GENERAL SERVICES ADMINISTRATION
FEDERAL ACQUISITION SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULES FSS PRICELIST

MULTIPLE AWARD SCHEDULE

FSC GROUP: Information Technology

Avint, LLC
205 Van Buren Street, Suite 400, Herndon, VA 20170
Phone: (571) 287-7715
Email: avint@avintllc.com
www.avintllc.com

Contract Number: 47QTCA19D00KZ
Period Covered by Contract: September 12, 2018 through September 11, 2029

Pricelist effective as of Mod PO-0021, March 13, 2025

Business Size:
Small Business
Women-Owned Small Business
SBA-Certified Women-Owned Small Business
SBA-Certified Economically Disadvantaged Women-Owned Small Business
Service Disabled Veteran Owned Small Business
SBA Certified Small Disadvantaged Business

Contract administration source:
Marcie Nagel

Online access to contract ordering information, terms and conditions, pricing, and the option to create an electronic delivery order are available through GSA Advantage!®. The website for GSA Advantage!® is: https://www.GSAAdvantage.gov.

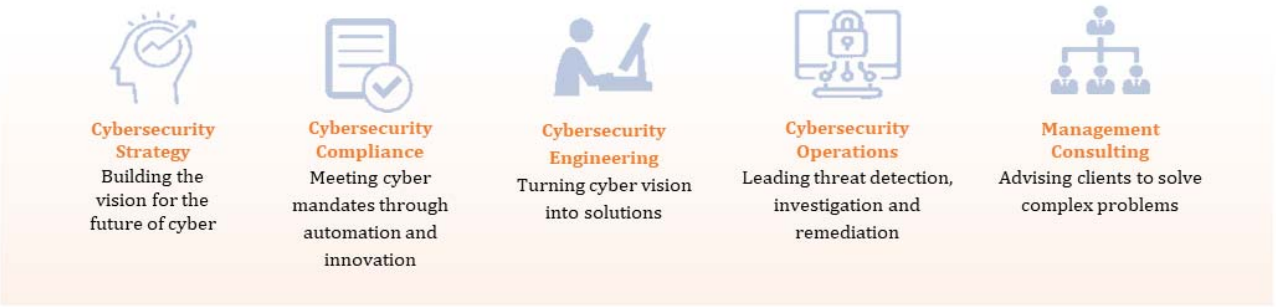
For more information on ordering, go to the following website: Https://www.gsa.gov/schedules

About Avint:

What is Avint?

Avint is a rapidly growing woman owned (WOSB), service disabled owned (SDVOSB), cybersecurity and management consulting firm providing our world-class expertise to solve the toughest challenges and build innovative solutions.

What do we do?



What is our brand?

Avint believes our brand is more than our name and logo. It represents our vision, core values, behaviors, performance and reputation in the market we serve. Collectively, our team defines the Avint brand by the way we work together and how we serve our clients.

Core values. ***Avid Integrity*****;** choose the right with passion and enthusiasm. ***Empower Excellence*****;** provide support and space to excel. ***Your Vision Achieved*****;** turn goals into reality.

Vision. To build a thriving cyber security services firm that harnesses the expertise of world class professionals.

INFORMATION FOR ORDERING ACTIVITIES APPLICABLE TO ALL SPECIAL ITEM NUMBERS

1a. AUTHORIZED SPECIAL ITEM NUMBERS (SINs):

SPECIAL ITEM NUMBER (SIN)	SIN DESCRIPTION	DESCRIPTION PAGE	AWARDED PRICE PAGE
54151S	Information Technology Professional Services	10 – 23	5 – 7
54151HACS	Highly Adaptive Cybersecurity Services (HACS)	24 – 37	7 – 9
OLM	Order-Level Materials (OLM)	Defined at Order Level	Defined at Order Level

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN: See Price List on page 5 – 9

1c. SERVICES OFFERED: See Price List on page 5 – 9

2. MAXIMUM ORDER:

SIN	MAXIMUM ORDER
54151HACS	$500,000 per SIN/Order
54151S	$500,000 per SIN/Order

3. MINIMUM ORDER: $100

4. GEOGRAPHIC COVERAGE (DELIVERY AREA): Domestic Only

5. POINT(S) OF PRODUCTION: United States

6. DISCOUNT FROM LIST PRICES OR STATEMENT OF NET PRICE: Prices listed are net, discounts have been deducted and the Industrial Funding Fee has been added.

7. QUANTITY DISCOUNTS: An additional 1% discount will be applied on single Task Orders above $250,000.

8. PROMPT PAYMENT TERMS: Net 30 – Information for the ordering offices: prompt payment terms cannot be negotiated out of contractual agreement in exchange for other concessions

9. FOREIGN ITEMS: None

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

10b. EXPEDITED DELIVERY: Contact Contractor

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

10d. URGENT REQUIREMENTS: Contact Contractor

11. F.O.B. POINT(S): FOB Destination

12a. ORDERING ADDRESS:

Avint, LLC
205 Van Buren Street, Suite 400
Herndon, VA 20170

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

13. PAYMENT ADDRESS: Same as Ordering Address

14. WARRANTY PROVISION: Standard Commercial Warranty

15. EXPORT PACKING CHARGES: Not Applicable

16. TERMS AND CONDITIONS OF RENTAL: Not Applicable

17. TERMS AND CONDITIONS OF INSTALLATION: Not Applicable

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

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

19. LIST OF SERVICE AND DISTRIBUTION POINTS: Not Applicable

20. LIST OF PARTICIPATING DEALERS: Not Applicable

21. PREVENTIVE MAINTENANCE: Not Applicable

22a. SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (E.G., RECYCLED CONTENT, ENERGY EFFICIENCY AND/OR REDUCED POLLUTANTS: Not Applicable

22b. SECTION 508 COMPLIANCE INFORMATION: Not Applicable

23. UNIQUE ENTITY IDENTIFIER (UEI) NUMBER: UW4CUW6QK8N7

24. NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE: Avint, LLC is registered in the System for Award Management (SAM) database. Cage Code: 7FU49

AVINT PRICE LIST - SIN 54151S LABOR CATEGORY RATES

Labor Category	Sep. 12, 2024 - Sep. 11, 2025	Sep. 12, 2024 - Sep. 11, 2026	Sep. 12, 2024 - Sep. 11, 2027	Sep. 12, 2024 - Sep. 11, 2028	Sep. 12, 2024 - Sep. 11, 2029
Cyber Security Project Manager	$182.67	$189.07	$195.69	$202.54	$209.63
Cyber Security Subject Matter Expert	$158.40	$163.94	$169.67	$175.61	$181.75
Cyber Security Subject Matter Expert (Master)	$246.13	$254.74	$263.66	$272.89	$282.44
Cyber Security Subject Matter Expert (Senior)	$205.75	$212.96	$220.41	$228.13	$236.11
Cyber Security Training Specialist (Senior)	$201.90	$208.97	$216.28	$223.85	$231.69
Enterprise Architect	$192.93	$199.68	$206.67	$213.90	$221.39
Information Assurance/Security Specialist	$158.40	$163.94	$169.67	$175.61	$181.75
IT Security Specialist (Senior)	$116.47	$120.55	$124.78	$129.14	$133.66
Quality Assurance Specialist (Master)	$151.12	$156.41	$161.88	$167.55	$173.41
Cyber Data Architect	$228.83	$236.84	$245.13	$253.71	$262.59
Cyber Engineer (Junior)	$72.90	$75.45	$78.09	$80.82	$83.65
Cybersecurity Analyst	$109.72	$113.56	$117.53	$121.64	$125.90
Engineer / Analyst (Principal)	$133.70	$138.38	$143.22	$148.24	$153.43
Engineer / Analyst (Senior)	$138.71	$143.57	$148.59	$153.79	$159.17
Enterprise Architect (Master)	$196.79	$203.68	$210.81	$218.19	$225.82
Governance, Risk, and Compliance (Lead)	$193.58	$200.35	$207.37	$214.62	$222.14
Information Assurance Engineer (Journeyman)	$116.48	$120.56	$124.79	$129.15	$133.67
Information Assurance Engineer (Master)	$196.79	$203.68	$210.81	$218.19	$225.82
Information Assurance Engineer (Senior)	$132.56	$137.20	$142.01	$146.97	$152.12
Information Assurance Engineer (SME)	$163.37	$169.08	$174.99	$181.12	$187.46
Information Systems Security Officer	$116.35	$120.42	$124.63	$129.00	$133.51
Information Systems Security Officer (Journeyman)	$116.46	$120.54	$124.77	$129.13	$133.65
Information Systems Security Officer (Senior)	$131.46	$136.06	$140.83	$145.75	$150.85
Penetration Tester	$228.83	$236.84	$245.13	$253.71	$262.59
Program Manager (Master)	$213.44	$220.91	$228.63	$236.63	$244.92
RMF Information Systems Security Officer	$142.04	$147.00	$152.15	$157.48	$162.99
Security Control Assessor (Senior)	$182.67	$189.07	$195.69	$202.54	$209.63
Security Tools Engineer (Senior)	$138.13	$142.96	$147.97	$153.15	$158.51
Splunk SME (Master)	$208.57	$215.88	$223.44	$231.25	$239.35
System Engineer	$196.79	$203.68	$210.81	$218.19	$225.82
Technical Writer (Junior)	$78.84	$81.60	$84.45	$87.41	$90.47
Technical Writer	$86.53	$89.56	$92.70	$95.94	$99.29
Technical Writer (Senior)	$163.44	$169.16	$175.08	$181.21	$187.55
Virtualization Engineer	$163.08	$168.80	$174.70	$180.82	$187.14

