APPENDIX C.1 SIN 54151HACS CYBERSECURITY LABOR RATES AND DESCRIPTIONS

LABOR RATES

SIN 54151HACS CyberSecurity Rate Template

Rates for 2023 Updated as of April 14, 2023

		(Jan 1, 2020 - Dec 31, 2020)		Year 1 (Jan 1, 2021 - Dec 31, 2021)	Year 2 (Jan 1, 2022 - Dec 31, 2022)	Year 3 (Jan 1, 2023 - Dec 31, 2023)	Year 4 (Jan 1, 2024 - Dec 31, 2024)	Year 5 (Jan 1, 2025 - Dec 31, 2025)
Labor Category	**Minimum Years of Experience (cannot be a range)**	**Degree**	**GSA PRICE w/IFF**	**GSA PRICE w/IFF**	**GSA PRICE w/IFF**	**GSA PRICE w/ IFF**	**GSA PRICE w/IFF**	**GSA PRICE w/IFF**
Security Analyst - Junior	1	Bachelor	$90.33	$92.13	$93.98	$112.77	$117.28	$120.80
Security Analyst - Intermediate	5	Bachelor	$126.68	$129.22	$131.80	$158.16	$164.48	$169.42
Security Analyst - Senior	7	Bachelor	$165.56	$168.87	$172.25	$215.31	$223.93	$230.65
Computer Network Defense (CND) Analyst - Junior	1	Bachelor	$101.79	$103.82	$105.90	$127.07	$132.15	$136.11
Computer Network Defense (CND) Analyst - Intermediate	5	Bachelor	$138.14	$140.90	$143.72	$179.65	$186.83	$192.43
Computer Network Defense (CND) Analyst - Senior	7	Bachelor	$177.01	$180.55	$184.17	$239.42	$248.99	$256.45
Security Architect - Junior	1	Bachelor	$142.71	$145.56	$148.47	$154.41	$160.58	$165.40
Security Architect - Intermediate	5	Bachelor	$179.06	$182.64	$186.29	$232.86	$242.17	$249.43
Security Architect - Senior	7	Bachelor	$217.93	$222.29	$226.74	$283.43	$294.76	$303.61
Information Assurance Analyst - Junior	1	Bachelor	$121.63	$124.06	$126.54	$145.52	$151.35	$155.89
Information Asurance Analyst - Intermediate	5	Bachelor	$157.98	$161.14	$164.36	$189.02	$196.57	$202.47
Information Assurance Analyst - Senior	7	Bachelor	$191.46	$195.29	$199.19	$239.03	$248.59	$256.05
Penetration Tester - Intermediate	3	Bachelor	$150.01	$153.01	$156.07	$179.48	$186.66	$192.26
Penetration Tester - Senior	6	Bachelor	$168.09	$171.45	$174.88	$218.60	$227.35	$234.17
Cybersecurity Engineer - Junior	1	Bachelor	$94.69	$96.58	$98.51	$118.21	$122.93	$126.62
Cybersecurity Engineer - Intermediate	5	Bachelor	$131.04	$133.66	$136.33	$163.60	$170.14	$175.24
Cybersecurity Engineer - Senior	7	Bachelor	$169.92	$173.31	$176.78	$212.13	$220.61	$227.23
Cybersecurity Technical Writer - Junior	1	Bachelor	$85.97	$87.69	$89.44	$107.32	$111.62	$114.96
Cybersecurity Technical Writer -Intermediate	5	Bachelor	$122.32	$124.77	$127.26	$159.08	$165.45	$170.42
CyberSecurity Assessment and Authorization (A&A) Analyst - Junior	1	Bachelor	$111.56	$113.79	$116.07	$133.48	$138.82	$142.98
CyberSecurity Assessment and Authorization (A&A) Analyst - Interme	5	Bachelor	$147.91	$150.87	$153.89	$184.68	$192.06	$197.82
CyberSecurity Assessment and Authorization (A&A) Analyst - Senior	7	Bachelor	$186.79	$190.53	$194.34	$242.92	$252.63	$260.21
Information Security Analyst (Data Protection) - Junior	1	Bachelor	$148.59	$151.56	$154.59	$160.78	$167.20	$172.22
Information Security Analyst (Data Protection) - Intermediate	5	Bachelor	$184.94	$188.64	$192.41	$211.66	$220.12	$226.72
Information Security Analyst (Data Protection) - Senior	7	Bachelor	$223.82	$228.29	$232.86	$256.15	$266.40	$274.39
Vulnerability Management Analyst - Junior	1	Bachelor	$143.55	$146.42	$149.34	$155.31	$161.53	$166.38
Vulnerability Management Analyst - Intermediate	5	Bachelor	$179.90	$183.50	$187.17	$205.88	$214.12	$220.54
Vulnerability Management Analyst - Senior	7	Bachelor	$218.77	$223.15	$227.61	$250.38	$260.39	$268.20
Cloud Computing Security Specialist (CCSS)-Subject Matter Expert (SM	3	Bachelor	$173.99	$177.47	$181.02	$188.26	$195.79	$201.66
Cloud Computing Security Specialist (CCSS)-Subject Matter Expert (SM	5	Bachelor	$217.27	$221.61	$226.05	$271.25	$282.11	$290.57
Cloud Computing Security Specialist (CCSS)-Subject Matter Expert (SM	7	Bachelor	$278.39	$283.96	$289.64	$347.57	$361.47	$372.31
Operational Technology Security Engineer - Junior	1	Bachelor	$134.90	$137.60	$140.35	$145.96	$151.80	$156.35
Operational Technology Security Engineer - Intermediate	5	Bachelor	$171.25	$174.68	$178.17	$195.99	$203.83	$209.94
Operational Technology Security Engineer - Senior	7	Bachelor	$210.13	$214.33	$218.62	$240.48	$250.11	$257.61

