

# **BLACKWATCH** INTERNATIONAL

## **GENERAL SERVICES ADMINISTRATION Federal Supply Service Authorized 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: GSAAvantage.gov.

### **MULTIPLE AWARD SCHEDULE (MAS)**

#### **Information Technology Category IT Professional Services**

**BLACKWATCH International  
1430 Spring Hill Road, STE 205  
McLean, VA 22102  
Phone: 571-395-8403  
Fax: 571-565-3756**

**Website: <http://www.blackwatchintel.com/>  
Email: [JOffutt@blackwatchintel.com](mailto:JOffutt@blackwatchintel.com)**

Contract Number: 47QTCA20D003Y

Period Covered by Contract: **October 1, 2019 through September 30, 2024**  
*Catalog effective through Mass Modification #PS-0005, dated February 7, 2022.*

#### *Small Business*

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at [fss.gsa.gov](http://fss.gsa.gov).



**INFORMATION FOR ORDERING ACTIVITIES:**

**1a. Table of Awarded Special Item Numbers (SINs)**

<u>SIN</u>	<u>DESCRIPTION</u>
54151S/STLOC/RC	IT Professional Services
54151HACS/STLOC/RC	Highly Adaptive Cybersecurity Services

**1b. Lowest Priced Model Number:** Not Applicable

**1b. Lowest Hourly Rate:** See pricelist

**2. Maximum order:** \$500,000.00

**3. Minimum order:** \$100.00

**4. Geographic coverage (delivery area):** Domestic

**5. Point(s) of production (city, county, and State or foreign country):** Not applicable

**6. Discount from list prices or statement of net price:** Prices shown are NET prices, basic discounts have been deducted.

**7. Quantity discounts:** None.

**8. Prompt payment terms:** Net 30 Days

Note: Prompt payment terms must be followed by the statement "Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions."

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

**10a. Time of delivery:** As agreed per task order.

**10b. Expedited Delivery:** As agreed per task order.

**10c. Overnight and 2-day delivery:** Not Applicable

**10d. Urgent Requirements:** When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

**11. F.O.B.:** Destination

**12a. Ordering address:**

BLACKWATCH International  
1430 Spring Hill Road, STE 205  
McLean, VA 22102

**12b. Ordering procedures:** Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's), and a sample BPA are found in Federal Acquisition Regulation (FAR) 8.405-3.

**13. Payment address:**

BLACKWATCH International  
1430 Spring Hill Road, STE 205  
McLean, VA 22102

**14. Warranty provision:** Standard Commercial Warranty

**15. Export packing charges:** Not Applicable

**16. Terms and conditions of rental, maintenance, and repair:** Not Applicable

**17. Terms and conditions of installation:** Not Applicable

**18. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices:** Not Applicable

**19. Terms and conditions for any other services:** Not Applicable

**20. List of service and distribution points:** Not Applicable

**21. List of participating dealers:** Not Applicable

**22. Preventive maintenance:** Not Applicable

**23a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants):** Not Applicable

**23b. Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services.** The EIT standards can be found at: [www.Section508.gov/](http://www.Section508.gov/).

**24. Unique Entity Identifier (UEI) number:** 962185513

**25. Notification regarding registration in the System for Award Management (SAM) database.** BLACKWATCH International is registered in the SAM database. The Cage code is 628B2.