Labor Category	Sep. 12, 2024 - Sep. 11, 2025	Sep. 12, 2024 - Sep. 11, 2026	Sep. 12, 2024 - Sep. 11, 2027	Sep. 12, 2024 - Sep. 11, 2028	Sep. 12, 2024 - Sep. 11, 2029
Governance, Risk, and Compliance (SME)	$173.31	$179.38	$185.65	$192.15	$198.87
Project Manager (Master)	$213.44	$220.91	$228.63	$236.63	$244.92
Information Systems Security Officer (SME)	$158.40	$163.94	$169.67	$175.61	$181.75
Platform Architect	$163.08	$168.80	$174.70	$180.82	$187.14
Agile Project Management (SME)	$178.85	$185.11	$191.59	$198.30	$205.24
Network Engineer	$148.68	$153.87	$159.26	$164.84	$170.61
Subject Matter Expert	$204.48	$211.64	$219.04	$226.71	$234.65
Training Specialist (Senior)	$154.18	$159.58	$165.16	$170.94	$176.93

AVINT PRICE LIST - SIN 54151HACS LABOR CATEGORY RATES

Labor Category	Sep. 12, 2024 - Sep. 11, 2025	Sep. 12, 2024 - Sep. 11, 2026	Sep. 12, 2024 - Sep. 11, 2027	Sep. 12, 2024 - Sep. 11, 2028	Sep. 12, 2024 - Sep. 11, 2029
Cyber Security Project Manager	$182.67	$189.07	$195.69	$202.54	$209.63
Cyber Security Subject Matter Expert	$158.40	$163.94	$169.67	$175.61	$181.75
Cyber Security Subject Matter Expert (Master)	$246.13	$254.74	$263.66	$272.89	$282.44
Cyber Security Subject Matter Expert (Senior)	$205.75	$212.96	$220.41	$228.13	$236.11
Cyber Security Training Specialist (Senior)	$201.90	$208.97	$216.28	$223.85	$231.69
Enterprise Architect	$192.93	$199.68	$206.67	$213.90	$221.39
Information Assurance/Security Specialist	$158.40	$163.94	$169.67	$175.61	$181.75
IT Security Specialist (Senior)	$116.47	$120.55	$124.78	$129.14	$133.66
Quality Assurance Specialist (Master)	$151.12	$156.41	$161.88	$167.55	$173.41
HACS Cyber Data Architect	$228.83	$236.84	$245.13	$253.71	$262.59
HACS Engineer (Junior)	$72.90	$75.45	$78.09	$80.82	$83.65
HACS Cybersecurity Analyst	$109.72	$113.56	$117.53	$121.64	$125.90
HACS Engineer / Analyst (Principal)	$133.70	$138.38	$143.22	$148.24	$153.43
HACS Engineer / Analyst (Senior)	$138.71	$143.57	$148.59	$153.79	$159.17
HACS Enterprise Architect (Master)	$196.79	$203.68	$210.81	$218.19	$225.82
HACS Governance, Risk, and Compliance (Lead)	$193.58	$200.35	$207.37	$214.62	$222.14
HACS Information Assurance Engineer (Journeyman)	$116.48	$120.56	$124.79	$129.15	$133.67
HACS Information Assurance Engineer (Master)	$196.79	$203.68	$210.81	$218.19	$225.82
HACS Information Assurance Engineer (Senior)	$132.56	$137.20	$142.01	$146.97	$152.12
HACS Information Assurance Engineer (SME)	$163.37	$169.08	$174.99	$181.12	$187.46

Labor Category	Sep. 12, 2024 - Sep. 11, 2025	Sep. 12, 2024 - Sep. 11, 2026	Sep. 12, 2024 - Sep. 11, 2027	Sep. 12, 2024 - Sep. 11, 2028	Sep. 12, 2024 - Sep. 11, 2029
HACS Information Systems Security Officer	$116.35	$120.42	$124.63	$129.00	$133.51
HACS Information Systems Security Officer (Journeyman)	$116.46	$120.54	$124.77	$129.13	$133.65
HACS Information Systems Security Officer (Senior)	$131.46	$136.06	$140.83	$145.75	$150.85
HACS Penetration Tester	$228.83	$236.84	$245.13	$253.71	$262.59
HACS Program Manager (Master)	$213.44	$220.91	$228.63	$236.63	$244.92
HACS RMF Information Systems Security Officer	$142.04	$147.00	$152.15	$157.48	$162.99
HACS Security Control Assessor (Senior)	$182.67	$189.07	$195.69	$202.54	$209.63
HACS Security Tools Engineer (Senior)	$138.13	$142.96	$147.97	$153.15	$158.51
HACS Splunk SME (Master)	$208.57	$215.88	$223.44	$231.25	$239.35
HACS System Engineer	$196.79	$203.68	$210.81	$218.19	$225.82
HACS Technical Writer (Junior)	$78.84	$81.60	$84.45	$87.41	$90.47
HACS Technical Writer	$86.53	$89.56	$92.70	$95.94	$99.29
HACS Technical Writer (Senior)	$163.44	$169.16	$175.08	$181.21	$187.55
HACS Virtualization Engineer	$163.08	$168.80	$174.70	$180.82	$187.14
HACS Governance, Risk, and Compliance (SME)	$173.31	$179.38	$185.65	$192.15	$198.87
HACS Project Manager (Master)	$213.44	$220.91	$228.63	$236.63	$244.92
HACS Information Systems Security Officer (SME)	$158.40	$163.94	$169.67	$175.61	$181.75
HACS Platform Architect	$163.08	$168.80	$174.70	$180.82	$187.14
HACS Agile Project Management (SME)	$178.85	$185.11	$191.59	$198.30	$205.24
HACS Network Engineer	$148.68	$153.87	$159.26	$164.84	$170.61
HACS Subject Matter Expert	$204.48	$211.64	$219.04	$226.71	$234.65
HACS Training Specialist (Senior)	$154.18	$159.58	$165.16	$170.94	$176.93

The following table demonstrates the additional years of experience required to substitute for the education requirements.

DEGREE REQUIRED	ADDITIONAL YEARS OF EXPERIENCE NEEDED
Associate Degree	2
Bachelor Degree	4
Master Degree	6

AVINT LCAT DESCRIPTIONS 54151S

CYBER SECURITY PROJECT MANAGER

- Serves as a Senior Leader to provide project management services over complex or mission critical client requirements related to cyber security and technology.
- Experienced senior level subject matter expert in the cybersecurity discipline that provides services outlined with project requirements and scope of work to include risk management, risk assessments, remediation management, configuration management, penetration testing, ICAM, cyber engineering, and compliance.
- Responsible for leading projects to apply enterprise information security standards and develops and implements information security standards and procedures.
- Provides tactical information security advice and examining the ramifications of new technologies.
- Responsible for overseeing the preparation of project reports and deliverables to include penetration testing report, security impact assessments, system security plans, risk assessments, audit reports, enterprise architectures, project management plans, integrated master schedules, and risk registers.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

CYBER SECURITY SUBJECT MATTER EXPERT

- Serves as subject matter expert, possessing in-depth knowledge of an area, such as cyber security architecture and engineering, cyber security operations, risk assessments, penetration testing, and cyber security compliance.
- Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.
- Participates as needed in all phases of cyber security and technology lifecycle with emphasis on the planning, design, analysis, testing, integration, documentation, and presentation phases.
- Applies principles, methods and knowledge of the functional cyber and technology capability areas to specific task order requirements, advanced cyber and technology principles and methods to exceptionally difficult and narrowly defined problems to arrive at automated.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

CYBER SECURITY SUBJECT MATTER EXPERT (MASTER)

- Serves as subject matter expert, possessing in-depth knowledge of areas, such as cyber security architecture and engineering, cyber security operations, and cyber security compliance.
- Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.
- Participates as needed in all phases of cyber security and technology lifecycle with emphasis on the planning, design, analysis, testing, integration, documentation, and presentation phases.
- Applies principles, methods, and knowledge of the functional cyber, physical, and technology capability areas to specific task order requirements, advanced cyber and technology principles, and methods to exceptionally difficult and narrowly defined problems to arrive at automated solutions.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 10 YEARS

