated with it. Cyber Security Architect 1 is experienced in designing and implementing protections for information architecture solutions for the stated information technology. This individual designs secure architecture to include the software, hardware, and communications to support the total requirements as well as provided for present and future cross-functional requirements and interfaces.	5	Bachelor's
Cyber Security Architect 2	The Cyber Security Architect 2 provides thought leadership related to current and future customer plans regarding protecting customer information technology from cyber threats. This individual possesses knowledge of the future direction and trends associated with the stated information technology and is up to date with current threats associated with it. Cyber Security Architect 2 is experienced in designing and implementing protections for information architecture solutions for the stated information technology. This individual designs secure architecture to include the software, hardware, and communications to support the total requirements as well as provided for present and future cross-functional requirements and interfaces.	8	Bachelor's
Cyber Security Architect 3	The Cyber Security Architect 3 provides thought leadership related to current and future customer plans regarding protecting customer information technology from cyber threats. This individual possesses knowledge of the future direction and trends associated with the stated information technology and is up to date with	10	Bachelor's

	current threats associated with it. Cyber Security Architect 3 is experienced in designing and implementing protections for information architecture solutions for the stated information technology. This individual directs, and establishes business, information, and strategy requirements for enterprise-wide or large-scale information process implementations, systems databases, and/or networks on cybersecurity related efforts.		
Cyber Security Architect 4	The Cyber Security Architect 4 provides leadership related to current and future customer plans regarding protecting customer information technology from cyber threats. This individual possesses in depth knowledge of the future direction and trends associated with the stated information technology and is up to date with current threats associated with it. Cyber Security Architect 4 is experienced in designing and implementing protections for information architecture solutions for the stated information technology. This individual directs, and establishes business, information, and strategy requirements for enterprise-wide or large-scale information process implementations, systems databases, and/or networks on cybersecurity related efforts. Oversees and leads the development of architecture projects including technical architecture, business architecture, strategic planning, and business process design. Oversees and lead that analysis and response to the customer.	15	Masters
Threat Hunt Analyst 1	The Threat Hunt Analyst will perform duties such as Intrusion Detection, Incident Response, Risk and Vulnerability Analysis to collect and analyze forensic network data to support cybersecurity related investigations. Additional responsibilities include forensic collection, intrusion correlation/tracking, and threat analysis, and/or malware/ malicious code analysis, as well as, performing malware triage on host-based instructions, cyber threat hunting to discover anomalies that lead to instruction discovery, identifying specific vulnerabilities and making recommendations to enable remediation, generate Intrusion Detection Signatures for multiple platforms.	4	Bachelor's or 4 years additional relevant experience

Threat Hunt Analyst 2	The Threat Hunt Analyst will perform duties such as Intrusion Detection, Incident Response, Risk and Vulnerability Analysis to collect and analyze forensic network data to support cybersecurity related investigations. Duties may also include ensuring policies and configurations are compliant with enterprise regulations, generating technical reports of findings and recommending cost effective security control adjustments to counter future intrusions. Additional responsibilities include forensic collection, intrusion correlation/tracking, and threat analysis, and/or malware/ malicious code analysis, as well as, performing malware triage on host-based instructions, cyber threat hunting to discover anomalies that lead to instruction discovery, identifying specific vulnerabilities and making recommendations to enable remediation, generate Intrusion Detection Signatures for multiple platforms.	6	Bachelor's or 4 years of additional relevant experience
Threat Hunt Analyst 3	The Threat Hunt Analyst will perform duties such as Intrusion Detection, Incident Response, Risk and Vulnerability Analysis to collect and analyze forensic network data to support cybersecurity related investigations. Duties may also include ensuring policies and configurations are compliant with enterprise regulations, generating technical reports of findings and recommending cost effective security control adjustments to counter future intrusions. Additional responsibilities include forensic collection, intrusion correlation/tracking, and threat analysis, and/or malware/ malicious code analysis, as well as, performing malware triage on host-based instructions, cyber threat hunting to discover anomalies that lead to instruction discovery, identifying specific vulnerabilities and making recommendations to enable remediation, generate Intrusion Detection Signatures for multiple platforms.	10	Bachelor's or 4 years of additional relevant experience
Threat Hunt Analyst 4	The Threat Hunt Analyst will perform duties such as Intrusion Detection, Incident Response, Risk and Vulnerability Analysis to collect and analyze forensic network data to support cybersecurity related investigations. Duties may also include ensuring policies and configurations are compliant with enterprise regulations,	18	Bachelor's or an additional 4 years of relevant experience

	generating technical reports of findings and recommending cost effective security control adjustments to counter future intrusions. Additional responsibilities include forensic collection, intrusion correlation/tracking, and threat analysis, and/or malware/ malicious code analysis, as well as, performing malware triage on host-based instructions, cyber threat hunting to discover anomalies that lead to instruction discovery, identifying specific vulnerabilities and making recommendations to enable remediation, generate Intrusion Detection Signatures for multiple platforms		
Cyber Threat Intelligence Analyst 1	The Cyber Threat Intelligence Analyst provides review of classified and unclassified cyber news fees, signature updates, incident reports, threat briefs, and vulnerability alerts from external sources and determines its applicability to the customer environment. The Cyber Threat Intelligence Analyst disseminates information externally within the cyber intelligence community, interprets and compiles the information received about emerging threats at different classification levels through data feeds from Internet security firms, Government organizations, private industry, and foreign Governments into actionable monitoring either by developing custom content or by some other means. The Cyber Threat Intelligence Analyst identifies potential threats based on enterprise utilized hardware and software and accounts for current and evolving hacking tools and methodologies available to disrupt these systems. The Cyber Threat Intelligence Analyst participates in cybersecurity exercises, designs, leads or supports cybersecurity exercises and supports Blue Team / Red Team activity.	4 years of project related experience or 2 years with a Bachelors. Meets or exceeds current industry certification requirements.	Bachelor's Degree or equivalent
Cyber Threat Intelligence Analyst 2	The Cyber Threat Intelligence Analyst 2 provides review of classified and unclassified cyber news fees, signature updates, incident reports, threat briefs, and vulnerability alerts from external sources and determines its applicability to the customer environment. The Cyber Threat Intelligence Analyst disseminates information externally within the cyber intelligence community, interprets and compiles the information received about emerging threats	6 years of project related experience or 3 years with a Bachelors. Meets or exceeds current industry	Bachelors