## GSA PRICELIST

Labor Category	GSA Price 10/1/21 -9/30/22	GSA Price 10/1/22 -9/30/23	GSA Price 10/1/23 -9/30/24
<b>SIN 54151S – IT Professional Services</b>			
Cybersecurity Specialist	\$106.99	\$109.45	\$111.97
Database Developer /Administrator	\$113.96	\$116.58	\$119.27
Information Systems Security Officer (ISSO)	\$147.54	\$150.94	\$154.41
IT Help Desk Specialist	\$68.71	\$70.29	\$71.91
Mid-Level Cybersecurity Specialist	\$120.07	\$122.83	\$125.66
Mid-Level SharePoint Developer /Administrator	\$130.24	\$133.24	\$136.30
Mobile Device Specialist	\$76.31	\$78.07	\$79.87
Network /Hardware Specialist	\$76.31	\$78.07	\$79.87
Network /Hardware Support Technician	\$61.05	\$62.46	\$63.89
Network Administrator	\$89.54	\$91.60	\$93.71
Program/Project Manager	\$136.83	\$139.97	\$143.19
Programmer	\$104.49	\$106.89	\$109.35
Senior Cybersecurity Engineer	\$138.18	\$141.36	\$144.61
Senior Cybersecurity Specialist	\$135.33	\$138.44	\$141.63
Senior Network Administrator	\$140.93	\$144.17	\$147.49
Senior Program/Project Manager	\$143.47	\$146.77	\$150.15
Senior Software Solutions Architect	\$156.70	\$160.30	\$163.99
Senior Systems Administrator	\$136.83	\$139.97	\$143.19
Senior Technical/Task Lead	\$136.83	\$139.97	\$143.19
Systems Administrator	\$96.67	\$98.89	\$101.16
Systems Analyst I	\$66.71	\$68.24	\$69.81
UNIX / Linux Solutions Architect	\$143.47	\$146.77	\$150.15
<b>SIN 54151HACS – Highly Adaptive Cybersecurity Services</b>			
Cyber Security Program Manager Level I	\$156.59	\$160.19	\$163.87
Cyber Security Project Manager Level I	\$131.30	\$134.32	\$137.41
Cyber Security Project Manager Level II	\$143.24	\$146.53	\$149.90
Cyber Security Project Manager Level III	\$163.62	\$167.38	\$171.23
Cyber Security Specialist Level I	\$102.24	\$104.59	\$106.99
Cyber Security Specialist Level II	\$111.72	\$114.29	\$116.91
Cyber Security Specialist Level III	\$125.33	\$128.21	\$131.16
Cyber Security Specialist Level IV	\$139.01	\$142.21	\$145.48
Cyber Security Specialist Level V	\$262.60	\$268.64	\$274.82
Cyber Systems Administrator Level I	\$65.16	\$66.66	\$68.19
Cyber Systems Administrator Level II	\$111.72	\$114.29	\$116.91
Cyber Systems Administrator Level III	\$119.36	\$122.10	\$124.91
Cyber Systems Administrator Level IV	\$127.07	\$129.99	\$132.98
Cyber Systems Administrator Level V	\$142.87	\$146.15	\$149.52
Cyber Systems Architect III	\$160.73	\$164.43	\$168.21
Cyber Security Analyst Level I	\$60.81	\$62.21	\$63.64
Cyber Security Analyst Level II	\$84.26	\$86.20	\$88.18
Cyber Security Analyst Level III	\$105.64	\$108.07	\$110.55
Cyber Security Analyst Level IV	\$130.25	\$133.24	\$136.31
Cyber Security Engineer Level I	\$103.27	\$105.64	\$108.07
Cyber Security Engineer Level II	\$132.04	\$135.07	\$138.18
Cyber Security Engineer Level III	\$154.22	\$157.77	\$161.40
Cyber Security Test Specialist Level II	\$172.82	\$176.80	\$180.87

## LABOR CATEGORY DESCRIPTIONS

### SIN 54151S – IT Professional Services

Labor Category	Description	Minimum Experience	Education Requirements
Cybersecurity Specialist	Performs IT security, information assurance (IA), cybersecurity and IT compliance support; participates in the day-to-day cybersecurity effort with assistance and guidance from more senior cybersecurity team members, as needed; implements DoD 8500 series and NIST 800 series policy/guidance; possesses good IT skills and working knowledge of hardware, software and networks; assesses security flaws of information systems and devices under supervision; possesses solid troubleshooting skills and meticulous attention to detail; conducts research into a wide range of IT security issues when directed; possesses some experience with HBSS, ACAS, SCAP, STIGs, IAVA notices, eMASS, RMF and vulnerability management; has excellent oral and written communication skills and exceptional interpersonal skills, with an emphasis on listening and questioning.	Three (3) years or more of increasingly complex and progressive experience in Department of Defense (DoD) IT security, information assurance (IA), cybersecurity and/or IT compliance support.	Associate's degree from an accredited college or university in any science, business, engineering or technology discipline.
Database Developer / Administrator	Performs planning, analyzing, designing, developing, testing and implementing of database systems and applications; skilled in logical and physical modeling; accomplishes performance and tuning tasks; configures and maintains the database environment; installs, maintains, and patches database servers and application software tools; performs database upgrades, backups and restores; configures, optimizes, and supports relational databases; develops and maintains web interfaces to database information; works with users to identify and develop system requirement; analyzes user needs to develop solutions; frequently interacts with the client, system and network team members.	Four (4) years of increasingly complex and progressive experience in Department of Defense (DoD) IT programming, database development and administration.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.
Information Systems Security Officer (ISSO)	Performs research, develops, implements, tests and reviews the organization's information security to protect information and prevent unauthorized access; serves as the principal advisor to the Information System Owner (SO), Business Process Owner, and the Information System Security Manager (ISSM) on all matters, technical and otherwise, involving the security of the information system; ensures the implementation and maintenance of security controls in accordance with the Security Plan (SP); informs users about security measures, explains potential threats, installs software, implements security measures and monitors networks; provides guidance, oversight, and expertise, but doesn't accomplish all functions without assistance; delegates, coordinates, facilitates, or otherwise ensures required activities are accomplished.	Eight (8) years of increasingly complex and progressive experience in Department of Defense (DoD) IT security, information assurance (IA), cybersecurity and/or IT compliance support.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.
IT Help Desk Specialist	Performs technical assistance and support related to computer systems, hardware, or software; provides courteous and accurate technical information and support in a timely, efficient and professional manner; responds to queries, runs diagnostic programs, isolates problems, and determines and implements solutions; provides phone, email, web, and in-person support to users in the areas of e-mail, directories, computer operating systems, desktop applications for all types of computer systems, and applications developed or deployed under this contract. Serve as the first point of contact for troubleshooting hardware/software, all types of computer systems and printer problems.	One (1) year of increasingly complex and progressive experience in Department of Defense (DoD) IT hardware installation and troubleshooting support.	High School Diploma or equivalent.