DESCRIPTIONS

SECURITY ANALYST

Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security. Performs all procedures necessary to ensure the safety of the organization's systems, information, and transactions across the Internet/intranet. Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Identifies and mitigates vulnerabilities using alternate or compensating controls if necessary. Applies Internet firewall technologies to maintain security. Ensures that the user community understands and adheres to necessary procedures to maintain security. Updates and deletes users, monitors and performs follow-up on compliance violations, and develops security policies, practices, and guidelines. Supports Security Operations Center (SOC).Assists with the installation, daily operation, and maintenance of IA systems to include technical support, troubleshooting, and system testing.

- Relevant certification from a nationally recognized organization (e.g. CISSP, CEH, CISM, CISA).

COMPUTER NETWORK DEFENSE (CND) ANALYST

Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats. Performs actions to protect, monitor, detect, analyze, and respond to unauthorized activity within assigned information systems and computer networks. Employs Cybersecuritycapabilities and deliberate actions to respond to a CND alert or emerging situational awareness/threat. Serves as an expert on CND requirements and compliance to such requirements by using IA tools and techniques to perform compliance analysis and correlation, tracking and remediation coordination, and escalating CND non-compliance. Provides technical analysis and sustainment support for the enterprise for IA tools and applications, and assists with the application of Defense-In-Depth signatures and perimeter defense controls to diminish network threats.

- Relevant certification from a nationally recognized organization (e.g. CISSP, CEH, CISM, CISA).

SECURITY ARCHITECT

Responsible for guiding the design and implementation of secure solutions and services across business and IT support areas. Driving the successful configuration and implementation of security solutions to reduce risk to an acceptable level. Ensures that the stakeholder security requirements necessary to protect the organization’s mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. Serves as an IA Subject Matter Expert (SME) with regards to IA Architecture policies and procedures. Provides IA Management support to Program Management Offices (PMO) for emerging information systems through the acquisition lifecycle and where applicable into sustainment. Provides technical support and guidance to facilitate the identification and integration of IA controls at the onset of the acquisition lifecycle for emerging IT capabilities. Serves as a principal liaison for Enterprise-level boundary defense initiatives to ensure consistent and sufficient identification and implementation of applicable IA controls in concert with the agency IA and IT architecture and National Institute of Standards and Technology (NIST) security guidelines. Provides oversight for the design and implementation of Enterprise-level IA solutions providing standards for access control capabilities across the Enterprise.