	at different classification levels through data feeds from Internet security firms, Government organizations, private industry, and foreign Governments into actionable monitoring either by developing custom content or by some other means. The Cyber Threat Intelligence Analyst identifies potential threats based on enterprise utilized hardware and software and accounts for current and evolving hacking tools and methodologies available to disrupt these systems. The Cyber Threat Intelligence Analyst participates in cybersecurity exercises, designs, leads or supports cybersecurity exercises and supports Blue Team / Red Team activity.	certification requirements.	
Cyber Threat Intelligence Analyst 3	The Cyber Threat Intelligence Analyst 3 provides review of classified and unclassified cyber news fees, signature updates, incident reports, threat briefs, and vulnerability alerts from external sources and determines its applicability to the customer environment. The Cyber Threat Intelligence Analyst disseminates information externally within the cyber intelligence community, interprets and compiles the information received about emerging threats at different classification levels through data feeds from Internet security firms, Government organizations, private industry, and foreign Governments into actionable monitoring either by developing custom content or by some other means. The Cyber Threat Intelligence Analyst identifies potential threats based on enterprise utilized hardware and software and accounts for current and evolving hacking tools and methodologies available to disrupt these systems. The Cyber Threat Intelligence Analyst participates in cybersecurity exercises, designs, leads or supports cybersecurity exercises and supports Blue Team / Red Team activity.	8 years of project related experience or 5 years with a Bachelors. Meets or exceeds current industry certification requirements.	Bachelors
Cyber Threat Intelligence Analyst 4	The Cyber Threat Intelligence Analyst provides review of classified and unclassified cyber news fees, signature updates, incident reports, threat briefs, and vulnerability alerts from external sources and determines its applicability to the customer environment. The Cyber Threat Intelligence Analyst disseminates information externally within the cyber intelligence community, interprets and compiles the	10 years of project related experience or 6 years with a Bachelors - Meets or exceeds current	Bachelors

	information received about emerging threats at different classification levels through data feeds from Internet security firms, Government organizations, private industry, and foreign Governments into actionable monitoring either by developing custom content or by some other means. The Cyber Threat Intelligence Analyst identifies potential threats based on enterprise utilized hardware and software and accounts for current and evolving hacking tools and methodologies available to disrupt these systems. The Cyber Threat Intelligence Analyst participates in cybersecurity exercises, designs, leads or supports cybersecurity exercises and supports Blue Team / Red Team activity.	industry certification requirements.	
Vulnerability Assessment Analyst 1	May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. The Vulnerability Assessment Analyst executes tests by following the steps and procedures listed in a test plan and documents results in a standardized format that is appropriate for future analyses, assists in the coordination of technical tests, network, scans and/or vulnerability scans that support the evaluation of information safeguard effectiveness. The Vulnerability Assessment Analyst conducts reconnaissance data gathering and vulnerability research and assists in the creation of risk and vulnerability reporting.	0	Associates
Vulnerability Assessment Analyst 2	May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. The Vulnerability Assessment Analyst2 supports development of and follows general test and evaluation plans to compare current and proposed technologies; assesses test results to determine whether they match requirements specifications, assists in the coordination of technical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness. The Vulnerability Assessment Analyst 2 also conducts reconnaissance, target assessment, data gathering and vulnerability research. The	3	Associates

	individual leverages COTS tools to conduct vulnerability assessments, analyzes results, identifies exploitable vulnerabilities, and verifies vulnerabilities. The Vulnerability Assessment Analyst 2 also prepares report documents by tailoring technical information and creates benchmark or security authorization reports; outlines key findings related to speed, risks, results and reliability, and recommends acceptance or rejection of technology for applied use.		
Vulnerability Assessment Analyst 3	May support in part or in whole technical vulnerabilityassessments of applications and infrastructure, vulnerability research, and generation of assessmentreports. The Vulnerability Assessment Analyst 3 contributes to the selection of appropriate technical tests, network or vulnerability scan tools, and/or pen testing tools based on review of requirements and purpose; lists all steps involved for executing selectedtest(s) and coaches others in the use of advanced research, development, or scan tools and the analysis of comparative findings between proposed and current technologies. The individual coordinates or leads teams to conducts ethical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness, conduct reconnaissance, target assessment, targetselection, and vulnerability research. The individual also utilized COTS tools, conduct or leads teams to conduct vulnerability assessments, analyzes results, identifiesexploitable vulnerabilities, and verifies vulnerabilities through manual assessment, prepares and reviews assessment documents, validates and communicates key findings to stakeholders	5	Bachelor's
Vulnerability Assessment Analyst 4	May support in part or in whole technical vulnerabilityassessments of applications and infrastructure, vulnerability research, and generation of assessmentreports. The Vulnerability Analyst 4 may devise and / or select appropriate technical tests,network or vulnerability scan tools, and/or pen testing tools based on review of requirements and purpose; lists all steps involved for executing selected test(s) and coaches others in the use of advanced research, development, or scan tools and the analysis of comparative findings	6	Bachelor's

	between proposed and current technologies, coordinates or leads teams to conducts ethical tests, network scans, and/or vulnerability scans that supportthe evaluation of information safeguard effectiveness, conduct reconnaissance, target assessment, target selection, and vulnerability research. The induvial creates custom tools and exploits to penetrate various levels of controls including network, operatingsystem, and physical, using COTS or custom tools, conduct or leads teams to conduct vulnerability assessments, analyzes results, identifies exploitable vulnerabilities, and verifies vulnerabilities through manual assessment and prepares and reviews assessment documents,validates and communicates key findings to stakeholders		
Risk Analyst 1	Participates in conduct of controls and security assessments to assess risk of exposure of proprietarydata through weaknesses in platforms, access procedures, or forms of access to the organization's systems and the data contained in them. The Risk Analyst 1 provides technical support on post event networksecurity logs and trend analysis, uncovers security and compliance violations, associates and correlates IP address related eventswith specific systems or devices in the IT infrastructure. The individual also supports development and analysis of system and security documentation and maintains documentation for exceptions to standards.	0	Bachelor's
Risk Analyst 2	Participates in conduct of controls and security assessments to assess risk of exposure of proprietarydata through weaknesses in platforms, access procedures, or forms of access to the organization's systems and the data contained in them. The Risk Analyst 2 develops, documents, and executes containment strategies, documents and briefs the business remediation options and executes the plan with stakeholders, produces final report and recommendation coordinates efforts of, and provides timely updates to multiple business units during response. This individual also performs in-depth analysis in support of incident response operations, develops requirements for technical capabilities for cyber incident management, investigates major breeches f security and recommends appropriate control improvements. The Risk Analyst 2 also works	4	Bachelor's