CYBER SECURITY SUBJECT MATTER EXPERT (SENIOR)

- Serves as subject matter expert, possessing in-depth knowledge of areas, such as cyber security architecture and engineering, cyber security operations, and cyber security compliance.
- Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.
- Participates as needed in all phases of cyber security and technology lifecycle with emphasis on the planning, design, analysis, testing, integration, documentation, and presentation phases.
- Applies principles, methods and knowledge of the functional cyber and technology capability areas to specific task order requirements, advanced cyber and technology principles and methods to exceptionally difficult and narrowly defined problems to arrive at automated.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

CYBER SECURITY TRAINING SPECIALIST (SENIOR)

- Develop course curriculum, and deliver training on the implementation and operation of cyber security solutions to include how to operate specific cyber security technologies and capabilities to include: asset management, identity and access management, security automation and orchestration, data integration, cyber operations, risk management, cyber security data reporting and visualization.
- Stays current with a multitude of cyber security disciplines to support a defense in depth cyber security curriculum.
- Assesses, designs, and conceptualizes cyber security training scenarios, approaches, objectives, plans, tools, aids, curriculums, and other state of the art technologies related to training and behavioral studies.
- Identifies the best approach training requirements to include, but not limited to hardware, software, simulations, course assessment and refreshment, assessment centers, oral examinations interviews, computer assisted and adaptive testing, behavior-based assessment and performance, and team and unit assessment and measurement.
- Develops and revises training courses. Prepares training catalogs and course materials.
- Trains personnel by conducting formal classroom courses, workshops, and seminars.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 7 YEARS

ENTERPRISE ARCHITECT

- Provides high-level cyber security, identity credential and access management (ICAM), or enterprise architectural expertise.
- Develops cyber, physical, and technical architectural products and deliverables for the enterprise and operational business lines.
- Provides engineering and technical support services to support enterprise integration of cyber and physical security solutions.
- Provide enterprise architecture subject matter expertise to align to cloud infrastructure and modernization strategies.
- Provide input into the security design and development of new and existing solution architecture.
- Provide technical expertise to plan for cloud growth strategies.

- Advises on selection of technological purchases with regards to security capabilities, data storage, data access, physical access control systems, identity credential and access control (ICAM), public key infrastructure (PKI) and applications development. Sets standards for the client/server relational database structure for the organization (SPLUNK, RSA ARCHER, SIEM, GRC etc.)
- Develops white papers, leads proof of concept initiatives, and advises on build or buy decisions.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 5 YEARS

INFORMATION ASSURANCE / SECURITY SPECIALIST

- Determines enterprise information assurance and security standards.
- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization. Recommends information assurance/security solutions to support customers' 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.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
- Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
- Performs analysis, design, and development of security features for system architectures.
- Analyzes and defines security requirements for computer systems which may include mainframes, workstations, and personal computers.
- Designs, develops, engineers, and implements solutions that meet security requirements.
- Provides integration and implementation of the computer system security solution.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.
- Ensures that all information systems are functional and secure.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 5 YEARS

INFORMATION TECHNOLOGY SECURITY SPECIALIST (SENIOR)

- Serves as advisor to system owners and CISO/ ISSM on all matters involving security of an organization's information systems.
- Responsible for day-to-day information technology / cyber security operations of information systems.
- Applies security controls, policies, and procedures to an organization's information systems to achieve compliance goals and objectives.
- Coordinates with external agencies and assists in the preparation of information security agreements.
- Provides cyber security support to plan, coordinate, and implement an organizations information security program, policies, and procedures.
- Applies in-depth cyber security, risk management, current security tools, diverse communication protocols, encryption techniques / tools to recommend security solutions and remediation plans.
- Assists with the development and maintenance of System Security Plans, Plan of Action and Milestones, Security Impact Assessments, Privacy Impact Assessments, Privacy Threshold Analysis, and other related security compliance documents and deliverables.

MINIMUM EDUCATION: BA/BS or equivalent work experience

MINIMUM YEARS OF EXPERIENCE: 7 YEARS

QUALITY ASSURANCE SPECIALIST (MASTER)

- Provides development of project Software Quality Assurance Plan and the implementation of procedures that conforms to the requirements of the contract.
- Provides an independent assessment of how the project's software development process is being implemented relative to the defined process and recommends methods to optimize the organization's process.
- May be responsible for all activities involving quality assurance and compliance with applicable regulatory requirements.
- Conducts audits and reviews/analyzes data and documentation.
- Develops and implements procedures and test plans for assuring quality in a system development environment which supports large databases and applications.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 10 YEARS

CYBER DATA ARCHITECT

- Create data dictionaries and business glossaries to document data lineages, data definitions and metadata for all business-critical data domains.
- Apply knowledge of reference models to data architecture design and maintain alignment with standards and best practices for ontology representation.
- Develop data governance framework that aligns with user needs and data governance practices and standards. Implement data architecture initiatives on data quality, data governance, data standards, and data policies across all core business functions to ensure consistency in data definitions and data usage.
- Guide efforts to define the mission, goals, critical success factors, principles, and policies for data strategy and architecture.
- Build a framework that encourages integration of policy, procedure, system help, training, and other useful resources.
- Help maintain the integrity and security of the database including data encryption.
- Design and implements effective database solutions and models to store and retrieve data. Examine and identify database structural necessities by evaluating client operations, applications, and programming. Assess database implementation procedures to ensure they comply with internal and external regulations.
- Install and organize information systems to guarantee functionality. Develop database design and architecture documentation.
- Provide data analysis and establishes data standardization. Oversee the migration of data from legacy systems to new solutions. Work closely with Database Administrator to monitor system performance by performing regular tests, troubleshooting, and integrating new features. Recommend solutions to improve new and existing database systems.
- Educate staff members through training and individual support. Develop presentations and reports.
- Provide operational database administration support as needed: Build, support, and maintain Microsoft SQL database systems of high availability including backup and recovery.
- Minimize database downtime and manage parameters to provide fast query responses.
- Determine, enforce and document database environment, policies, procedures and standards. Perform tests and evaluations regularly to ensure data security, privacy, and integrity. Monitor database performance, implement changes and apply new patches and versions when required. Utilize monitoring and performance analysis to troubleshoot and isolate problems/issues/incidents.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

CYBER ENGINEER (JUNIOR)

- Assist higher level cybersecurity engineers in performing job functions. The junior engineer supports the installation, implementation, and integration of security technologies, system hardening, and network configurations.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 2 YEARS

CYBERSECURITY ANALYST

With oversight, carry out the following:

- Develop and promote best practices for information security.
- Analyze and create cybersecurity policies that are compliant with industry standards and client requirements.
- Assist in the development of cybersecurity documentation such as integration guides, SSPs, POA&Ms, etc.
- Identify, analyze, and mitigate system vulnerabilities.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 2 YEARS

ENGINEER / ANALYST (PRINCIPAL)

- Establishes system engineering and information requirements using analysis of the information engineer in the development of enterprise-wide or large scale information technology systems.
- Designs architecture to include software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces.
- Ensures these systems are compatible and in compliance with the standards for open systems architectures (OSI, ISO, IEEE, OSE) as they apply to the implementation and specification of information technology solutions.
- Analyzes system requirements and develops design alternatives to satisfy those requirements.
- Provides technical leadership developing solutions for engineering studies and internet/intranet applications.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

ENGINEER / ANALYST (SENIOR)

- Provide design, programming, documentation, and implementation of applications which requires knowledge of government information technology systems for effective development and deployment of software modules.
- Directs and participates in all phases of software development with emphasis on analysis, coding, testing, documentation, and acceptance phases. Responsible for identifying new and emerging technology to support strategic planning initiatives required to meet business needs.
- Conducts assessments, evaluations, selections, site surveys, requirements analysis and definition, technology prototyping, and cost analysis related to information technology.
- Designs and prepares technical reports and documentation to record results. Gathers information by developing and implementing data collection instruments and conducts surveys, document reviews, and interviews.