Labor Category	Description	Minimum Experience	Education Requirements
Mid-Level Cybersecurity Specialist	Performs IT security, information assurance (IA), cybersecurity and IT compliance support; participates in the day-to-day cybersecurity effort and provides assistance and guidance to other more junior cybersecurity team members; implements DoD 8500 series and NIST 800 series policy/guidance; possesses strong IT skills and knowledge including hardware, software and networks; assesses security flaws of information systems and devices; possesses solid troubleshooting skills and meticulous attention to detail; conducts research into a wide range of IT security issues; seeks out vulnerabilities in IT infrastructures; possesses experience with HBSS, ACAS, SCAP, STIGs, IAVA notices, eMASS, RMF and vulnerability management; has excellent oral and written communication skills and exceptional interpersonal skills, with an emphasis on listening and questioning.	Five (5) years of increasingly complex and progressive experience in Department of Defense (DoD) IT security, information assurance (IA), cybersecurity and/or IT compliance support.	Associate's degree from an accredited college or university in any science, business, engineering or technology discipline.
Mid-Level SharePoint Developer / Administrator	Performs the planning, designing, troubleshooting and supporting of SharePoint solutions; experienced in developing SharePoint applications using customization and configuration techniques; works directly with client to assess the current environment, develop requirements and solutions using out-of-the box SharePoint features and design solutions which extend SharePoint through various customization techniques; designs solutions based on established patterns and best practices around Content Management, User Adoption, Governance and Change Management; creates SharePoint workflows in compliance with established Governance policies; validates functional and technical requirements with the relevant business and IT stakeholders.	Six (6) years of increasingly complex and progressive experience in Department of Defense (DoD) IT application development and/or systems administration. Two (2) years must have been in a SharePoint SME role.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.
Mobile Device Specialist	Performs the configuration and installation of end user devices used on wireless network architectures, including laptops, cellular phones and tablets; experienced with configuration and deployment of end user devices in a large Enterprise environment, including provisioning, patching and updates, certificate configuration, equipment inventory and tracking and STIG compliance; demonstrates strong working knowledge of wireless network operation and security, 802.1X/802.11 standards, and WPA Enterprise encryption, VPN client software and VPN concentrators, RSA and ECDHA digital certificates used to authenticate users and user devices, and implementing and managing a certificate authority for PKI.	Three (3) years of increasingly complex and progressive experience in Department of Defense (DoD) IT wireless environment. One (1) years' experience working with Android and iOS operating system configuration and operation.	Associate's degree from an accredited college in any science, business, engineering technology discipline.
Network /Hardware Specialist	Performs hardware, software, and network support utilizing hardware and software testing tools and techniques; assists with installation of terminals and associated hardware; tests, debugs and writes documentation as required; provides client support setting up PCs and peripherals and/or installing software packages; provides user training for hardware/software products; identifies problems and resolves hardware/software/network malfunctions; performs minor hardware/software/network maintenance such as board replacement, cable switching, communication assistance, hardware installation/replacement; interfaces with mainframe, CAD/CAM, digitizers, networks, and provides analysis support.	Two (2) years of increasingly complex and progressive experience in Department of Defense (DoD) IT hardware installation and troubleshooting support.	Associate's degree from an accredited college in any science, business, engineering technology discipline.
Network /Hardware Support Technician	Performs repair and/or replace activities on all computer systems and servers; supports the installation, set-up and maintenance of workstations, peripherals, and cabling; ensures systems are configured correctly and are running efficiently using hardware	One (1) year of increasingly complex and progressive experience in	High School Diploma or equivalent.