	with infrastructure and application support teams to drive closure of follow up actions identified through incident and problem management, performs Security Control Assessments on systems to validate the results of risk assessments and ensure controls in the security pan are present and operating correctly on the system; provides thorough report of the risks to the system and its data. The Risk Analyst 2 develops and analyzes the system and security documentation.		
Risk Analyst 3	Participates in conduct of controls and security assessments to assess risk of exposure of proprietarydata through weaknesses in platforms, access procedures, or forms of access to the organization's systems and the data contained in them. The Risk Analyst 3 supports engineering design teams by assessing network and system security design features and making recommendations concerning overall security accreditation readiness and compliance and best practices, supports interoperability assessment teams and presents written analysis and conclusions in all phases of analysis The individual develops and analyses system and security documentation, follow up with site administrators for status on non-compliant platforms and maintains any necessary exception documentation. The Risk Analyst 3 also maintains documentation for exceptions to standards and participates in Security Control Assessments on systems to validate the results of risk assessments and ensure controls in the security plan are present and operating correctly on the system; provides thorough report of the risks to the system and its data. This individual also evaluates system findings, develop PO&AMs, and briefs stakeholders on key finding, recommendations, risk, and impact.	7	Bachelor's
Risk Analyst 4	Participates in conduct of controls and security assessments to assess risk of exposure of proprietarydata through weaknesses in platforms, access procedures, or forms of access to the organization's systems and the data contained in them. The Risk Analyst 4 holds the ability to actively lead and manage project update briefings, working sessions and stakeholder meetings. The individual possesses and applies strong analytical/assessment to security systems and enterprise architecture (e.g., conducting gap analyses, risk	10	Bachelors

	assessments). The Risk Analyst4 participates in Security Control Assessments and ensures controls in the security plan are present and operating correctly on the system; provides thorough reporting of the risks to the system; and its data and evaluates system findings, develops PO&AMS, and briefs stakeholders on key findings, recommendations, risk, and impact.		
Forensics Analyst 1	Conducts forensic acquisition and analysis of cyber security incidents, performs Hunt Operations actively searching for indicators of compromise. The Forensics Analyst provides information for the indicator database and assists with signature creation and tuning to ensure proper agency cyber defenses. This individual works directly with system administrators to remediate systems to mitigate and/or prevent incidents of compromise, actively works to reduce and mitigate findings from "Hunt Operations" or from other assessments and will report progress as requested by the customer. The Forensics Analyst assists digital forensics investigations and has experience maintaining chain of custody ad cataloguing evidence/information related to forensics investigations, eDiscovery and possesses working knowledge of EnCase or similar forensics tools.	4 years of project related experience or 2 years with a Bachelors. Meets or exceeds current industry certification requirements.	Bachelor's or equivalent
Forensics Analyst 2	Conducts forensic acquisition and analysis of cyber security incidents, performs Hunt Operations actively searching for indicators of compromise. The Forensics Analyst provides information for the indicator database and assists with signature creation and tuning to ensure proper agency cyber defenses. This individual works directly with system administrators to remediate systems to mitigate and/or prevent incidents of compromise, actively works to reduce and mitigate findings from "Hunt Operations" or from other assessments and will report progress as requested by the customer. The Forensics Analyst assists or leads digital forensics investigations and has experience maintaining chain of custody ad cataloguing evidence/information related to forensics investigations, eDiscovery and possesses working knowledge of EnCase or similar forensics tools.	6 years of project related experience or 3 years with a Bachelors. Meets or exceeds current industry certification requirements	Bachelors or Equivalent

Forensics Analyst 3	Conducts forensic acquisition and analysis of cyber security incidents, performs Hunt Operations actively searching for indicators of compromise. The Forensics Analyst provides information for the indicator database and assists with signature creation and tuning to ensure proper agency cyber defenses. This individual works directly with system administrators to remediate systems to mitigate and/or prevent incidents of compromise, actively works to reduce and mitigate findings from "Hunt Operations" or from other assessments and will report progress as requested by the customer. The Forensics Analyst assists or leads digital forensics investigations and has experience maintaining chain of custody ad cataloguing evidence/information related to forensics investigations, eDiscovery and possesses working knowledge of EnCase or similar forensics tools.	8 years of project related experience or 5 years with a Bachelors. Meets or exceeds current industry certification requirements.	Bachelors or Equivalent
Forensics Analyst 4	Conducts forensic acquisition and analysis of cyber security incidents, performs Hunt Operations actively searching for indicators of compromise. The Forensics Analyst provides information for the indicator database and assists with signature creation and tuning to ensure proper agency cyber defenses. This individual works directly with system administrators to remediate systems to mitigate and/or prevent incidents of compromise, actively works to reduce and mitigate findings from "Hunt Operations" or from other assessments and will report progress as requested by the customer. The Forensics Analyst assists or leads digital forensics investigations and has experience maintaining chain of custody ad cataloguing evidence/information related to forensics investigations, eDiscovery and possesses working knowledge of EnCase or similar forensics tools.	10 years of project related experience or 6 years with a Bachelors - Meets or exceeds current industry certification requirements.	
Computer Network Operations Planning Support Specialist 1	Supports various types of planning efforts in support of Computer Network Operations, most entail development of CNO requirements and/or providing actionable recommendations and technical support. This individual identifies, organizes, and documents steps to conduct CNO, which may include the development of	4	Bachelor's

	long-term functional requirements, assists in the determination of risks and benefits when recommending actions to mitigate cyber threats, develops success criteria associated with CNO to be performed, and prepares assessments of CNO. The Computer Network Operations Planning Support Specialist (CNOPSS)performs multi-sours research of all U.S. exercises involving CNO to support operations personnel and overall CNO synchronization, assesses value and material compiled from research, documents objectives and benefits of each activity or plan based on available material, documents common NCO threads based on CNO activity, outlines key operations processes and metrics. This individual will also provide the means to assess the effects of mission partner execution of CNO, develop and document processes and procedures for assessing impact, Measure of Effectiveness, and follow-on courses of action development, assists in determination of what established processes and procedures will need to become more automated. The COPSS will recommend areas for improvement, attend mission related forums and address emerging operational requirements, share emerging findings as they become known, complete and implement operations processes, maintain awareness of internal and external customer information needs and collaborate with other Intelligence Community members to produce plans, reports, and lessons learned.		
Computer Network Operations Planning Support Specialist 2	Supports various types of planning efforts in support of Computer Network Operations, most entail development of CNO requirements and/or providing actionable recommendations and technical support. This individual identifies, organizes, and documents steps to conduct CNO, which may include the development of long-term functional requirements, assists in the determination of risks and benefits when recommending actions to mitigate cyber threats, develops success criteria associated with CNO to be performed, and prepares assessments of CNO. The Computer Network Operations Planning Support Specialist (CNOPSS)performs multi-sours research of all U.S. exercises	6	Bachelor's