- Provides group facilitation, interviewing, training, and provides additional forms of knowledge transfer. Facilitation support includes cross-functional team building, project scoping work sessions, facilitation using creative dynamics techniques, and conflict resolution techniques.
- Performs manual or automated modeling of process or data models, data flow diagrams, and simulation models.
- Develops prototype database systems.
- Designs transaction driven modules to satisfy functional requirement in an online or internet/intranet environment.
- Designs test environments for new applications against databases. Creates entity relationships models to support logical and physical database designs.
- Creates the metadata describing the database design and attribute descriptions.
- Creates the schema for building the database.
- Assists in the management of database projects. Assists in the preparation and delivery of presentations on database management systems concepts.
- Responsible for overall administration and maintenance of the database, identification and resolution of problems encountered by the users of the system, analysis and implementation of enhancements, and operation and maintenance of databases.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

ENTERPRISE ARCHITECT (MASTER)

- Provide all the necessary technical expertise to architect and design cyber security enterprise solutions into a client's overarching enterprise.
- Ensure effective execution of all architecture tasks with the agency assigned projects.
- Provide thought leadership for stakeholders.
- Provide technical oversight for solution deployment engagements.
- Understand the client's strategic and programmatic needs.
- Propose and implement effective solutions.
- Architects and designs enterprise-class security systems for a production environment.
- Align standards, frameworks and security with overall business and technology strategy.
- Identify and communicate current and emerging security threats.
- Design security architecture elements to mitigate threats as they emerge.
- Create solutions that balance business requirements with information and cyber security requirements.
- Identify security design gaps in existing and proposed architectures and recommend changes or enhancements.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

GOVERNANCE, RISK, AND COMPLIANCE (LEAD)

- Lead development of cybersecurity best practices, and deployment of repeatable cybersecurity methodologies.
- Leverage Risk Management Framework (RMF) principles to obtain system authorizations.
- Provide technical knowledge and expertise in cyber governance, risk management and compliance.
- Develop, maintain and manage cyber security and information assurance related technical system requirements.
- Develop and program partner-specific cyber security requirements based on the Risk Management Framework (RMF) control catalog and associated overlays.

- Plan, execute, and document independent cybersecurity assessments of systems under development. Document residual risk, system deficiencies, and recommend remediation actions to bring systems into cybersecurity compliance.
- Review and provide feedback on cybersecurity documentation provided by integrators to ensure documentation meets cybersecurity requirements.
- Develop the technical data necessary to support RMF activities for information systems.
- Develop governance, risk, and compliance documentation to include cybersecurity policies, plans, and procedures in support of standing up cyber program capabilities.
- Work closely with relevant stakeholders to tailor GRC documentation

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

INFORMATION ASSURANCE ENGINEER (JOURNEYMAN)

- Help manage the client's Cybersecurity / Information Assurance Posture, monitor all Operations and Infrastructure, maintain all security tools and technology, monitor internal and external policy compliance, monitor regulation compliance, and work to mitigate risk across security system's infrastructure.

With oversight:

- Perform comprehensive security assessments using the Risk Management Framework (RMF).
- Utilize knowledge of Confidentiality, Integrity, and Availability Levels and National Institute of Standards and Technology (NIST) Special Publication 800-53 controls associated with each level.
- Analyze information assurance systems in unclassified and/or classified environments for compliance with client requirements, and industry best practices.
- Responsible for documentation review, reading over policy and procedures, SOPs, and previous accreditation documents; compile and generate deliverables, and present those deliverables to the client.
- Review Information Assurance Controls with the client for specific applicability and compliancy.
- Prepare and review program documentation to include but not limited to Risk Assessment Reports, Accreditation Packages, and security policy guides.
- Ensure compliance with client requirements and industry standards to perform cybersecurity / information assurance duties.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 4 YEARS

INFORMATION ASSURANCE ENGINEER (MASTER)

- Perform cybersecurity / Information Assurance for all client managed systems, applications, and hardware in the environment.
- Provide subject master expertise in Security, Vulnerability tools, and RMF.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

INFORMATION ASSURANCE ENGINEER (SENIOR)

- Help develop and implement the client's Cybersecurity / Information Assurance Program, monitor all Operations and Infrastructure, maintain all security tools and technology, monitor internal and external policy compliance, monitor regulation compliance, and work to mitigate risk across security system's infrastructure.

- Perform cybersecurity / Information Assurance for all client managed systems, applications, and hardware.
- Conduct security/vulnerability scans using provided Security and Vulnerability tools.
- Have expert knowledge of Risk Management Framework (RMF).

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

INFORMATION ASSURANCE ENGINEER (SME)

- Perform cybersecurity / Information Assurance for all client managed systems, applications, and hardware in the environment.
- Provide subject mater expertise in Security and Vulnerability tools and RMF.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

INFORMATION SYSTEMS SECURITY OFFICER

- Provide knowledge of Risk Management Framework (RMF) and support Cybersecurity Inspections, Operations, and Orders Processing.
- Assist in the performance of RMF.
- Support the security assessment and authorization activities for information systems.
- Maintain 100% ATO status.
- Assist in cybersecurity related audits, inspections, and assessments.
- Ensure information systems comply with client requirements and industry standards.
- Help conduct weekly or ad-hoc audits, inspections and assessment reports, as well as remediation status briefings / reports.
- Develop system security contingency plans and disaster recovery plans.
- Assist in the development and implementation of programs as required to ensure that systems, networks, and data users are aware of, understand, and adhere to systems security policies and procedures.
- Ensure the rigorous application of information security / information assurance policies, principals, and practices in the delivery of all IT services.
- Assist in coordinating user and private account processing.
- Ensure all necessary certification information is confirmed and documented.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

INFORMATION SYSTEMS SECURITY OFFICER (JOURNEYMAN)

- Provide knowledge of Risk Management Framework (RMF) and support Cybersecurity Inspections, Operations, and Orders Processing.
- Assist in the performance of RMF.
- Support the security assessment and authorization activities for information systems.
- Maintain 100% ATO status.
- Assist in cybersecurity related audits, inspections, and assessments.
- Ensure information systems comply with client requirements and industry standards.
- Help conduct weekly or ad-hoc audits, inspections and assessment reports, as well as remediation status briefings / reports.
- Develop system security contingency plans and disaster recovery plans.

- Assist in the development and implementation of programs as required to ensure that systems, networks, and data users are aware of, understand, and adhere to systems security policies and procedures.
- Ensure the rigorous application of information security / information assurance policies, principals, and practices in the delivery of all IT services.
- Assist in coordinating user and private account processing.
- Ensure all necessary certification information is confirmed and documented.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 4 YEARS

INFORMATION SYSTEMS SECURITY OFFICER (SENIOR)

- Provide subject matter expertise and knowledge of RMF.
- Lead cybersecurity inspections, operations, and orders processing.
- Perform RMF for all information systems and applications.
- Lead the security assessment and authorization activities for information systems.
- Maintain 100% ATO status.
- Follow RMF to identify, implement, assess, and manage cybersecurity capabilities and services, expressed as security controls, and authorizing the operation of an information system.
- Lead cybersecurity related audits, inspections, and assessments.
- Ensure information systems comply with client requirements and industry standards.
- Help conduct the appropriate remediation actions associated with findings from inspections and evaluations, generate status reports, and brief to clients.
- Develop system security contingency plans and disaster recovery plans.
- Develop and implement programs as required to ensure that systems, networks, and data users are aware of, understand, and adhere to systems security policies and procedures.
- Ensure the rigorous application of information security / information assurance policies, principals, and practices in the delivery of all IT services.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

PENETRATION TESTER

- Assess security systems.
- Conduct tests and purposefully attempt to exploit existing computer systems and software to detect and correct system weaknesses.
- Develop recommendations and implement solutions to bolster the cybersecurity posture of IT systems.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 4 YEARS

PROGRAM MANAGER (MASTER)

- Oversee all contract personnel and serve as Avint's primary point-of-contact for all matters related to contract performance.
- Is ultimately responsible for all contractual deliverables, ensuring operational excellence, and ensuring program activities stay on schedule and within budget.
- Track and report performance of Team.
- Act as a liaison between the team and the Government.
- Provide technical guidance to meet Government requirements.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

RMF Information Systems Security Officer

- Develop, maintain, and manage cyber security and information assurance related technical system requirements.
- Review and provide feedback on cybersecurity documentation to ensure they meet cybersecurity requirements. Help ensure systems meet cybersecurity standards.
- Verify and validate systems are built, configured, and hardened in a way that will pass assessment and receive authorization.
- Develop and document remediations for technical areas that cannot be hardened following best practices.
- Execute and document risk assessments of systems to evaluate compliance with government requirements and industry best practices.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

Security Control Assessor (Senior)

- Conducts independent comprehensive assessments of the management, operational, and technical security/privacy controls and control enhancements employed within or inherited by information technology (IT) systems to determine the overall effectiveness of the controls.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

Security Tools Engineer (Senior)

- Design and deploy custom, cutting-edge security tool solutions that meet the client's needs.
- Manage and maintain existing security tools.
- Stay abreast of new and emerging technologies to continually provide client the best-value solutions.
- Deploy, manage, and maintain the endpoint security for systems applications in the IT environment.
- Conduct test analysis and technical evaluations for vulnerabilities.
- Recommend and apply security countermeasures to mitigate identified risks.
- Troubleshoot and resolve technical and/or compliance issues.
- Provide weekly status reports and metrics including but not limited to vulnerability assessment results, patch management statics, asset inventory, system configurations, waver request generation / validation, and general information technology security guidance.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

Splunk SME (Master)

- Conceptualize, design, implement, and maintain Splunk infrastructure solutions.
- Create, manage, and support automation solutions for Splunk deployment and orchestration.
- Conduct periodic architectural reviews of Splunk and related systems to assess effectiveness and propose and implement optimal solutions as required.
- Develop and manage comprehensive documentation, artifacts, procedures, and processes for the optimal management of the Splunk infrastructure.