Labor Category	Description	Minimum Experience	Education Requirements
	and software testing tools and techniques; builds systems and servers, installs and patches operating systems, software and applications; configures software and drivers; performs regular system upgrades; diagnoses and repairs hardware and software issues; coordinates with client on all tracking and changes to hardware inventory; provides client training in the use of hardware, software, and/or network products; assists help desk by responding to requests for assistance when needed.	Department of Defense (DoD) IT hardware installation and troubleshooting support.	
Network Administrator	Performs a variety of network management functions related to the operation, performance or availability of data communications networks; accomplishes the installation, implementation, troubleshooting, and maintenance of agency wide-area networks (WANs) and local-area networks (LANs); performs day-to-day network administration; has experience with cable/LAN meters, protocol analyzers, SNMP and RMON based software products; has working knowledge of Ethernet, network operating systems, FDDI and high-speed WANs and routers; analyzes client LANs/WANs, isolates source of problems and recommends solutions; modifies command language programs, network start up files and participates in load balancing efforts to achieve optimum device utilization and performance; establishes new user accounts granting access to required network files and programs; manages network E-mail functions; establishes mail boxes and monitors mail performance on the network; troubleshoots network/user problems, presents resolutions for implementation; prepares a variety of network resource reports.	Four (4) years of increasingly complex and progressive experience in Department of Defense (DoD) IT network administration support.	Associate's degree from an accredited college or university in any science, business, engineering or technology discipline.
Program/Project Manager	Performs management activities for all aspects of one or more complex projects; provides on-site leadership for assigned project teams; develops and manages all aspects of project engagement including planning, communications, resources, execution, budget, change, risks and issues and closure; participates in establishing practices, templates, policies and tools; prepares estimates and detailed project plans for all phases of projects; ensures adequate resources to achieve project objectives in planned timeframes; monitors staff performance and completes performance reviews; provides leadership and stakeholders with status reporting, success criteria results and metrics regarding project milestones, deliverables, dependencies and risks; sets and continually manages project expectations; monitors, tracks and controls outcomes to resolve issues, conflicts, dependencies and critical path deliverables.	Six (6) years of increasingly complex and progressive experience in Department of Defense (DoD) IT project management. Four (4) years must have been in a Program/Project Manager role.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline. Active (PMI) Project Management Professional (PMP) certification required.
Programmer	Performs analysis of functional business applications and design specifications for functional areas such as production, payroll, logistics, and contracts; develops block diagrams and logic flow charts; translates detailed design requirements into computer software; creates and/or maintains operating systems, communications software, database packages, compilers, assemblers, and utility programs; modifies existing software and creates special-purpose software to ensure efficiency and integrity between systems and applications; tests, debugs, and refines computer software to produce the required product; prepares required program-level and user-level documentation;	Four (4) years of increasingly complex and progressive experience in Department of Defense (DoD) IT programming.	Associate's degree from an accredited college or university in any science, business, engineering or technology discipline.

Labor Category	Description	Minimum Experience	Education Requirements
	demonstrates the ability to work independently or under only general direction.		
Senior Cybersecurity Engineer	Performs a number of IT security functions from ensuring the security of software, through developing, testing and deploying broader network security systems; understands complex cybersecurity issues and provides subject matter expertise within a fast-paced technical environment; accomplishes and monitors a thorough risk assessment to identify current and emerging technology issues including security trends, vulnerabilities and threats; conducts proactive research to analyze security weaknesses and recommend appropriate strategies; provides guidance to cybersecurity team on implementing new security solutions to better protect the organization; possesses outstanding communication skills and the ability to translate complex IT concepts to stakeholders that don't have a strong IT background.	Eight (8) years of increasingly complex and progressive experience in Department of Defense (DoD) IT security, information assurance (IA), cybersecurity and/or IT compliance support.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.
Senior Cybersecurity Specialist	Performs IT security, information assurance (IA), cybersecurity and IT compliance support; leads the day-to-day cybersecurity effort and provides assistance and guidance to other more junior cybersecurity team members; brings experience implementing DoD 8500 series and NIST 800 series policy/guidance; possesses strong IT skills and knowledge including hardware, software and networks; assesses security flaws of information systems and devices; possesses solid troubleshooting skills and meticulous attention to detail; conducts research into a wide range of IT security issues; seeks out vulnerabilities in IT infrastructures; possesses experience with HBSS, ACAS, SCAP, STIGs, IAVA notices, eMASS, RMF and vulnerability management; has excellent oral and written communication skills and exceptional interpersonal skills, with an emphasis on listening and questioning.	Eight (8) years of increasingly complex and progressive experience in Department of Defense (DoD) IT security, information assurance (IA), cybersecurity and/or IT compliance support. Four (4) years must have been in a supervisory role.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.
Senior Network Administrator	Performs the installation, implementation, troubleshooting, and maintenance of agency wide-area networks (WANs) and local-area networks (LANs); leads the day-to-day network administration effort and provides assistance and guidance to other more junior network admin team members; works on complex, distributed, heterogeneous computing environments, which may involve different types of hardware platforms, operating systems, applications, database systems and network environments; designs and manages the WAN infrastructure and any processes related to the WAN; oversees day-to-day operations, monitoring and problem resolution of all client networks; provides third tier problem diagnosis and resolution; possesses a superior knowledge of all software systems and architectures, communications protocols and network hardware devices.	Eight (8) years of increasingly complex and progressive experience in Department of Defense (DoD) IT network administration support. Four (4) years must have been in a supervisory role.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.
Senior Program/Project Manager	Performs management activities for all aspects of multiple complex projects across multiple lines of business to ensure the overall program is aligned to and directly supports the client's strategic objectives; provides on-site leadership for project teams; develops and manages all aspects of project engagement including planning, communications, resources, execution, budget, change, risks and issues and closure; prepares estimates and detailed project plans for all phases of projects; ensures adequate resources to achieve project objectives in planned timeframes; monitors staff performance and completes performance reviews; provides client leadership and stakeholders with status reporting, success criteria	Eight (8) years of increasingly complex and progressive experience in Department of Defense (DoD) IT project management. Six (6) years must have been in a IT Program/Project Manager role.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline. Active Project