Qualifications:

- Knowledge and experience in managing information technology services and strategies
- Relevant certification from a nationally recognized organization (e.g. CISSP, CEH, CISM, CISA).

INFORMATION ASSURANCE ANALYST – SENIOR

Conducts comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-53 and/or SP 800-37). Demonstrated ability to independently perform complex security analysis of applications and systems for compliance with security requirements. Performs cybersecurity vulnerability evaluations. Uses a variety of security techniques, technologies, and tools to evaluate security posture in highly complex computer systems and networks. Analyzes and defines security requirements for systems, applications and infrastructure. Recommends solutions to meet security requirements. Gathers and organizes technical information about an organization's mission goals and needs, and makes recommendations to improve existing security posture. Demonstrated experience and ability to provide enterprise-wide technical analysis and direction for problem definition, analysis and remediation for complex systems and enclaves. Ability to provide workable recommendations and advice to client executive management on system security posture and process improvements, optimization and maintenance. Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance. Reviews, consolidates, develops and/or implements cybersecurity policy in accordance with agency/client and NIST security requirements and assess IT policies, standards, guidelines or procedures to ensure a balance of security and operational requirements.

Qualifications:

- Strong analytical and problem solving skills for resolving security issues
- Relevant certification from a nationally recognized organization (e.g. CISSP, CEH, CGEIT, CRISC, CISM, CISA).

INFORMATION ASSURANCE ANALYST- INTERMEDIATE

Under general supervision, conducts comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-53 and/or SP 800-37). Demonstrated ability to independently perform complex security analysis of applications and systems for compliance with security requirements. Performs cybersecurity vulnerability evaluations. Uses a variety of security techniques, technologies, and tools to evaluate security posture in highly complex computer systems and networks. Analyzes and defines security requirements for systems, applications and infrastructure. Recommends solutions to meet security requirements. Gathers and organizes technical information about an organization's mission goals and needs, and makes recommendations to improve existing security posture. Demonstrated experience and ability to provide enterprise-wide technical analysis and direction for problem definition, analysis and remediation for complex systems and enclaves. Ability to provide workable recommendations and advice to client executive management on system security posture and process improvements, optimization and maintenance. Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance. Reviews, consolidates, develops and/or implements cybersecurity policy in accordance with agency/client and NIST security requirements and assess IT policies, standards, guidelines or procedures to ensure a balance of security and operational requirements.
Qualifications:

- Strong analytical and problem solving skills for resolving security issues
- Relevant certification from a nationally recognized organization is preferred (e.g. CISSP, CEH, CISM, CISA).

PENETRATION TESTER – SENIOR

Demonstrated ability to independently perform penetration testing of applications, systems and enclaves belonging to or managed by clients. Identifies security flaws in computing platforms and applications and devise strategies and techniques to mitigate identified cybersecurity risks. Perform application and network penetration testing and wireless security assessments. Apply offensive cybersecurity testing techniques, coordinate testing projects with internal and external system owners. Reports the nature of identified cyber security risks and recommends risk mitigation measures to improve the cyber security posture of the enterprise.

- Qualifications

  - Proven proficiency in performing extensive vulnerability assessment and penetration testing.
  - Experience with testing tools, including NESSUS, METASPLOIT, CANVAS, NMAP, Burp Suite, and Kismet
  - Experience with network vulnerability assessments and penetration testing methods
  - Experience with writing testing assessment reports

- Relevant certification from a nationally recognized organization (e.g. CISSP, CEH, LPT, CEPT, CISM, CISA).
- Knowledge of open security testing standards and projects, including OWASP

PENETRATION TESTER - INTERMEDIATE

Under general supervision, perform penetration testing of applications, systems and enclaves belonging to or managed by clients. Identify security flaws in computing platforms and applications and devise strategies and techniques to mitigate identified cybersecurity risks. Perform application and network penetration testing and wireless security assessments. Apply offensive cybersecurity testing techniques, coordinate testing projects with internal and external system owners. Reports the nature of identified cyber security risks and recommends risk mitigation measures to improve the cyber security posture of the enterprise.