- Work closely with all relevent stakeholders to solve technical problems at the network, system, and application levels.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

SYSTEM ENGINEER

- Provide SME-level System Engineering Support.
- Ensure Network architecture meet defense in depth methodologies
- Support FIM implementation (File integrity management)
- Create and maintain SSP Documentation

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

TECHNICAL WRITER (JUNIOR)

- Develop professional, informative documents designed for both technical and non-technical audiences

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 1 YEAR

TECHNICAL WRITER

- Develop professional, informative documents designed for both technical and non-technical audiences

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 2 YEARS

TECHNICAL WRITER (SENIOR)

- Develop professional, informative documents designed for both technical and non-technical audiences

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 4 YEARS

VIRTUALIZATION ENGINEER

- Design integrated software and hardware solutions in virtualized enterprise and consumer systems.
- Leads systems planning, performance management, capacity planning, testing and validation, benchmarking, and information engineering.
- Perform technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for virtual systems.
- Create as-built and other systems drawings (flowcharts, diagrams).
- Design system security and data assurance.
- Analyze user requirements to automate or improve existing systems.
- Identify system integrity issues and solutions for the full system life cycle.
- Work with vendors to ensure operational capabilities

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

GOVERNANCE, RISK, AND COMPLIANCE (SME)

- Develop and oversee Governance Risk and Compliance (GRC) programs and GRC program staff, supporting GRC policy, and needs of GRC executives and their teams.
- Knowledgeable of laws, policies, and procedures within the GRC domain. Provide guidance on security risks, mitigations, and input on GRC related technical risks.
- Assist in the creation and maintenance of GRC related policies.
- Engage in security risk assessments to identify gaps, provide recommendations.
- Support continuous compliance with policies and standards and collect and validate audit evidence.
- Drive remediation of any identified gaps. Advise on compliance frameworks.
- Advise and support audit requirements.
- Ensure all security documentation is updated to reflect new federal mandates, policy releases or updated security frameworks. or updated security frameworks.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

PROJECT MANAGER (MASTER)

- Lead, coordinate, communicate, integrate, and maintain accountability for the overall success of the project.
- Ensure alignment with agency or enterprise priorities.
- Drive solutions involving finance, scheduling, technology, staffing, forecasting cost estimates, methodology, tools, and solution components.
- Ensure all contractual obligations are achieved.
- Apply knowledge of data, information, processes, organizational interactions, skills, and analytical expertise to manage projects.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

INFORMATION SYSTEMS SECURITY OFFICER (SME)

- Oversee the information assurance (IA) program of an information system.
- Oversee and ensure that the appropriate operational security posture (e.g., network and system security, physical and environmental protection, personnel security, incident handling, security training and awareness) is implemented and maintained for an information system or program.
- Advises the Authorizing Official (AO), an information system owner, or the Chief Information Security Officer (CISO) on the security of an information system or program.
- Provides Risk Management Framework (RMF) expertise and support with Cybersecurity Inspections, Operations, and Orders Processing.
- Support the security assessment and authorization activities for information systems.
- Assist in cybersecurity related audits, inspections, and assessments.
- Ensure information systems comply with client requirements and industry standards.
- Ensure system security documentation is current and authorization boundary is accurate for all information systems.
- Working knowledge of automated tools deployed in the environment is preferred.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

PLATFORM ARCHITECT

- Provides high-level architectural expertise to managers and technical staff.
- Develops architectural products and deliverables for the enterprise and operational business lines.
- Develops strategy of system and the design infrastructure necessary to support that strategy.
- Advises on selection of technological purchases with regards to processing, data storage, data access, and applications development.
- Sets standards for the client/server relational structure and security for the organization (SQL, ORACLE, SYBASE, etc.).
- Advises of feasibility of potential future projects to management.
- Experience in the development and maintenance of systems, Integration Tier, Security, Standards compliance, business activity monitoring, systems design, system analysis, and development preferred.
- Experience in defining and implementing a systems architecture using a combination of COTS processing, networking and data storage components into an embedded solution preferred.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

AGILE PROJECT MANAGEMENT (SME)

- Provide supervisory technical and administrative direction for personnel performing software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules.
- May serve as the Scrum Master and facilitate stand-ups and Sprint Review/Planning meetings.
- Manage the design, implementation and support of platform architecture.
- Analyze requirements for capabilities and determining system functions.
- Coordinate with Contractor Program Manager and Government Project Manager to ensure problem solution and user satisfaction.
- Prepare and deliver presentations on the system concept to colleagues, subordinates and user representatives.
- Systems analysis/programming experience preferred. Independent analysis/programming experience, with complete responsibility for tasks involving analysis, programming and implementation preferred.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

NETWORK ENGINEER

- Assist in the development and maintenance of network communications.
- Assist in monitoring any disruptions to ensure availability of the network.
- Use knowledge of LAN/WAN systems to help design and install internal and external networks.
- Test and evaluate network systems to eliminate problems and make improvements. Experience in the field or in a related area preferred.
- Familiarity with a variety of the field's concepts, practices, and procedures preferred.
- Relies on experience and judgment to plan and accomplish goals.
- Performs a variety of tasks. May lead and direct the work of others. A wide degree of creativity and latitude is preferred. Typically reports to a manager.
- Expert knowledge of LAN/WAN systems, networks, and applications preferred.
- Identification of security vulnerabilities and mitigation solutions.

- Working knowledge in vulnerability scan configuration and network modeling and network maintenance.
- May work with information security analyst to improve and implement security controls.
- Knowledgeable in existing COTS products is preferred.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

SUBJECT MATTER EXPERT

- Serve as subject matter expert, provide in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences.
- Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.
- Interfaces directly with stakeholders and executives as the responsible party to ensure all technical requirements are completed.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

TRAINING SPECIALIST (SENIOR)

- Assesses, designs, and conceptualizes training scenarios, approaches, objectives, plans, tools, aids, curriculum, and other state of the art technologies related to training and behavioral studies.
- Identifies the best approach training requirements to include, but not limited to hardware, software, simulations, course assessment and refreshment, assessment centers, oral examinations, interviews, computer assisted and adaptive testing, behavior-based assessment and performance, and team and unit assessment and measurement.
- Develops and revises training courses. Prepares training catalogs and course materials.
- Trains personnel by conducting formal classroom courses, workshops, and seminars.
- Performs a review of organizational best practice in order to evaluate and implement current training needs.
- Design and conduct training to improve performance based on the evaluation of the organization's needs.
- Plan and coordinate training across all individuals and track/report key metrics.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

AVINT LCAT DESCRIPTIONS 54151HACS

Note: For all LCATs under 54151HACS, a professional cybersecurity certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+) is required in addition to a BA/BS or equivalent work experience.

CYBER SECURITY PROJECT MANAGER

- Serves as a Senior Leader to provide project management services over complex or mission critical client requirements related to cyber security and technology.
- Experienced senior level subject matter expert in the cybersecurity discipline that provides services outlined with project requirements and scope of work to include risk management, risk assessments, remediation management, configuration management, penetration testing, ICAM, cyber engineering, and compliance.
- Responsible for leading projects to apply enterprise information security standards and develops and implements information security standards and procedures.
- Provides tactical information security advice and examining the ramifications of new technologies.
- Responsible for overseeing the preparation of project reports and deliverables to include penetration testing report, security impact assessments, system security plans, risk assessments, audit reports, enterprise architectures, project management plans, integrated master schedules, and risk registers.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

CYBER SECURITY SUBJECT MATTER EXPERT

- Serves as subject matter expert, possessing in-depth knowledge of an area, such as cyber security architecture and engineering, cyber security operations, risk assessments, penetration testing, and cyber security compliance.
- Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.
- Participates as needed in all phases of cyber security and technology lifecycle with emphasis on the planning, design, analysis, testing, integration, documentation, and presentation phases.
- Applies principles, methods and knowledge of the functional cyber and technology capability areas to specific task order requirements, advanced cyber and technology principles and methods to exceptionally difficult and narrowly defined problems to arrive at automated.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

CYBER SECURITY SUBJECT MATTER EXPERT (MASTER)

- Serves as subject matter expert, possessing in-depth knowledge of areas, such as cyber security architecture and engineering, cyber security operations, and cyber security compliance.
- Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.
- Participates as needed in all phases of cyber security and technology lifecycle with emphasis on the planning, design, analysis, testing, integration, documentation, and presentation phases.