	involving CNO to support operations personnel and overall CNO synchronization, assesses value and material compiled from research, documents objectives and benefits of each activity or plan based on available material, documents common NCO threads based on CNO activity, outlines key operations processes and metrics. This individual will also provide the means to assess the effects of mission partner execution of CNO, develop and document processes and procedures for assessing impact, Measure of Effectiveness, and follow-on courses of action development, assists in determination of what established processes and procedures will need to become more automated. The COPSS will recommend areas for improvement, attend mission related forums and address emerging operational requirements, share emerging findings as they become known, complete and implement operations processes, maintain awareness of internal and external customer information needs and collaborate with other Intelligence Community members to produce plans, reports, and lessons learned.		
Computer Network Operations Planning Support Specialist 3	Supports various types of planning efforts in support of Computer Network Operations, most entail development of CNO requirements and/or providing actionable recommendations and technical support. This individual identifies, organizes, and documents steps to conduct CNO, which may include the development of long-term functional requirements, assists in the determination of risks and benefits when recommending actions to mitigate cyber threats, develops success criteria associated with CNO to be performed, and prepares assessments of CNO. The Computer Network Operations Planning Support Specialist (CNOPSS)performs multi-sours research of all U.S. exercises involving CNO to support operations personnel and overall CNO synchronization, assesses value and material compiled from research, documents objectives and benefits of each activity or plan based on available material, documents common NCO threads based on CNO activity, outlines key operations processes and metrics. This individual will also provide the	8	Bachelor's

	means to assess the effects of mission partner execution of CNO, develop and document processes and procedures for assessing impact, Measure of Effectiveness, and follow-on courses of action development, assists in determination of what established processes and procedures will need to become more automated. The COPSS will recommend areas for improvement, attend mission related forums and address emerging operational requirements, share emerging findings as they become known, complete and implement operations processes, maintain awareness of internal and external customer information needs and collaborate with other Intelligence Community members to produce plans, reports, and lessons learned.		
Computer Network Operations Planning Support Specialist 4	Supports various types of planning efforts in support of Computer Network Operations, most entail development of CNO requirements and/or providing actionable recommendations and technical support. This individual identifies, organizes, and documents steps to conduct CNO, which may include the development of long-term functional requirements, assists in the determination of risks and benefits when recommending actions to mitigate cyber threats, develops success criteria associated with CNO to be performed, and prepares assessments of CNO. The Computer Network Operations Planning Support Specialist (CNOPSS)performs multi-sours research of all U.S. exercises involving CNO to support operations personnel and overall CNO synchronization, assesses value and material compiled from research, documents objectives and benefits of each activity or plan based on available material, documents common NCO threads based on CNO activity, outlines key operations processes and metrics. This individual will also provide the means to assess the effects of mission partner execution of CNO, develop and document processes and procedures for assessing impact, Measure of Effectiveness, and follow-on courses of action development, assists in determination of what established processes and procedures will need to become more automated. The COPSS will recommend areas for improvement,	10	Bachelor's

	attend mission related forums and address emerging operational requirements, share emerging findings as they become known, complete and implement operations processes, maintain awareness of internal and external customer information needs and collaborate with other Intelligence Community members to produce plans, reports, and lessons learned.		
Network Engineer 1	The Network Engineer designs and plans network communications systems for firewalls and overall security posture. Provides specifications and detailed schematics for network architecture. Conducts cost/benefit analysis and provides specific detailed information for hardware and software selection, implementation techniques and tools for the most efficient solution to meet business needs, including present and future capacity requirements. Plans implementation of enhancements and upgrades to the network firewalls. Evaluates and reports on new communications technologies to enhance capabilities of the network. Presents configuration changes to the Firewall Advisory Board.	3	Bachelor's or Equivalent - Meets or exceeds current industry certification requirements.
Network Engineer 2	Applies advanced state-of-the-art networking concepts. Designs or develops testing that requires application of advanced theory. Evaluates, implements, and maintains local-, wide-, and metropolitan area networks to operate across all customer platforms. Resolves interoperability problems to obtain operations across all platforms, including e-mail, file transfers, multi-media, teleconferencing, etc. Supports acquisition of hardware and software, and subcontractor services.	5	Bachelor's or Equivalent - Meets or exceeds current industry certification requirements.
Network Engineer 3	Applies advanced, state-of-the-art networking concepts. Designs or develops testing that requires application of advanced theory. Designs, evaluates, implements, and maintains local-, wide-, and metropolitan area networks to operate across all customer platforms. Selects operating systems and protocol suites, and configures media with concentrators, bridges, and other devices. Resolves interoperability problems to obtain operations across all platforms, including e-mail, file transfers, multi-	8	Bachelor's or Equivalent - Meets or exceeds current industry certification requirements.

	media, teleconferencing, etc. Supports acquisition of hardware and software, and subcontractor services. May provide task direction to team members.		
Network Engineer 4	Applies advanced, state-of-the-art networking concepts. Designs or develops testing that requires application of advanced theory. Designs, evaluates, implements, and maintains local-, wide-, and metropolitan area networks to operate across all customer platforms. Selects operating systems and protocol suites, and configures media with concentrators, bridges, and other devices. Resolves interoperability problems to obtain operations across all platforms, including e-mail, file transfers, multi-media, teleconferencing, etc. Supports acquisition of hardware and software, and subcontractor services. Provides task direction to team members.	10	Bachelor's or Equivalent - Meets or exceeds current industry certification requirements.
Penetration Tester 1	Performs penetration testing on organizational information systems using both automated tools and manual methods to exploit identified weaknesses in applications, systems and networks. The individual conducts technical and physical social engineering activities to obtain unauthorized information disclosure while identifying human error and weakness in an organization. The individual is responsible for adhering to the developed test plan, rules of engagement, conducting system testing per pre-defined test cases, complete test reporting documentation, and recommending actions and strategies to mitigate known vulnerabilities and exploitation.	4 years of project related experience or 2 years with an Associates. Meets or exceeds current industry certification requirements.	Associates or Equivalent
Penetration Tester 2	Performs penetration testing on organizational information systems using both automated tools and manual methods to exploit identified weaknesses in applications, systems and networks. The Penetration Tester conducts extensive research and capitalizes on experience and skill to craft new exploitations, stress systems to achieve non-standard responses, and breech authorization boundaries mimics threat adversary capabilities, tactics, techniques, and procedures to attain information disclosure, root/administrative access, or other exploitation success. The individual conducts	6 years of project related experience or 3 years with an Associates. Meets or exceeds current industry certification requirements	Associates or Equivalent