- Qualifications
  - Proven proficiency in performing vulnerability assessment and penetration testing.
  - Experience with testing tools, including NESSUS, METASPLOIT, CANVAS, NMAP, Burp Suite, and Kismet
  - Experience with network vulnerability assessments and penetration testing methods
  - Experience with writing testing assessment reports
  - Relevant certification from a nationally recognized organization (e.g. CISSP, CEH, LPT, CEPT, CISM, CISA).
  - Knowledge of open security testing standards and projects, including OWASP

CYBERSECURITY ENGINEER

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Identifies and mitigates vulnerabilities using alternate or compensating controls if necessary. Supports, monitors, tests, and troubleshoots IA software issues in conjunction with other IA staff to ensure timely response actions to security incidents. Recognizes potential security violations, takes appropriate action to report the incident as required by regulation, and mitigates any adverse impact. Implements applicable patches including vulnerabilities from the National Vulnerability Database, US CERT alerts, IA vulnerability alerts (IAVA), IA vulnerability bulletins (IAVB), and technical advisories (TA) for assigned operating system(s), Under technical supervision, performs information assurance activities in data center environments. Supports Security Operations Center (SOC). Assists with the installation, daily operation, and maintenance of IA systems to include technical support, troubleshooting, and system testing. Conducts and/or supports authorized penetration testing on enterprise network assets.

Performs a variety of routine project tasks applied to specialized Cybersecurity problems. Tasks involve integration of tools and processes or methodologies to resolve total system problems, or technology problems as they relate to cybersecurity requirements. Analyzes information security requirements. Applies analytical and systematic approaches in the resolution of problems of work flow, organization, and planning. Provides security engineering support for planning, design, development, testing, demonstration, integration of information systems.

- Minimum Experience/ Qualification:
  -
  - Relevant certification from a nationally recognized organization (e.g. CISSP, CEH, CISM, CISA).
  - Experience with security tools such as SIEM tools, vulnerability scanners, monitoring tools and incident response processes and tools

CYBERSECURITYASSESSMENT AND AUTHORIZATION (A&A/C&A) ANALYST

Serves as a cybersecurity Subject Matter Expert (SME) with regards to Authorization of information systems and all associated cybersecurity policies and procedures. Fully versed in the general tenets supporting the overall organization implementation of its authorization process, to include supporting cybersecurity policy, procedures and processes. Performs a cybersecurity process while either authorizing an information system or serving as a SME for an information system undergoing authorization. Possess an understanding of how the security controls identified in the NIST 800-53 apply to the process of assessing and authorizing a large organization's IT infrastructure, in which there is a compilation of large and small enclaves, applications and IT processes. Determines the applicable severity value for an identified vulnerability (e.g., non-compliant security control), and determines the possible ramifications on the system's current or future authorization. Required to brief senior management on the progress or results of an information system undergoing the authorization process. Prepares, reviews, and evaluates documentation of compliance. Verifies that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. Reviews IA and IA enabled software, hardware, and firmware for compliance with appropriate security configuration guidelines, policies, and procedures. Developed, reviews or updates IA security plans and A&A documentation. Identifies alternative functional IA security strategies to address organizational security concerns. Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. Prepares, recommendations for the Designated Approving Authority (DAA) or Authorizing Official (AO).

- Minimum Experience:
- Relevant A&A (formerly known as C&A) experience;

- Risk Management Framework (RMF) and NIST A&A experience;
- Experience in assessing security controls and conducting authorization reviews for large, complex organizations.

        - Relevant certification from a nationally recognized organization (e.g. CISSP, CEH, CISM, CISA).