Labor Category	Description	Minimum Experience	Education Requirements
	results and metrics regarding project milestones, deliverables, dependencies and risks; sets and continually manages project expectations; monitors, tracks and controls outcomes to resolve issues, conflicts, dependencies and critical path deliverables.		Management Institute (PMI) Project Management Professional (PMP) certification required.
Senior Software Solutions Architect	Performs research, design, development, test, deployment, and oversees maintenance of software solutions; possesses expert knowledge and experience with front-end and back-end software development including client-side, server-side and database development; provides guidance on software maintenance of current applications on a live application servers; participates in analysis, isolation and correction of software defects; implements software design/corrections IAW our CMMI ML2-DEV processes; demonstrates outstanding written and verbal communication skills; possesses expertise in various SDLC methodologies including Waterfall, Agile, and Test Driven Development and design patterns and Object Oriented Programming (OOP); Aids in the creation and updating of software technical documentation IAW CMMI ML2-DEV processes; provides technical direction to programmers as required to ensure that all solution deadlines are met.	Ten (10) years of increasingly complex and progressive experience developing and implementing Department of Defense (DoD) software solutions. Five (5) years must have been in a supervisory role.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.
Senior Systems Administrator	Performs the configuration and operation of all client systems and servers; leads the day-to-day systems administration effort and provides assistance and guidance to other more junior sys admin team members; works on complex, distributed, heterogeneous computing environments, which may involve different types of hardware platforms, operating systems, applications, database systems and network environments; provides technical support for both hardware and software issues; oversees the monitoring of systems on a daily basis and formulates an immediate response to security or usability concerns; responds to and resolves third tier server and system problems; recommends and oversees upgrades to systems and processes as required for enhanced functionality and security issue resolution; oversees all systems processes and client infrastructure administration, including servers, databases, software and other applications and equipment as required.	Eight (8) years of increasingly complex and progressive experience in Department of Defense (DoD) IT systems administration support. Four (4) years must have been in a supervisory role.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.
Senior Technical/ Task Lead	Performs in a lead capacity on multiple complex technical projects across multiple lines of business to ensure the quality of technical execution meets or exceeds client's expectations; the focal point for all technical guidance and direction; routinely interacts with project team members, client leadership and key stakeholders on all technical requirements; provides guidance on design, development, procurement, installation, implementation and troubleshooting; gives oversight and direction to team members on all technical aspects of the project.	Eight (8) years of increasingly complex and progressive experience in Department of Defense (DoD) IT projects. Four (4) years must have been in the role of a lead.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.
Systems Administrator	Performs the configuration and operation of all client systems and servers; accomplishes the day-to-day systems administration effort with assistance and guidance from more senior systems admin team members, as needed; works on complex, distributed, heterogeneous computing environments, which may involve different types of hardware platforms, operating systems,	Four (4) years of increasingly complex and progressive experience in Department of Defense (DoD) IT	Associate's degree from an accredited college or university in any science,

