

GENERAL SERVICES ADMINISTRATION
AUTHORIZED FEDERAL SUPPLY SERVICE
MULTIPLE AWARDS SCHEDULE

Large Category: Information Technology

Sub Category: IT Services

Avint, LLC
40868 Tulip Poplar Place
Aldie, VA 20105
Phone: 703-678-9969
Email: Marcie.nagel@avintllc.com
www.avintllc.com

Contract Number: 47QTCA19D00KZ
Period Covered by Contract: September 12, 2019 through September 11, 2024

Pricelist current through modification #PS-A812, effective April 15, 2020

Products and ordering information in this Authorized FSS Information Technology Schedule Pricelist are also available on the GSA Advantage! System.

For more information on ordering from Federal Supply Schedule click on the FSS Schedules button at <http://www.fss.gsa.gov/>

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?



Cybersecurity Strategy

Building the vision for the future of cyber



Cybersecurity Engineering

Turning cyber vision into solutions



Cybersecurity Compliance

Meeting cyber mandates through automation and innovation



Management Consulting

Advising clients to solve complex problems



Cybersecurity Operations

Leading threat detection, investigation and



Identity, Credentials, Access Management

Ensuring authorized access to your technical and physical assets

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):

<u>SIN</u>	<u>DESCRIPTION</u>
54151HACS	Highly Adaptive Cybersecurity Services (HACS)
54151S	Information Technology Professional Services
OLM	Order-Level Materials

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN: See Price List

1c. SERVICES OFFERED: See Price List

2. MAXIMUM ORDER PER SIN:

<u>SIN</u>	<u>MAXIMUM ORDER</u>
54151HACS	\$500,000 per SIN/Order
54151S	\$500,000 per SIN/Order

This maximum order threshold is a dollar amount at which it is suggested that the ordering agency request higher discounts from the contractor before issuing the order. The contractor may: (1) Offer a new lower price, (2) Offer the lowest price available under the contract, or (3) Decline the order within five (5) days. In accordance with the Maximum Order provisions contained in the Schedule, a delivery order may be placed against the Schedule contract even though it exceeds the maximum order threshold.

3. MINIMUM ORDER: \$100

4. GEOGRAPHIC COVERAGE (DELIVERY AREA): Domestic Only

5. POINT OF PRODUCTION: United States

6. BASIC DISCOUNT: Prices listed are net, discounts have been deducted and the Industrial Funding Fee has been added

7. QUANTITY DISCOUNT: 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

- 9a. **GOVERNMENT PURCHASE CARDS ARE ACCEPTED UP TO THE MICRO-PURCHASE THRESHOLD.**
- 9b. **GOVERNMENT PURCHASE CARDS ARE ACCEPTED ABOVE THE MICRO-PURCHASE THRESHOLD.**
10. **FOREIGN ITEMS:** None
- 11a. **TIME OF DELIVERY:** As negotiated with the Ordering Agency
- 11b. **EXPEDITED DELIVERY:** Contact Contractor
- 11c. **OVERNIGHT AND 2-DAY DELIVERY:** Contact Contractor
- 11d. **URGENT REQUIREMENTS:** Contact Contractor
12. **F.O.B. POINT:** FOB Destination
- 13a. **ORDERING ADDRESS:** Avint, LLC
40868 Tulip Poplar Place
Aldie, VA 20105
- 13b. **ORDERING PROCEDURES:** *For supplies and service the ordering procedures, information on Blanket Purchase Agreements (BPAs) are found in Federal Acquisition Regulation (FAR) 8.405-3*
14. **PAYMENT ADDRESS:** Same as Ordering Address
15. **WARRANTY PROVISION:** Standard Commercial Warranty
16. **EXPORT PACKING CHARGES:** Not Applicable
17. **TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE:**
None
18. **TERMS AND CONDITIONS OF RENTAL:** Not Applicable
19. **TERMS AND CONDITIONS OF INSTALLATION:** Not Applicable

- 20a. TERMS AND CONDITIONS OF REPAIR PARTS:** Not Applicable
- 20b. TERMS AND CONDITIONS FOR ANY OTHER SERVICES:** See Terms and Conditions Section
- 21. LIST OF SERVICE AND DISTRIBUTION POINTS:** None
- 22. LIST OF PARTICIPATING DEALERS:** None
- 23. PREVENTIVE MAINTENANCE:** See Pricelist for available options
- 24a. SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (E.G., RECYCLED CONTENT, ENERGY EFFICIENCY AND/OR REDUCED POLLUTANTS):** Not Applicable
- 24b. SECTION 508 COMPLIANCE INFORMATION:** Not Applicable
- 25. DATA UNIVERSAL NUMBER SYSTEM (DUNS) NUMBER:** 079953992
- 26. AVINT, LLC HAS REGISTERED IN THE SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE.**
CAGE CODE: 7FU49