	technical and physical social engineering activities to obtain unauthorized information disclosure while identifying human error and weakness in an organization. The individual is responsible for adhering to the developed test plan, rules of engagement, conducting system testing per pre-defined test cases, complete test reporting documentation, and recommending actions and strategies to mitigate known vulnerabilities and exploitation		
Penetration Tester 3	Performs penetration testing on organizational information systems using both automated tools and manual methods to exploit identified weaknesses in applications, systems and networks. The Penetration Tester conducts extensive research and capitalizes on experience and skill to craft new exploitations, stress systems to achieve non-standard responses, and breech authorization boundaries mimics threat adversary capabilities, tactics, techniques, and procedures to attain information disclosure, root/administrative access, or other exploitation success. The individual conducts technical and physical social engineering activities to obtain unauthorized information disclosure while identifying human error and weakness in an organization. The individual is responsible for adhering to the developed test plan, rules of engagement, conducting system testing per pre-defined test cases, complete test reporting documentation, and recommending actions and strategies to mitigate known vulnerabilities and exploitation. May provide direction to the team.	8 years of project related experience or 5 years with a Bachelors. Meets or exceeds current industry certification requirements	Bachelor's or Equivalent
Penetration Tester 4	Performs penetration testing on organizational information systems using both automated tools and manual methods to exploit identified weaknesses in applications, systems and networks. The Penetration Tester conducts extensive research and capitalizes on experience and skill to craft new exploitations, stress systems to achieve non-standard responses, and breech authorization boundaries mimics threat adversary capabilities, tactics, techniques, and procedures to attain information disclosure, root/administrative access, or other exploitation success. The individual conducts	10 years of project related experience or 6 years with a Bachelors. Meets or exceeds current industry certification requirements	Bachelor's or Equivalent

	technical and physical social engineering activities to obtain unauthorized information disclosure while identifying human error and weakness in an organization. The individual is responsible for adhering to the developed test plan, rules of engagement, conducting system testing per pre-defined test cases, complete test reporting documentation, and recommending actions and strategies to mitigate known vulnerabilities and exploitation. Provides direction to the team.		
Cyber Analyst 1	The Cyber Analyst is responsible for ensuring the organization's networks, as well as information is secure. The individual will employ continuous monitoring of intrusion detection/prevention and other perimeter defense devices. They will ensure appropriate data encryption (in transit and at rest) levels based on protection needs of targeted data. The Cyber Analyst maintains awareness of system/network security posture to include vulnerability scanning to facilitate application of quick and effective corrective measures, while ensuring configuration management requirements are met. Provides technical knowledge and information assurance analysis support, to include security assessment of applications, operating systems internet-facing interfaces, intranet, and other interconnections. The individual possesses strong knowledge of best practices associated with as well as appropriate authoritative guidance for physical and network security, security risk assessments, critical infrastructure protection, continuity and contingency planning, emergency preparedness, security awareness and training. Provide analysis of existing systems vulnerabilities including possible intrusion/entry points, resource manipulation, denial of service, and/or destruction of resources. Provide technical support and analysis to document organizational information protection framework, and support policy and procedures preparation and implementation.	3	Bachelor's or 3 years of additional relevant experience
Cyber Analyst 2	The Cyber Analyst is responsible for ensuring the organization's networks, as well as information is secure. The individual will employ	5	Bachelor's or 5 years of additional

	continuous monitoring of intrusion detection/prevention and other perimeter defense devices. They will ensure appropriate data encryption (in transit and at rest) levels based on protection needs of targeted data. The Cyber Analyst maintains awareness of system/network security posture to include vulnerability scanning to facilitate application of quick and effective corrective measures, while ensuring configuration management requirements are met. Provides technical knowledge and information assurance analysis support, to include security assessment of applications, operating systems internet-facing interfaces, intranet, and other interconnections. The individual possesses strong knowledge of best practices associated with as well as appropriate authoritative guidance for physical and network security, security risk assessments, critical infrastructure protection, continuity and contingency planning, emergency preparedness, security awareness and training. Provide analysis of existing systems vulnerabilities including possible intrusion/entry points, resource manipulation, denial of service, and/or destruction of resources. Provide technical support and analysis to document organizational information protection framework, and support policy and procedures preparation and implementation.		relevant experience
Cyber Analyst 3	The Cyber Analyst is responsible for ensuring the organization's networks, as well as information is secure. The individual will employ continuous monitoring of intrusion detection/prevention and other perimeter defense devices. They will ensure appropriate data encryption (in transit and at rest) levels based on protection needs of targeted data. The Cyber Analyst maintains awareness of system/network security posture to include vulnerability scanning to facilitate application of quick and effective corrective measures, while ensuring configuration management requirements are met. Provides technical knowledge and information assurance analysis support, to include security assessment of applications, operating systems internet-facing	7	Bachelor's or 7 years of additional relevant experience

	interfaces, intranet, and other interconnections. The individual possesses strong knowledge of best practices associated with as well as appropriate authoritative guidance for physical and network security, security risk assessments, critical infrastructure protection, continuity and contingency planning, emergency preparedness, security awareness and training. Provide analysis of existing systems vulnerabilities including possible intrusion/entry points, resource manipulation, denial of service, and/or destruction of resources. Provide technical support and analysis to document organizational information protection framework, and support policy and procedures preparation and implementation.		
Cyber Analyst 4	The Cyber Analyst is responsible for ensuring the organization's networks, as well as information is secure. The individual will employ continuous monitoring of intrusion detection/prevention and other perimeter defense devices. They will ensure appropriate data encryption (in transit and at rest) levels based on protection needs of targeted data. The Cyber Analyst maintains awareness of system/network security posture to include vulnerability scanning to facilitate application of quick and effective corrective measures, while ensuring configuration management requirements are met. Provides technical knowledge and information assurance analysis support, to include security assessment of applications, operating systems internet-facing interfaces, intranet, and other interconnections. The individual possesses strong knowledge of best practices associated with as well as appropriate authoritative guidance for physical and network security, security risk assessments, critical infrastructure protection, continuity and contingency planning, emergency preparedness, security awareness and training. Provide analysis of existing systems vulnerabilities including possible intrusion/entry points, resource manipulation, denial of service, and/or destruction of resources. Provide technical support and analysis to document organizational information protection framework,	10	Bachelor's or 10 years of additional relevant experience

	and support policy and procedures preparation and implementation.		

2. Maximum order:

SINs	Maximum Order
54151S	$500,000
54151HACS	$500,000
OLM	$250,000

3. Minimum order: $100

4. Geographic coverage (delivery area). 48 contiguous states, Alaska, Hawaii, Washington D.C., Puerto Rico, U.S. Territories, and to a port or consolidation point within the aforementioned locations for orders that are received from overseas activities.