- Applies principles, methods, and knowledge of the functional cyber, physical, and technology capability areas to specific task order requirements, advanced cyber and technology principles, and methods to exceptionally difficult and narrowly defined problems to arrive at automated solutions.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 10 YEARS

CYBER SECURITY SUBJECT MATTER EXPERT (SENIOR)

- Serves as subject matter expert, possessing in-depth knowledge of areas, such as cyber security architecture and engineering, cyber security operations, and cyber security compliance.
- Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.
- Participates as needed in all phases of cyber security and technology lifecycle with emphasis on the planning, design, analysis, testing, integration, documentation, and presentation phases.
- Applies principles, methods and knowledge of the functional cyber and technology capability areas to specific task order requirements, advanced cyber and technology principles and methods to exceptionally difficult and narrowly defined problems to arrive at automated.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

CYBER SECURITY TRAINING SPECIALIST (SENIOR)

- Develop course curriculum, and deliver training on the implementation and operation of cyber security solutions to include how to operate specific cyber security technologies and capabilities to include: asset management, identity and access management, security automation and orchestration, data integration, cyber operations, risk management, cyber security data reporting and visualization.
- Stays current with a multitude of cyber security disciplines to support a defense in depth cyber security curriculum.
- Assesses, designs, and conceptualizes cyber security training scenarios, approaches, objectives, plans, tools, aids, curriculums, and other state of the art technologies related to training and behavioral studies.
- Identifies the best approach training requirements to include, but not limited to hardware, software, simulations, course assessment and refreshment, assessment centers, oral examinations interviews, computer assisted and adaptive testing, behavior-based assessment and performance, and team and unit assessment and measurement.
- Develops and revises training courses. Prepares training catalogs and course materials.
- Trains personnel by conducting formal classroom courses, workshops, and seminars.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 7 YEARS

ENTERPRISE ARCHITECT

- Provides high-level cyber security, identity credential and access management (ICAM), or enterprise architectural expertise.
- Develops cyber, physical, and technical architectural products and deliverables for the enterprise and operational business lines.
- Provides engineering and technical support services to support enterprise integration of cyber and physical security solutions.

- Provide enterprise architecture subject matter expertise to align to cloud infrastructure and modernization strategies.
- Provide input into the security design and development of new and existing solution architecture.
- Provide technical expertise to plan for cloud growth strategies.
- Advises on selection of technological purchases with regards to security capabilities, data storage, data access, physical access control systems, identity credential and access control (ICAM), public key infrastructure (PKI) and applications development. Sets standards for the client/server relational database structure for the organization (SPLUNK, RSA ARCHER, SIEM, GRC etc.)
- Develops white papers, leads proof of concept initiatives, and advises on build or buy decisions.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 5 YEARS

INFORMATION ASSURANCE / SECURITY SPECIALIST

- Determines enterprise information assurance and security standards.
- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization. Recommends information assurance/security solutions to support customers' 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.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
- Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
- Performs analysis, design, and development of security features for system architectures.
- Analyzes and defines security requirements for computer systems which may include mainframes, workstations, and personal computers.
- Designs, develops, engineers, and implements solutions that meet security requirements.
- Provides integration and implementation of the computer system security solution.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.
- Ensures that all information systems are functional and secure.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 5 YEARS

INFORMATION TECHNOLOGY SECURITY SPECIALIST (SENIOR)

- Serves as advisor to system owners and CISO/ ISSM on all matters involving security of an organization's information systems.
- Responsible for day-to-day information technology / cyber security operations of information systems.
- Applies security controls, policies, and procedures to an organization's information systems to achieve compliance goals and objectives.
- Coordinates with external agencies and assists in the preparation of information security agreements.
- Provides cyber security support to plan, coordinate, and implement an organizations information security program, policies, and procedures.
- Applies in-depth cyber security, risk management, current security tools, diverse communication protocols, encryption techniques / tools to recommend security solutions and remediation plans.

- Assists with the development and maintenance of System Security Plans, Plan of Action and Milestones, Security Impact Assessments, Privacy Impact Assessments, Privacy Threshold Analysis, and other related security compliance documents and deliverables.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 7 YEARS

QUALITY ASSURANCE SPECIALIST (MASTER)

- Provides development of project Software Quality Assurance Plan and the implementation of procedures that conforms to the requirements of the contract.
- Provides an independent assessment of how the project's software development process is being implemented relative to the defined process and recommends methods to optimize the organization's process.
- May be responsible for all activities involving quality assurance and compliance with applicable regulatory requirements.
- Conducts audits and reviews/analyzes data and documentation.
- Develops and implements procedures and test plans for assuring quality in a system development environment which supports large databases and applications.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 10 YEARS

HACS CYBER DATA ARCHITECT

- As a Cybersecurity Data Governance Specialist, your primary responsibility is to ensure the security, integrity, and compliance of critical business data while maintaining robust data governance practices.
- You will play a pivotal role in creating, securing, and managing databases, as well as implementing data governance frameworks to protect sensitive information.
- Data Governance, and Documentation: Create comprehensive data dictionaries, business glossaries, and metadata documentation for business-critical data domains. Document data lineages, definitions, and metadata while prioritizing cybersecurity aspects.
- Data Architecture and Security: Apply your knowledge of reference models to design data architectures with a strong focus on cybersecurity principles. Maintain alignment with industry standards and best practices for secure ontology representation.
- Data Governance Framework: Develop and implement a data governance framework that aligns with user needs and cybersecurity practices and standards. Ensure data governance practices prioritize security and compliance.
- Data Quality and Security Initiatives: Drive data architecture initiatives focused on data quality, data standards, and data policies across all core business functions. Ensure consistency in data definitions and secure data usage.
- Data Strategy and Security: Lead efforts to define the mission, goals, critical success factors, principles, and policies for data strategy and architecture with a strong emphasis on cybersecurity. Promote integration of security policies, procedures, and resources.
- Database Integrity and Security: Assist in maintaining the integrity and security of databases, including data encryption and access controls. Work closely with the Database Administrator to monitor system security and implement security best practices.

- Database Design and Implementation: Design and implement effective database solutions and models with a cybersecurity-first mindset to ensure data security. Evaluate database structural requirements based on security considerations.
- Compliance and Regulation: Assess database implementation procedures to ensure compliance with internal and external cybersecurity regulations. Implement security measures to protect data privacy and integrity.
- Database Administration: Provide operational database administration support as needed, including building, supporting, and maintaining Microsoft SQL database systems with a focus on high availability and data security.
- Performance Monitoring: Minimize database downtime and ensure fast query responses by managing database parameters and conducting regular performance tests. Troubleshoot and isolate cybersecurity-related issues.Security
- Patch Management: Stay updated with cybersecurity threats and vulnerabilities. Apply patches and updates to maintain database security.
- Training and Reporting: Educate staff members on cybersecurity best practices through training and individual support. Develop presentations and reports to communicate cybersecurity status and improvements.

  By focusing on cybersecurity within the realm of data governance and database management, this role ensures that critical business data remains secure, compliant, and resilient against cyber threats and vulnerabilities.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Engineer (Junior)

- As an Entry-Level Cybersecurity Technician, your role is pivotal in assisting higher-level cybersecurity engineers in safeguarding critical systems and networks. Your primary responsibilities include supporting the deployment, configuration, and integration of cutting-edge security technologies, emphasizing system hardening and network fortification.
- Collaborative Support: Collaborate with senior cybersecurity engineers to execute critical cybersecurity functions. Assist in the assessment, design, and implementation of security measures.
- Security Technology Implementation: Play a hands-on role in the installation and integration of security technologies, focusing on next-generation solutions that enhance cyber defenses. Contribute to the setup of intrusion detection and prevention systems, firewalls, and security software.
- System Hardening: Support the process of system hardening to reduce vulnerabilities and enhance security posture. Implement security configurations and controls on various operating systems and platforms.
- Network Fortification: Assist in the configuration of network security settings and devices to bolster defenses against cyber threats. Collaborate in the setup of secure network architectures and segmentation strategies.
- Monitoring and Analysis: Work alongside cybersecurity engineers in monitoring security events and conducting preliminary analyses. Help identify potential threats and vulnerabilities within the infrastructure.
- Incident Response Support: Contribute to incident response activities by providing valuable assistance during security incidents. Assist in containment and mitigation efforts under the guidance of senior team members.
- Documentation and Reporting: Maintain accurate documentation of security configurations, changes, and incident reports. Assist in the preparation of reports that summarize security activities and findings.
- Security Awareness: Stay informed about the latest cybersecurity threats, trends, and best practices. Continuously expand your knowledge and skills to better support the cybersecurity team.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 2 YEARS

HACS Cybersecurity Analyst

- Identify, analyze, and mitigate system vulnerabilities. Under supervision, execute the following tasks: Develop and advocate information security best practices. Create compliant cybersecurity policies aligned with industry standards and client needs. Aid in crafting cybersecurity documentation, including integration guides, SSPs, POA&Ms, etc. Detect, assess, and mitigate system vulnerabilities.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 2 YEARS

HACS Engineer / Analyst (Principal)