Labor Category	Description	Minimum Experience	Education Requirements
	applications, database systems and network environments; provides technical support and troubleshooting for both hardware and software issues; monitors systems on a daily basis and identifies security or usability concerns; performs user account management, network configuration, routine maintenance, workstation/disk configuration and management, troubleshooting, documentation, training, and support for UNIX, LINUX, and Windows systems, peripherals, kernels, and scripts; installs and maintains software applications and provide recommendations on methods to improve or update existing systems to maximize performance.	systems administration support.	business, engineering or technology discipline.
Systems Analyst I	Performs a variety of tasks in connection with the analysis, development, installation, implementation, procurement, or support of IT systems; works under general supervision of a Technical Lead or Project Manager; develops systems requirements into system design specifications; analyzes data and situations; identifies and solves problems; reasons logically and draws valid conclusions; applies creative thinking in the development of effective solutions; monitors and resolves problems with IT system hardware, software and processes; establishes and maintains effective working relationships with others; communicates effectively verbally and in writing.	Two (2) years of increasingly complex and progressive experience in Department of Defense (DoD) IT hardware installation and troubleshooting support.	High School Diploma or equivalent.
UNIX / Linux Solutions Architect	Applies UNIX/Linux experience and current technology to deliver cutting edge solutions; provides highly technical UNIX/Linux expertise to business application solutions; manages and directs systems administration, maintenance, and engineering in multiple large enterprise server environments involving UNIX and Linux; provides technical guidance in software engineering techniques and automated support tools; analyzes functional business applications and design specifications for functional activities; ensures required documentation is prepared, including both program-level and user-level documentation; assists in establishing standards for information systems procedures; assists in response to server failures, full systems outages, and troubleshooting; assists in special projects; supports client in the development and maintenance of systems baselines.	Ten (10) years of increasingly complex and progressive experience developing and implementing Department of Defense (DoD) UNIX/Linux solutions. Five (5) years must have been in a supervisory role.	Bachelor's degree from an accredited college or university in any science, business, engineering or technology discipline.

## SIN 54151HACS – Highly Adaptive Cybersecurity Services

Labor Category	Description	Education	Years of Experience
Cyber Security Program Manager Level I	Manages moderately complex programs or projects and provides leadership in the development and implementation of cyber security, cloud, and engineering programs. Plans, organizes, and controls the overall activities of the contract involving cybersecurity services and solutions. Responsible for formulating and enforcing work standards, schedules, supervising personnel, and communicating policies, procedures, and Federal goals to team personnel. Serves as primary client interface and ensure programs meet government cost, schedule, and technical quality objectives; performs and meets contract administrative requirements; and identifies and ensures effectiveness of any corrective action resolution.	Bachelor's degree	5
Cyber Security Project Manager Level I	Oversees small IT related projects involving cybersecurity services and solutions. Assists Program Manager in working with Government Contracting Officer, or Contracting Officer's Representative, Government management personnel, or other key government stakeholders. Responsible for developing the Project Management plans and other contract documents. Directs the day-to-day efforts of technical personnel. Ensures the quality of deliverable cyber documentation, software, engineering and testing plans, or network installations. Monitors activities under the contract to ensure that all activities are executed in accordance with contract requirements and the COR's direction.	Bachelor's degree	3
Cyber Security Project Manager Level II	Oversee all aspects of the cyber security IT project, leading a team on large projects or a significant segment of large and complex project. Analyze new and complex project related challenges and develops innovative solutions for cost, schedule, technology, and quality solutions. Performs day-to-day management of delivery order projects, from original concept through final implementation while coordinating the Contracting Officer's Representative or key government stakeholders. Utilizes proven skills in those technical areas to analyze new and complex cyber project related problems and create innovative solutions involving financial management, scheduling, technology, methodology, tools, and solution components. Organizes, directs, and coordinates the planning and production of all activities associated with assigned delivery order projects.	Bachelor's degree	5
Cyber Security Project Manager Level III	Oversees large, complex IT related projects involving cyber security services and solutions. Monitors technical tasks and keeps the Contracting Officer's Representative or key customer stakeholders abreast of status and accomplishments of the cyber security IT project. Reviews cyber project plans to determine schedule, funding, plans for accomplishing projects, staffing requirements and allocates available resources to project phases. Establishes work plans and coordinates cyber staffing for each project phase and organizes assignments of project personnel. Identifies functional and cross-functional requirements and resources required for each task area.	Bachelor's degree	7
Cyber Security Specialist Level I	Provide support to monitor or maintain network, laptop, software, or cloud cyber security IT operations. Provides analysis to management and senior level technical personnel. Performs analysis and evaluations of existing or proposed processes, applications, systems, security, or software. Establishes system information requirements in the development of large-scale information systems. Provides support for the design of cyber security architectures to include the software, hardware, and communications to support the requirements and interfaces.	Bachelor's degree	3