5. Point(s) of production (city, county, and State or foreign country). 11817 Canon Blvd, Newport News, VA 23606-2569

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

7. Quantity discounts. 1% on orders over $1,000,000.00

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

9. Foreign items (list items by country of origin). Not Applicable

10a. Time of delivery. (Contractor insert number of days.) To Be Determined at the Task Order level

10b. Expedited Delivery. Items available for expedited delivery are noted in this price list. Contact Contractor

10c. Overnight and 2-day delivery. Contact Contractor

10d. Urgent Requirements. Contact Contractor

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

12a. Ordering address(es). 11817 Canon Blvd, Newport News, VA 23606-2569

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(es). 11817 Canon Blvd, Newport News, VA 23606-2569

14. Warranty provision. Standard Commercial Warranty Terms & Conditions

15. Export packing charges, if applicable. Not Applicable

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

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

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

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

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

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

21. Preventive maintenance (if applicable). Not Applicable

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). Not Applicable

22b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor's website or other location.) The EIT standards can be found at: www.Section508.gov/.
Not Applicable

23. Unique Entity Identifier (UEI) number. 079459870

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

Price List:

SIN 54151S:

Gov't Site

Labor Category	7/9/18-7/8/19 GSA Rate w/IFF	7/9/19-7/8/20 GSA Rate w/IFF	7/9/20-7/8/21 GSA Rate w/IFF	7/9/21-7/8/22 GSA Rate w/IFF	7/9/22-7/8/23 GSA Rate w/IFF
Subject Matter Expert Level 1	*$91.07*	*$93.35*	*$95.68*	*$98.07*	*$100.52*
Subject Matter Expert Level 2	*$102.95*	*$105.52*	*$108.16*	*$110.86*	*$113.63*
Subject Matter Expert Level 3	*$115.82*	*$118.72*	*$121.69*	*$124.73*	*$127.85*
Subject Matter Expert Level 4	*$124.74*	*$127.86*	*$131.06*	*$134.34*	*$137.70*
Subject Matter Expert Level 5	*$143.54*	*$147.13*	*$150.81*	*$154.58*	*$158.44*
Software Developer Level 1	*$82.37*	*$84.43*	*$86.54*	*$88.70*	*$90.92*
Software Developer Level 2	*$107.08*	*$109.76*	*$112.50*	*$115.31*	*$118.19*
Software Developer Level 3	*$115.08*	*$117.96*	*$120.91*	*$123.93*	*$127.03*
Software Developer Level 4	*$141.37*	*$144.90*	*$148.52*	*$152.23*	*$156.04*
Software Developer Level 5	*$177.85*	*$182.30*	*$186.86*	*$191.53*	*$196.32*

System Administrator Level 1	*$74.25*	*$76.11*	*$78.01*	*$79.96*	*$81.96*
System Administrator Level 2	*$82.66*	*$84.73*	*$86.85*	*$89.02*	*$91.25*
System Administrator Level 3	*$86.13*	*$88.28*	*$90.49*	*$92.75*	*$95.07*
System Administrator Level 4	*$97.45*	*$99.89*	*$102.39*	*$104.95*	*$107.57*
System Administrator Level 5	*$110.92*	*$113.69*	*$116.53*	*$119.44*	*$122.43*
IT Engineer Level 1	*$81.18*	*$83.21*	*$85.29*	*$87.42*	*$89.61*
IT Engineer Level 2	*$99.98*	*$102.48*	*$105.04*	*$107.67*	*$110.36*
IT Engineer Level 3	*$107.90*	*$110.60*	*$113.37*	*$116.20*	*$119.11*
IT Engineer Level 4	*$117.80*	*$120.75*	*$123.77*	*$126.86*	*$130.03*
IT Engineer Level 5	*$132.85*	*$136.17*	*$139.57*	*$143.06*	*$146.64*
IT Analyst Level 1	*$81.18*	*$83.21*	*$85.29*	*$87.42*	*$89.61*
IT Analyst Level 2	*$99.98*	*$102.48*	*$105.04*	*$107.67*	*$110.36*
IT Analyst Level 3	*$107.90*	*$110.60*	*$113.37*	*$116.20*	*$119.11*
IT Analyst Level 4	*$117.80*	*$120.75*	*$123.77*	*$126.86*	*$130.03*
IT Analyst Level 5	*$132.85*	*$136.17*	*$139.57*	*$143.06*	*$146.64*

Contractor Site

Labor Category	7/9/18-7/8/19 GSA Rate w/IFF	7/9/19-7/8/20 GSA Rate w/IFF	7/9/20-7/8/21 GSA Rate w/IFF	7/9/21-7/8/22 GSA Rate w/IFF	7/9/22-7/8/23 GSA Rate w/IFF
Subject Matter Expert Level 1	*$100.18*	*$102.68*	*$105.25*	*$107.88*	*$110.58*

Subject Matter Expert Level 2	*$113.25*	*$116.08*	*$118.98*	*$121.95*	*$125.00*
Subject Matter Expert Level 3	*$125.23*	*$128.36*	*$131.57*	*$134.86*	*$138.23*
Subject Matter Expert Level 4	*$137.20*	*$140.63*	*$144.15*	*$147.75*	*$151.44*
Subject Matter Expert Level 5	*$157.89*	*$161.84*	*$165.89*	*$170.04*	*$174.29*
Software Developer Level 1	*$94.73*	*$97.10*	*$99.53*	*$102.02*	*$104.57*
Software Developer Level 2	*$123.14*	*$126.22*	*$129.38*	*$132.61*	*$135.93*
Software Developer Level 3	*$132.77*	*$136.09*	*$139.49*	*$142.98*	*$146.55*
Software Developer Level 4	*$162.58*	*$166.64*	*$170.81*	*$175.08*	*$179.46*
Software Developer Level 5	*$204.52*	*$209.63*	*$214.87*	*$220.24*	*$225.75*
System Administrator Level 1	*$85.38*	*$87.51*	*$89.70*	*$91.94*	*$94.24*
System Administrator Level 2	*$95.05*	*$97.43*	*$99.87*	*$102.37*	*$104.93*
System Administrator Level 3	*$99.61*	*$102.10*	*$104.65*	*$107.27*	*$109.95*
System Administrator Level 4	*$112.06*	*$114.86*	*$117.73*	*$120.67*	*$123.69*
System Administrator Level 5	*$127.56*	*$130.75*	*$134.02*	*$137.37*	*$140.80*