- Establishes rigorous system engineering and cybersecurity requirements through the analysis of information engineers, emphasizing the development of enterprise-wide or large-scale information technology systems with a strong focus on cybersecurity.
- Architects comprehensive solutions encompassing software, hardware, and communication elements, prioritizing robust security to meet current and future cross-functional requirements and interfaces.
- Ensures systems align with and adhere to open systems architecture standards (such as OSI, ISO, IEEE, OSE), with a specific emphasis on cybersecurity considerations for implementing and specifying information technology solutions.
- Analyzes system requirements, emphasizing cybersecurity, and devises design alternatives to fulfill those requirements.
- Assumes a leadership role in delivering technical solutions for engineering studies and internet/intranet applications, with a cybersecurity-first approach.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Engineer / Analyst (Senior)

- Lead the development, programming, and secure deployment of government information technology systems.
- Oversee all software development phases, focusing on analysis, coding, testing, and documentation.
- Identify and integrate emerging cybersecurity technologies to support strategic planning aligned with cybersecurity priorities.
- Conduct cybersecurity assessments, evaluations, site surveys, and requirements analysis.
- Generate technical reports and documentation to record results.
- Collect data through surveys, document reviews, and interviews.
- Provide group facilitation, training, and knowledge transfer, including cross-functional team building and conflict resolution.
- Model process and data flows manually or with automation, including data flow diagrams and simulation models. Prototype database systems with cybersecurity measures.
- Design transaction-driven modules for online and internet/intranet environments with security in mind.
- Develop test environments for new applications with a focus on secure database interactions.
- Create entity relationship models and metadata descriptions for database designs.
- Administer and maintain databases, resolve user issues, implement security enhancements, and ensure database operations and maintenance align with cybersecurity best practices.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Enterprise Architect (Master)

- Architect and design cybersecurity solutions for clients' enterprise systems while ensuring effective execution.
- Provide thought leadership to stakeholders, offering technical oversight during solution deployments.
- Understand and address the client's strategic and programmatic cybersecurity needs.
- Propose and implement effective security solutions for enterprise environments, aligning them with business and technology strategies.
- Identify, communicate, and mitigate current and emerging security threats through architectural design.
- Create solutions that harmonize business requirements with robust cybersecurity measures.
- Identify security design deficiencies in existing and proposed architectures and recommend necessary enhancements.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Governance, Risk, and Compliance (Lead)

- Lead the development of cybersecurity best practices and implement repeatable cybersecurity methodologies.
- Apply Risk Management Framework (RMF) principles to secure system authorizations.
- Offer technical expertise in cyber governance, risk management, and compliance.
- Manage cybersecurity and information assurance system requirements.
- Develop and program partner-specific cybersecurity requirements based on the RMF control catalog.
- Conduct independent cybersecurity assessments for systems in development, documenting residual risk and system deficiencies.
- Provide remediation recommendations for cybersecurity compliance.
- Review and enhance integrator-provided cybersecurity documentation to ensure compliance.
- Generate technical data to support RMF activities.
- Develop governance, risk, and compliance documentation, including cybersecurity policies, plans, and procedures.
- Collaborate with stakeholders to customize GRC documentation.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Information Assurance Engineer (Journeyman)

- Under guidance, conduct thorough security assessments using the Risk Management Framework (RMF), applying knowledge of Confidentiality, Integrity, and Availability Levels and National Institute of Standards and Technology (NIST) Special Publication 800-53 controls associated with each level.
- Evaluate information assurance systems in both unclassified and classified environments to meet client requirements and industry best practices.
- Review policy, procedures, SOPs, and previous accreditation documents; compile and produce deliverables for client presentations.
- Collaborate with the client to assess the applicability and compliance of Information Assurance Controls.
- Prepare and review program documentation, including Risk Assessment Reports, Accreditation Packages, and security policy guides.
- Ensure adherence to client requirements and industry standards in performing cybersecurity and information assurance tasks.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 4 YEARS

HACS Information Assurance Engineer (Master)

- Execute cybersecurity and Information Assurance procedures for all client-managed systems, applications, and hardware within the environment.
- Offer subject matter expertise in Security and Vulnerability tools, as well as Risk Management Framework (RMF).

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Information Assurance Engineer (Senior)

- Contribute to the development and implementation of the client's Cybersecurity and Information Assurance Program. Monitor all Operations and Infrastructure, ensuring the maintenance of security tools and technology.
- Oversee internal and external policy compliance, regulation compliance, and risk mitigation across the security system's infrastructure.
- Additionally, execute cybersecurity and Information Assurance procedures for all client-managed systems, applications, and hardware.
- Perform security/vulnerability scans using provided Security and Vulnerability tools.
- Demonstrate expert knowledge of the Risk Management Framework (RMF).

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Information Assurance Engineer (SME)

- Conduct cybersecurity and information assurance activities for all systems, applications, and hardware managed by the client within the environment.
- Responsibilities include offering subject matter expertise in Security and Vulnerability tools and the Risk Management Framework (RMF).

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Information Systems Security Officer

- Provide expertise in the Risk Management Framework (RMF) and support various aspects of Cybersecurity, including inspections, operations, and orders processing.
- Assist in executing RMF processes, support security assessment and authorization activities for information systems, and maintain a 100% Authorization to Operate (ATO) status.
- Additionally, contribute to cybersecurity-related audits, inspections, and assessments, ensuring compliance with client requirements and industry standards.
- Responsibilities also involve conducting regular audits, inspections, and assessment reports, as well as providing status briefings and reports on remediation efforts.
- You'll play a key role in developing system security contingency plans and disaster recovery plans.
- Assist in implementing programs to promote awareness of and adherence to system security policies and procedures among systems, networks, and data users. Ensuring the rigorous application of information security and information assurance practices in all IT services delivery will be central to your role.
- Help coordinate user and privileged account processing and ensure the proper confirmation and documentation of certification information.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Information Systems Security Officer (Journeyman)

- Provide expertise in the Risk Management Framework (RMF) to support various aspects of Cybersecurity, including inspections, operations, and orders processing.
- Actively participate in RMF processes, assisting in security assessment and authorization activities for information systems while maintaining a 100% Authorization to Operate (ATO) status.
- Aid in cybersecurity-related audits, inspections, and assessments, ensuring compliance with both client requirements and industry standards.
- Conduct regular audits, inspections, and assessment reports, as well as delivering status briefings and reports on remediation efforts.
- Develop of system security contingency plans and disaster recovery plans.
- Contribute to the development and implementation of programs to ensure that systems, networks, and data users are well-informed, understand, and adhere to system security policies and procedures.
- Ensure the rigorous application of information security and information assurance policies, principles, and practices in the delivery of all IT services.
- Assist in coordinating user and privileged account processing and ensure the proper confirmation and documentation of certification information.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 4 YEARS

HACS Information Systems Security Officer (Senior)

- Provide subject matter expertise and knowledge of RMF.
- Lead cybersecurity inspections, operations, and orders processing.
- Perform RMF for all information systems and applications.
- Lead the security assessment and authorization activities for information systems, maintaining 100% ATO status.
- Follow RMF to identify, implement, assess, and manage cybersecurity capabilities and services, expressed as security controls, and authorizing the operation of an information system.
- Lead cybersecurity-related audits, inspections, and assessments.
- Ensure information systems comply with client requirements and industry standards.
- Help conduct the appropriate remediation actions associated with findings from inspections and evaluations, generate status reports, and brief clients.
- Develop system security contingency plans and disaster recovery plans.
- Develop and implement programs as required to ensure that systems, networks, and data users are aware of, understand, and adhere to systems cybersecurity policies and procedures.
- Ensure the rigorous application of cybersecurity policies, principles, and practices in the delivery of all IT cybersecurity services.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Penetration Tester

- Conduct comprehensive approach to assessing and strengthening security systems.
- Conduct rigorous tests aimed at deliberately exploiting vulnerabilities in existing computer systems and software.

- Detect weaknesses and potential threats, which will then enable you to develop recommendations and implement effective solutions to enhance the cybersecurity posture of IT systems.
- Play a vital role in safeguarding the integrity and security of critical digital assets.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 4 YEARS

HACS Program Manager (Master)

- Cybersecurity Leader responsible for overseeing all contract personnel and serve as Avint's primary point-of-contact for all matters related to contract performance.
- Is ultimately responsible for all contractual deliverables, ensuring operational excellence, and ensuring program activities stay on schedule and within budget.
- Track and report performance of Team.
- Act as a liaison between the team and the Government.
- Provide technical guidance to meet Government requirements.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS RMF Information Systems Security Officer

- Ultimately responsible for the cybersecurity posture for assigned information system boundaries.
- Develop, maintain, and manage cyber security and information assurance related technical system requirements.
- Review and provide feedback on cybersecurity documentation to ensure they meet cybersecurity requirements.
- Help ensure systems meet cybersecurity standards.
- Verify and validate systems are built, configured, and hardened in a way that will pass assessment and receive authorization.
- Develop and document remediations for technical areas that cannot be hardened following best practices.
- Execute and document risk assessments of systems to evaluate compliance with government requirements and industry best practices.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Security Control Assessor (Senior)

- Cybersecurity professional, conducts independent comprehensive assessments of the management, operational, and technical security/privacy controls and control enhancements employed within or inherited by information technology (IT) systems to determine the overall effectiveness of the controls.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Security Tools Engineer (Senior)

- Design and deploy custom, cutting-edge cybersecurity tool solutions that meet the client's needs.
- Manage and maintain existing cybersecurity tools.
- Stay abreast of new and emerging technologies to continually provide client the best-value solutions.
- Deploy, manage, and maintain the endpoint security for systems applications in the IT environment.
- Conduct test analysis and technical evaluations for vulnerabilities.