Labor Category	Description	Education	Years of Experience
Cyber Security Specialist Level II	Identify and resolve highly complex technical issues to prevent cyber-attacks on government information systems and keeps IT systems secure from service interruptions, intellectual property theft, viruses, data mining, and sensitive customer data left to ensure operations continue uninterrupted. Identify information technology risks or deficiencies that affect the customer ability to support/meet organizational goals. Performs process modeling in support of cyber security planning and analysis efforts.	Bachelor's degree	5
Cyber Security Specialist Level III	Designs, develops, engineers, and implements integrated security solutions to ensure government data and systems are secure. Gathers and organizes technical information for cyber mission, goals, and needs, existing security protocols, and computer security programs to translate security and business requirements into technical solutions. Configures and validates secure systems; tests security products and systems to detect security vulnerabilities. Conducts regular audits to ensure that systems are being operated securely, and computer security policies and procedures are being implemented as defined in security plans.	Bachelor's degree	7
Cyber Security Specialist Level IV	Coordinates cyber strategy sessions, strategic assessments, and design reviews to validate cyber security approach and work products and implements solutions to highly complex problems and tasks. Plans and manages the work of cyber security-IT systems project teams. Assists organizations in translating a cyber security vision and strategy into resource and cyber processes. Designs cyber security architectures to include the software, hardware, and communications to support the requirements and interfaces. Lead customers through streamlining, reengineering and transforming processes and procedures to be more secure.	Bachelor's degree	10
Cyber Security Specialist Level V	Recognized as a cyber security subject matter expert in the cyber security domain, or proficient in highly demanded emergent cyber tools or processes. Applies subject matter expertise and authority to incidents, security applications or enterprise environments to improve security posture and/or resolve organizational issues Generate cyber security policies, procedures, or reporting documentation. Advise senior leadership on security issues. Provide direct support for day-to-day operations of IT systems, including the detection and correction of operational risks.	Bachelor's degree	12
Cyber Systems Administrator Level I	Conducts routine system administration tasks, including monitoring and performing preventative maintenance on supported systems and logging system support in system administration logs. Installs software, upgrades, and patches to operating systems and system software. May provide support for software applications and security tools, perform hardware and software configuration, perform scheduled system backups, or conduct audits. Performs work in accordance with established cyber policies and follows standard operating procedures.	Bachelor's degree	1
Cyber Systems Administrator Level II	Applies experience of operating systems, network infrastructure, and network operations to provide system administration and security support for a variety of IT related systems and networks. Conducts risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs. Provides support for diagnostic evaluations, implementation of corrections, and training users in operation of new systems and programs. Monitors and calibrates systems to achieve optimum performance. Conducts risk and vulnerability assessments of planned and installed systems to identify vulnerabilities, risks, and protection requirements.	Bachelor's degree	3

Labor Category	Description	Education	Years of Experience
Cyber Systems Administrator Level III	Develop, run tests, implement, and maintain operating system and software in support of cyber related activities. Implements standards for computer operations that are consistent with documented customer cyber policies and procedures. Resolves software, operating system, and networking cyber risks identified in vulnerability scans, penetration tests, or other cyber security testing performed across customer systems. Diagnoses risk and identifies issues and implement corrective actions or escalates problems to senior level support. May supervise and/or provide technical direction to subordinates.	Bachelor's degree	5
Cyber Systems Administrator Level IV	Contributes to the client cyber security vision by integrating a broad range of IT administrative solutions for various network client requirements. Develops and/or modifies processes to solve complex problems for computer systems to achieve desired cyber customer results through implementation of innovative technologies or solutions. Applies advanced cyber-IT administration methods or techniques to solve complex system requirements for hardware/software and applications and solutions. Implements key phases of significant projects.	Bachelor's degree	7
Cyber Systems Administrator Level V	Specializes in providing the full range of cyber security data collection, correlation, network administration, analysis, testing, or support. The scope of responsibility includes data, hardware or software, networks, mobile computing, cloud, and/or applications. Conducts advanced system administration tasks, including monitoring and performing preventative maintenance and logs system support in system administration logs. Monitors and calibrates systems to achieve optimum performance. Applies knowledge and expertise in debugging protocols and processes to diagnose problems and issues and implements corrective actions.	Bachelor's degree	10
Cyber Systems Architect III	Participates in design, development, and implementation of IT security architectures and solutions. Applies knowledge and expertise designing, deploying, and supporting systems in secure environments to provide oversight and management of system administrators, system engineers, developers, or other technical staff. Participates in discussions with government stakeholders to gather and validate requirements, conduct reviews, and identify process improvements. Provides implementation and technical advice for software engineering cyber security requirements. Supports projects and teams in the technical analysis of large complex mission critical systems in defining system security or software architecture.	Bachelor's degree	7
Cyber Security Analyst Level I	Performs analysis and research for projects involving cyber security services and solutions and/or in support of business processes and supporting systems. Collects and analyzes information security performance data and metrics. Analyzes stakeholder requirements and applicable industry, agency, and Federal guidelines and requirements. Develops technical work products which may include processes, descriptions, diagrams, requirements, end-user documentation, training documentation, and deliverables.	Bachelor's degree	1
Cyber Security Analyst Level II	Develops and implements cyber security standards and procedures. Coordinates, develops, and evaluates security programs. Recommends cyber security solutions to solve complex government requirements. Identifies, reports, and resolves security violations. Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Performs analysis, design, and development of security features for system architectures. Analyzes and defines security requirements for IT	Bachelor's degree	3