IT Engineer Level 1	*$93.35*	*$95.68*	*$98.07*	*$100.52*	*$103.03*
IT Engineer Level 2	*$116.12*	*$119.02*	*$122.00*	*$125.05*	*$128.18*
IT Engineer Level 3	*$124.09*	*$127.19*	*$130.37*	*$133.63*	*$136.97*
IT Engineer Level 4	*$135.48*	*$138.87*	*$142.34*	*$145.90*	*$149.55*
IT Engineer Level 5	*$152.78*	*$156.60*	*$160.52*	*$164.53*	*$168.64*
IT Analyst Level 1	*$93.35*	*$95.68*	*$98.07*	*$100.52*	*$103.03*
IT Analyst Level 2	*$116.12*	*$119.02*	*$122.00*	*$125.05*	*$128.18*
IT Analyst Level 3	*$124.09*	*$127.19*	*$130.37*	*$133.63*	*$136.97*
IT Analyst Level 4	*$135.48*	*$138.87*	*$142.34*	*$145.90*	*$149.55*
IT Analyst Level 5	*$152.78*	*$156.60*	*$160.52*	*$164.53*	*$168.64*

SIN 54151HACS:

Customers Site

Labor Category	7/9/18-7/8/19 GSA Rate w/IFF	7/9/19-7/8/20 GSA Rate w/IFF	7/9/20-7/8/21 GSA Rate w/IFF	7/9/21-7/8/22 GSA Rate w/IFF	7/9/22-7/8/23 GSA Rate w/IFF
Subject Matter Expert 1	*N/A*	*N/A*	*N/A*	*$184.54*	*$189.15*
Subject Matter Expert 2	*N/A*	*N/A*	*N/A*	*$194.44*	*$199.30*
Subject Matter Expert 3	*N/A*	*N/A*	*N/A*	*$204.34*	*$209.45*
Subject Matter Expert 4	*N/A*	*N/A*	*N/A*	*$214.24*	*$219.60*
Incident Response Analyst 1	*N/A*	*N/A*	*N/A*	*$100.40*	*$102.91*
Incident Response Analyst 2	*N/A*	*N/A*	*N/A*	*$117.82*	*$120.77*
Incident Response Analyst 3	*N/A*	*N/A*	*N/A*	*$149.03*	*$152.76*
Incident Response Analyst 4	*N/A*	*N/A*	*N/A*	*$165.58*	*$169.72*
Cyber Security Engineer 1	*N/A*	*N/A*	*N/A*	*$103.29*	*$105.87*
Cyber Security Engineer 2	*N/A*	*N/A*	*N/A*	*$131.90*	*$135.20*
Cyber Security Engineer 3	*N/A*	*N/A*	*N/A*	*$164.94*	*$169.06*
Cyber Security Engineer 4	*N/A*	*N/A*	*N/A*	*$202.02*	*$207.07*
Cyber Security Architect 1	*N/A*	*N/A*	*N/A*	*$102.80*	*$105.37*
Cyber Security Architect 2	*N/A*	*N/A*	*N/A*	*$131.97*	*$135.27*

Cyber Security Architect 3	*N/A*	*N/A*	*N/A*	*$163.57*	*$167.66*
Cyber Security Architect 4	*N/A*	*N/A*	*N/A*	*$202.81*	*$207.88*
Threat Hunt Analyst 1	*N/A*	*N/A*	*N/A*	*$100.40*	*$102.91*
Threat Hunt Analyst 2	*N/A*	*N/A*	*N/A*	*$117.82*	*$120.77*
Threat Hunt Analyst 3	*N/A*	*N/A*	*N/A*	*$149.03*	*$152.76*
Threat Hunt Analyst 4	*N/A*	*N/A*	*N/A*	*$165.58*	*$169.72*
Cyber Threat Intelligence Analyst 1	*N/A*	*N/A*	*N/A*	*$92.45*	*$94.76*
Cyber Threat Intelligence Analyst 2	*N/A*	*N/A*	*N/A*	*$110.86*	*$113.63*
Cyber Threat Intelligence Analyst 3	*N/A*	*N/A*	*N/A*	*$135.26*	*$138.64*
Cyber Threat Intelligence Analyst 4	*N/A*	*N/A*	*N/A*	*$161.85*	*$165.90*
Vulnerability Assessment Analyst 1	*N/A*	*N/A*	*N/A*	*$100.40*	*$102.91*
Vulnerability Assessment Analyst 2	*N/A*	*N/A*	*N/A*	*$117.82*	*$120.77*
Vulnerability Assessment Analyst 3	*N/A*	*N/A*	*N/A*	*$149.03*	*$152.76*
Vulnerability Assessment Analyst 4	*N/A*	*N/A*	*N/A*	*$165.58*	*$169.72*
Risk Analyst 1	*N/A*	*N/A*	*N/A*	*$100.40*	*$102.91*
Risk Analyst 2	*N/A*	*N/A*	*N/A*	*$117.82*	*$120.77*
Risk Analyst 3	*N/A*	*N/A*	*N/A*	*$165.58*	*$169.72*
Risk Analyst 4	*N/A*	*N/A*	*N/A*	*$175.49*	*$179.88*
Forensic Analyst 1	*N/A*	*N/A*	*N/A*	*$134.59*	*$137.95*
Forensic Analyst 2	*N/A*	*N/A*	*N/A*	*$144.49*	*$148.10*
Forensic Analyst 3	*N/A*	*N/A*	*N/A*	*$154.39*	*$158.25*
Forensic Analyst 4	*N/A*	*N/A*	*N/A*	*$164.29*	*$168.40*
Computer Network Operations Planning Support Specialist 1	*N/A*	*N/A*	*N/A*	*$136.75*	*$140.17*
Computer Network Operations Planning Support Specialist 2	*N/A*	*N/A*	*N/A*	*$158.67*	*$162.64*
Computer Network Operations Planning Support Specialist 3	*N/A*	*N/A*	*N/A*	*$168.57*	*$172.78*
Computer Network Operations Planning Support Specialist 4	*N/A*	*N/A*	*N/A*	*$178.47*	*$182.93*
Network Engineer 1	*N/A*	*N/A*	*N/A*	*$97.40*	*$99.84*
Network Engineer 2	*N/A*	*N/A*	*N/A*	*$119.29*	*$122.27*
Network Engineer 3	*N/A*	*N/A*	*N/A*	*$168.17*	*$172.37*
Network Engineer 4	*N/A*	*N/A*	*N/A*	*$178.47*	*$182.93*
Penetration Tester 1	*N/A*	*N/A*	*N/A*	*$100.40*	*$102.91*
Penetration Tester 2	*N/A*	*N/A*	*N/A*	*$117.82*	*$120.77*
Penetration Tester 3	*N/A*	*N/A*	*N/A*	*$149.03*	*$152.76*
Penetration Tester 4	*N/A*	*N/A*	*N/A*	*$165.58*	*$169.72*
Cyber Analyst 1	*N/A*	*N/A*	*N/A*	*$113.76*	*$116.60*
Cyber Analyst 2	*N/A*	*N/A*	*N/A*	*$138.25*	*$141.71*
Cyber Analyst 3	*N/A*	*N/A*	*N/A*	*$148.14*	*$151.84*
Cyber Analyst 4	*N/A*	*N/A*	*N/A*	*$174.32*	*$178.68*