- Recommend and apply cybersecurity countermeasures to mitigate identified risks.
- Troubleshoot and resolve technical and/or compliance issues.
- Provide weekly status reports and metrics including but not limited to vulnerability assessment results, patch management statics, asset inventory, system configurations, waver request generation / validation, and general information technology security guidance.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Splunk SME (Master)

- Conceptualize, design, implement, and maintain Splunk infrastructure solutions to support cybersecurity missions. Create, manage, and support automation solutions for Splunk deployment and orchestration. Conduct periodic architectural reviews of Splunk and related systems to assess effectiveness and propose and implement optimal solutions as required. Develop and manage comprehensive documentation, artifacts, procedures, and processes for the optimal management of the Splunk infrastructure. Work closely with all relevant stakeholders to solve technical problems at the network, system, and application levels.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS System Engineer

- Provide SME-level System Engineering Support for cybersecurity solutions.
- Ensure Network architecture meet defense in depth methodologies.
- Lead FIM implementation (File integrity management).
- Create and maintain SSP Documentation.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Technical Writer (Junior)

- Develop professional, informative documents designed for both technical and non-technical audiences, in support of cybersecurity solutions, missions and objectives.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 1 YEAR

HACS Technical Writer

- Develop professional, informative documents designed for both technical and non-technical audiences, in support of cybersecurity solutions, missions and objectives.

MINIMUM EDUCATION: Associate degree or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 2 YEARS

HACS Technical Writer (Senior)

- Develop professional, informative documents designed for both technical and non-technical audiences, in support of cybersecurity solutions, missions and objectives.

MINIMUM EDUCATION: BA/BS or equivalent work experience

MINIMUM YEARS OF EXPERIENCE: 4 YEARS

HACS Virtualization Engineer

- Design integrated cybersecurity solutions in virtualized enterprise and consumer systems.
- Leads systems planning, performance management, capacity planning, testing and validation, benchmarking, and information engineering.
- Perform technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for virtual systems.
- Create as-built and other systems drawings (flowcharts, diagrams).
- Design system security and data assurance.
- Analyze user requirements to automate or improve existing systems.
- Identify system integrity issues and solutions for the full system life cycle.
- Work with vendors to ensure operational capabilities.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Governance, Risk, and Compliance (SME)

- Develop and oversee Governance Risk and Compliance (GRC) programs and GRC program staff, supporting GRC policy, and needs of GRC executives and their teams.
- Knowledgeable of cybersecurity laws, policies, and procedures within the GRC domain.
- Provide guidance on security risks, mitigations, and input on GRC related technical risks.
- Assist in the creation and maintenance of GRC related policies.
- Engage in security risk assessments to identify gaps, provide recommendations.
- Support continuous compliance with policies and standards and collect and validate audit evidence.
- Drive remediation of any identified gaps.
- Advise on compliance frameworks.
- Advise and support audit requirements.
- Ensure all cybersecurity documentation is updated to reflect new federal mandates, policy releases or updated security frameworks. or updated security frameworks.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Project Manager (Master)

- Lead, coordinate, communicate, integrate, and maintain accountability for the overall success of cybersecurity projects.
- Ensure alignment with agency or enterprise priorities.
- Drive solutions involving finance, scheduling, technology, staffing, forecasting cost estimates, methodology, tools, and solution components.
- Ensure all contractual obligations are achieved.
- Apply knowledge of data, information, processes, organizational interactions, skills, and analytical expertise to manage projects.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Information Systems Security Officer (SME)

- Oversee the information assurance (IA) program of an information system.
- Oversee and ensure that the appropriate operational security posture (e.g., network and system security, physical and environmental protection, personnel security, incident handling, security training and awareness) is implemented and maintained for an information system or program.
- Advises the Authorizing Official (AO), an information system owner, or the Chief Information Security Officer (CISO) on the security of an information system or program.
- Provides Risk Management Framework (RMF) expertise and support with Cybersecurity Inspections, Operations, and Orders Processing.
- Support the security assessment and authorization activities for information systems.
- Assist in cybersecurity related audits, inspections, and assessments.
- Ensure information systems comply with client requirements and industry standards.
- Ensure system security documentation is current and authorization boundary is accurate for all information systems.
- Working knowledge of automated tools deployed in the environment is preferred.
- Ultimately responsible for the day-to-day cyber operations of assigned systems.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Platform Architect

- Provides high-level cybersecurity architectural expertise to managers and technical staff.
- Develops architectural products and deliverables for the enterprise and operational business lines.
- Develops strategy of system and the design infrastructure necessary to support that strategy.
- Advises on selection of technological purchases with regards to processing, data storage, data access, and applications development. Sets standards for the client/server relational structure and security for the organization (SQL, ORACLE, SYBASE, etc.).
- Advises of feasibility of potential future projects to management.
- Experience in the development and maintenance of systems, Integration Tier, Security, Standards compliance, business activity monitoring, systems design, system analysis, and development preferred.
- Experience in defining and implementing a systems architecture using a combination of COTS processing, networking and data storage components into an embedded solution preferred.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Agile Project Management (SME)

- Provide supervisory technical and administrative direction for personnel performing software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules, specifically for cybersecurity projects and initiatives.
- May serve as the Scrum Master and facilitate stand-ups and Sprint Review/Planning meetings.
- Manage the design, implementation and support of platform architecture.
- Analyze requirements for capabilities and determining system functions.
- Coordinate with Contractor Program Manager and Government Project Manager to ensure problem solution and user satisfaction.

- Prepare and deliver presentations on the system concept to colleagues, subordinates and user representatives.
- Systems analysis/programming experience preferred.
- Independent analysis/programming experience, with complete responsibility for tasks involving analysis, programming and implementation preferred.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Network Engineer

- Assist in the development and maintenance of network security communications.
- Assist in monitoring any disruptions to ensure availability of the network.
- Use knowledge of LAN/WAN systems to help design and install internal and external networks.
- Test and evaluate network systems to eliminate problems and make improvements.
- Experience in the field or in a related area preferred.
- Familiarity with a variety of the field's concepts, practices, and procedures preferred.
- Relies on experience and judgment to plan and accomplish goals.
- Performs a variety of tasks. May lead and direct the work of others.
- A wide degree of creativity and latitude is preferred.
- Typically reports to a manager. Expert knowledge of LAN/WAN systems, networks, and applications preferred.
- Identification of security vulnerabilities and mitigation solutions.
- Working knowledge in vulnerability scan configuration and network modeling and network maintenance.
- May work with information security analyst to improve and implement security controls.
- Knowledgeable in existing COTS products is preferred.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

HACS Subject Matter Expert

- Serve as a cybersecurity subject matter expert, provide in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences.
- Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.
- Interfaces directly with stakeholders and executives as the responsible party to ensure all technical requirements are completed.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 8 YEARS

HACS Training Specialist (Senior)

- With an emphasis on cybersecurity, assesses, designs, and conceptualizes training scenarios, approaches, objectives, plans, tools, aids, curriculum, and other state of the art technologies related to training and behavioral studies.

- Identifies the best approach training requirements to include, but not limited to hardware, software, simulations, course assessment and refreshment, assessment centers, oral examinations, interviews, computer assisted and adaptive testing, behavior-based assessment and performance, and team and unit assessment and measurement.
- Develops and revises training courses. Prepares training catalogs and course materials. Trains personnel by conducting formal classroom courses, workshops, and seminars.
- Performs a review of organizational best practice in order to evaluate and implement current training needs.
- Design and conduct training to improve performance based on the evaluation of the organization's needs.
- Plan and coordinate training across all individuals and track/report key metrics.

MINIMUM EDUCATION: BA/BS or equivalent work experience
MINIMUM YEARS OF EXPERIENCE: 6 YEARS

SERVICE CONTRACT LABOR STANDARDS (SCLS) STATEMENT

The Service Contract Labor Standards, formerly the Service Contract Act (SCA), is applicable to this contract as it applies to all services provided. While no specific labor categories have been identified as being subject to SCLS 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 eligible labor categories. If and/or when the contractor adds SCLS labor categories/employees to the contract through the modification process, the contractor must inform the Contracting Officer and establish a SCLS matrix identifying the GSA labor category titles, the occupational code, SCLS labor category titles and the applicable WD number. Failure to do so may result in cancellation of the contract.