Avint LCAT Descriptions -- 54151S

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 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

Cyber Security Project Manager

- Acts 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

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 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 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 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

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

Avint LCAT Descriptions -- 54151HACS

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 and professional cyber security certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+)

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 and professional cyber security certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+)

MINIMUM YEARS OF EXPERIENCE: 7 YEARS

Cyber Security Project Manager

- Acts 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 and professional cyber security certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+)

MINIMUM YEARS OF EXPERIENCE: 8 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 and professional cyber security certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+)

MINIMUM YEARS OF EXPERIENCE: 10 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 and professional cyber security certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+)

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 and professional cyber security certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+)

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 and professional cyber security certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+)

MINIMUM YEARS OF EXPERIENCE: 6 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 and professional cyber security certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+)

MINIMUM YEARS OF EXPERIENCE: 7 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 and professional cyber security certification (e.g., CISSP, CISM, CISA, CEH, SEC +, CCNP, GCIH, GCED or CASP+)

MINIMUM YEARS OF EXPERIENCE: 5 YEARS

Avint GSA Price List

SIN(s)	SERVICE CATEGORY	UOI	SEPT 12 2019 thru SEPT 11 2020	SEPT 12 2020 thru SEPT 11 2021	SEPT 12 2021 thru SEPT 11 2022	SEPT 12 2022 thru SEPT 11 2023	SEPT 12 2023 thru SEPT 11 2024
54151S	IT Security Specialist (Senior)	Hourly	\$83.95	\$86.21	\$88.54	\$90.93	\$93.39
54151S	Cyber Security Project Manager	Hourly	\$146.88	\$150.84	\$154.92	\$159.10	\$163.40
54151S	Cyber Security Subject Matter Expert (Master)	Hourly	\$203.49	\$208.98	\$214.62	\$220.42	\$226.37
54151S	Cyber Security Subject Matter Expert (Senior)	Hourly	\$180.09	\$184.95	\$189.94	\$195.07	\$200.34
54151S	Cyber Security Subject Matter Expert	Hourly	\$134.66	\$138.30	\$142.03	\$145.86	\$149.80
54151S	Cyber Security Training Specialist (Senior)	Hourly	\$139.65	\$143.42	\$147.29	\$151.27	\$155.35
54151S	Quality Assurance Specialist (Master)	Hourly	\$132.27	\$135.84	\$139.50	\$143.27	\$147.14
54151S	Enterprise Architect	Hourly	\$162.79	\$167.18	\$171.70	\$176.33	\$181.10
54151S	Information Assurance/Security Specialist	Hourly	\$127.18	\$130.61	\$134.14	\$137.76	\$141.48
54151HACS	IT Security Specialist (Senior)	Hourly	\$83.95	\$86.21	\$88.54	\$90.93	\$93.39
54151HACS	Cyber Security Project Manager	Hourly	\$146.88	\$150.84	\$154.92	\$159.10	\$163.40
54151HACS	Cyber Security Subject Matter Expert (Master)	Hourly	\$203.49	\$208.98	\$214.62	\$220.42	\$226.37
54151HACS 54151S	Cyber Security Subject Matter Expert (Senior)	Hourly	\$180.09	\$184.95	\$189.94	\$195.07	\$200.34
54151HACS	Cyber Security Subject Matter Expert	Hourly	\$134.66	\$138.30	\$142.03	\$145.86	\$149.80
54151HACS	Cyber Security Training Specialist (Senior)	Hourly	\$139.65	\$143.42	\$147.29	\$151.27	\$155.35

SIN(s)	SERVICE CATEGORY	UOI	SEPT 12 2019 thru SEPT 11 2020	SEPT 12 2020 thru SEPT 11 2021	SEPT 12 2021 thru SEPT 11 2022	SEPT 12 2022 thru SEPT 11 2023	SEPT 12 2023 thru SEPT 11 2024
54151HACS	Quality Assurance Specialist (Master)	Hourly	\$132.27	\$135.84	\$139.50	\$143.27	\$147.14
54151HACS	Enterprise Architect	Hourly	\$162.79	\$167.18	\$171.70	\$176.33	\$181.10
54151HACS	Information Assurance/Security Specialist	Hourly	\$127.18	\$130.61	\$134.14	\$137.76	\$141.48

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.