Labor Category	Description	Education	Years of Experience
	systems. Leads development of documentation which may include systems scope statements, process models, process updates, workflows, functional requirements, testing documentation, training materials, and cyber IT specific deliverables.		
Cyber Security Analyst Level III	Leads a team on large projects or significant portions of a complex cyber security and IT program. Analyzes new and complex cyber related problems and creates innovative solutions involving technology, methodology, tools, risk management, and solution components. Provides application or systems analysis activities. Prepares long and short-range plans for cyber security application or system selection, development, maintenance, and production activities. Gathers and disseminates cyber analysis data and information to other analysts and organizational stakeholders. Assist in the identification and proliferation of IT security enhancements to better protect the customer environments. Leads development of various technical deliverables, work products, and documentation across a myriad of cyber security requirements.	Bachelor's degree	5
Cyber Security Analyst Level IV	Provides expert cyber security analysis and leadership in specialized functional or technical areas. Coordinates with government leadership at all levels to ensure that the cyber challenges are defined and that proposed solutions solve critical government requirements. Designs, organizes, leads, and conducts executive level analysis, workshops, benchmarking, surveys, and requirements gathering. Analyzes technical and cyber security risk, schedule, and cost impacts of proposed approaches. Establishes cyber security performance and technical standards. Leads development of documentation which may include systems scope statements, process models, process descriptions, workflow diagrams, functional and non-functional requirements, program documentation, end-user documentation, testing documentation, training documentation, and other work products and deliverables.	Bachelor's degree	7
Cyber Security Engineer Level I	Provides support related to the design, development, integration, and security of hardware, software, interfaces, and system level requirements to provide integrated IT solutions. Assists with design, development, and implementation of security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation. Leads the installation, monitoring, maintenance, support, and optimization of all network hardware, software, and communication links. Assists with system and security test requirements, strategies, devices, and systems. Works under supervision of a team lead or manager.	Bachelor's degree	3
Cyber Security Engineer Level II	Leads a team of security engineers, manages large scale deployments, assessments, and cyber security engineering or maintenance projects. Validates and verifies security requirements and establishes system security designs. Designs, develops, implements security systems and system components for network, cloud, mobile, application and/or other environments. Provides engineering services for cyber security investigations, recovery, and solution implementation. Provides in-depth knowledge of various security tools and educates teams to ensure their understanding and adherence to policies and procedures for implementing security standards. Responds to audit requests regarding compliance of security plans, policies, or procedures.	Bachelor's degree	5
Cyber Security Engineer Level III	Responsible for engineering, implementing, and monitoring security measures for the protection of IT systems, networks, and government information. Designs computer security architectures and develops detailed cyber security designs. Ensures networks have adequate	Bachelor's degree	7

Labor Category	Description	Education	Years of Experience
	security to prevent unauthorized access. Conducts risk and vulnerability analysis. Develops reports for administrators about the efficiency of security policies and recommends changes. Provides subject matter expertise and direction for information assurance, security, digital forensics, and incident responses. Assist in analysis and evaluation of the cyber security IT environment and with the preparation of recommendations for system improvements, optimization, development, and maintenance in multiple cyber security specialties.		
Cyber Security Test Specialist II	Assists with test strategies and tools for cybersecurity services and solutions. Develops and executes test and evaluation procedures to validate system and security requirements. Develops, maintains, and upgrades manual or automated test scripts. Develops and reviews testing status and results. Provides risk management support emphasizing requirements for testability, test design, test tools, and test environments. Provide expertise, guidance, and support using tools and techniques to conduct cyber vulnerability and penetration testing and supporting. Follows approved standard operating procedures and contributes to development, maintenance, and continuous improvement of cybersecurity testing procedures.	Bachelor's degree	5