Contractor Site

Labor Category	7/9/18-7/8/19 GSA Rate w/IFF	7/9/19-7/8/20 GSA Rate w/IFF	7/9/20-7/8/21 GSA Rate w/IFF	7/9/21-7/8/22 GSA Rate w/IFF	7/9/22-7/8/23 GSA Rate w/IFF
Subject Matter Expert 1	*N/A*	*N/A*	*N/A*	$202.99	*$208.06*
Subject Matter Expert 2	*N/A*	*N/A*	*N/A*	$213.88	*$219.23*
Subject Matter Expert 3	*N/A*	*N/A*	*N/A*	$224.78	*$230.40*
Subject Matter Expert 4	*N/A*	*N/A*	*N/A*	$235.67	*$241.56*
Incident Response Analyst 1	*N/A*	*N/A*	*N/A*	$110.44	*$113.20*
Incident Response Analyst 2	*N/A*	*N/A*	*N/A*	$129.60	*$132.84*
Incident Response Analyst 3	*N/A*	*N/A*	*N/A*	$163.93	*$168.03*
Incident Response Analyst 4	*N/A*	*N/A*	*N/A*	$182.15	*$186.70*
Cyber Security Engineer 1	*N/A*	*N/A*	*N/A*	$113.63	*$116.47*
Cyber Security Engineer 2	*N/A*	*N/A*	*N/A*	$145.09	*$148.72*
Cyber Security Engineer 3	*N/A*	*N/A*	*N/A*	$181.43	*$185.97*
Cyber Security Engineer 4	*N/A*	*N/A*	*N/A*	$222.22	*$227.78*
Cyber Security Architect 1	*N/A*	*N/A*	*N/A*	$113.09	*$115.92*
Cyber Security Architect 2	*N/A*	*N/A*	*N/A*	$145.16	*$148.79*
Cyber Security Architect 3	*N/A*	*N/A*	*N/A*	$179.92	*$184.42*
Cyber Security Architect 4	*N/A*	*N/A*	*N/A*	$223.09	*$228.67*
Threat Hunt Analyst 1	*N/A*	*N/A*	*N/A*	$110.44	*$113.20*
Threat Hunt Analyst 2	*N/A*	*N/A*	*N/A*	$129.60	*$132.84*
Threat Hunt Analyst 3	*N/A*	*N/A*	*N/A*	$163.93	*$168.03*
Threat Hunt Analyst 4	*N/A*	*N/A*	*N/A*	$182.15	*$186.70*
Cyber Threat Intelligence Analyst 1	*N/A*	*N/A*	*N/A*	$101.69	*$104.23*
Cyber Threat Intelligence Analyst 2	*N/A*	*N/A*	*N/A*	$121.94	*$124.99*
Cyber Threat Intelligence Analyst 3	*N/A*	*N/A*	*N/A*	$148.79	*$152.51*
Cyber Threat Intelligence Analyst 4	*N/A*	*N/A*	*N/A*	$178.04	*$182.49*
Vulnerability Assessment Analyst 1	*N/A*	*N/A*	*N/A*	$110.44	*$113.20*
Vulnerability Assessment Analyst 2	*N/A*	*N/A*	*N/A*	$129.60	*$132.84*
Vulnerability Assessment Analyst 3	*N/A*	*N/A*	*N/A*	$163.93	*$168.03*
Vulnerability Assessment Analyst 4	*N/A*	*N/A*	*N/A*	$182.15	*$186.70*
Risk Analyst 1	*N/A*	*N/A*	*N/A*	$110.44	*$113.20*
Risk Analyst 2	*N/A*	*N/A*	*N/A*	$129.60	*$132.84*
Risk Analyst 3	*N/A*	*N/A*	*N/A*	$182.15	*$186.70*
Risk Analyst 4	*N/A*	*N/A*	*N/A*	$193.03	*$197.86*
Forensic Analyst 1	*N/A*	*N/A*	*N/A*	$148.05	*$151.75*
Forensic Analyst 2	*N/A*	*N/A*	*N/A*	$158.94	*$162.91*
Forensic Analyst 3	*N/A*	*N/A*	*N/A*	$169.82	*$174.07*

Forensic Analyst 4	*N/A*	*N/A*	*N/A*	$180.72	*$185.24*
Computer Network Operations Planning Support Specialist 1	*N/A*	*N/A*	*N/A*	$150.42	*$154.18*
Computer Network Operations Planning Support Specialist 2	*N/A*	*N/A*	*N/A*	$174.54	*$178.90*
Computer Network Operations Planning Support Specialist 3	*N/A*	*N/A*	*N/A*	$185.43	*$190.07*
Computer Network Operations Planning Support Specialist 4	*N/A*	*N/A*	*N/A*	$196.32	*$201.23*
Network Engineer 1	*N/A*	*N/A*	*N/A*	$107.13	*$109.81*
Network Engineer 2	*N/A*	*N/A*	*N/A*	$131.22	*$134.50*
Network Engineer 3	*N/A*	*N/A*	*N/A*	$184.99	*$189.61*
Network Engineer 4	*N/A*	*N/A*	*N/A*	$196.31	*$201.22*
Penetration Tester 1	*N/A*	*N/A*	*N/A*	$110.44	*$113.20*
Penetration Tester 2	*N/A*	*N/A*	*N/A*	$129.60	*$132.84*
Penetration Tester 3	*N/A*	*N/A*	*N/A*	$163.93	*$168.03*
Penetration Tester 4	*N/A*	*N/A*	*N/A*	$182.15	*$186.70*
Cyber Analyst 1	*N/A*	*N/A*	*N/A*	$125.14	*$128.27*
Cyber Analyst 2	*N/A*	*N/A*	*N/A*	$152.07	*$155.87*
Cyber Analyst 3	*N/A*	*N/A*	*N/A*	$162.95	*$167.02*
Cyber Analyst 4	*N/A*	*N/A*	*N/A*	$191.75	*$196.54*

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