CYBERSECURITY TECHNICAL WRITER

Under general supervision, edits and rewrites documents for grammatical, syntactical, and usage errors, spelling, punctuation, and adherence to standards. Proofreads documentation and graphics for accuracy and adherence to original content provides quality control checking for documents received from photocopying and word processing; assembles Master copies, including graphics, appendices, table of contents, and title pages; assists in scheduling printing, and copying. Assists in document tracking and logging, and consults with technical staff to determine format, contents, and the organization of technical reports and proposals. Assists in collecting and organizing information required for preparation of user's manuals, training materials, installation guides, proposals, and reports. Edits functional descriptions, system specifications, user's manuals, special reports, or any other customer deliverables and documents.

- Minimum Experience:
    - Relevant Technical Writing experience

CLOUD COMPUTING SECURITY SPECIALIST (CCSS)-SUBJECT MATTER EXPERT (SME)

Serves as an Information Assurance and Cloud computing SME with regards to Assessment and Authorization (A&A) (formerly known as C&A) and a broad coverage of the application of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) standards and guidance as outlined in the NIST Special Publication(s) (SP) 800-53 and 800-37 (Current versions). Possesses the ability to work independently with substantial cloud computing security knowledge. The assessor must have the essential skill sets to identify, manage and resolve cloud computing security risk and implement "best practices" as applied within a cloud environment (across all of the different deployment and service models, and derivatives).The CCSS must be well versed in FedRAMP assessment methodology of security and privacy controls deployed in cloud information systems to include six (6) domain areas. The six domains include:

- Architectural Concepts & Design Requirements
- Cloud Data Security
- Cloud Platform & Infrastructure Security
- Cloud Application Security
- Operations
- Legal & Compliance

Qualifications:

- Relevant A&A experience; Risk Management Framework (RMF) and NIST A&A experience
- Relevant certification from a nationally recognized organization (e.g. CISSP, CCSP, CCSK, CEH, CISM, CISA).
- Experience in assessing IA Controls and conducting A&A reviews for large, complex Information systems

INFORMATION SECURITY ANALYST (DATA PROTECTION)

Serves as information security analyst performing incident response (identification, containment, eradication, recovery) for Personally Identifiable Information (PII) incidents and PII-related data breaches. Investigates, analyzes, and responds to cyber incidents within the network environment or enclave. Utilizes data loss prevention (DLP) tools to identify improperly stored PII data at rest and improperly transmitted PII data. Performs the quarantining of improperly stored PII data. Recommends appropriate actions to mitigate the risk of unauthorized access to PII data and ensures the implementation of appropriate security controls to safeguard PII data. Engages with stakeholders and mission partners to facilitate containment, eradication, and recovery for PII incidents. Validates remedial actions and ensures compliance with NIST and agency specific information security and privacy policy.

Qualifications

- Relevant certification from a nationally recognized organization (e.g. CISSP, CEH, CISM, CISA).
- Hands-on experience performing computer security incident handling
- Hands-on experience with data loss prevention software/tools

OPERATIONAL TECHNOLOGY SECURITY ENGINEER

Performs a variety of routine project tasks applied to specialized information assurance problems with IT systems. Tasks involve integration of processes or methodologies with information systems to resolve total system problems, or technology problems as they relate to IA requirements. Analyzes information security requirements. Applies analytical and systematic approaches in the resolution of problems of work flow, organization, and planning. Provides security engineering support for planning, design, development, testing, demonstration, integration of IT systems.

VULNERABILITY MANAGEMENT ANALYST
Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. Serves as vulnerability management analyst for assigned applications. Analyzes vulnerabilities and characterizes risk. Engages with stakeholders and mission partners to facilitate application, infrastructure and/or web vulnerability assessments. Performs code review, software assurance testing, and application vulnerability scanning. Facilitates the coordination of remediation efforts, prioritizing remediation efforts based on risk. Recommends appropriate actions to remediate vulnerabilities and mitigate risks and ensures the implementation of appropriate security settings to include those required by NIST and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). Tracks and reports security and compliance issues. Validates remedial actions and ensures compliance with NIST and agency specific information security policy.
Qualifications:

- Hands-on experience working with application vulnerability scanners
- Understanding of application vulnerabilities and remediation techniques

Substitution Table

Degree	Experience Equivalence	Other Equivalence
Bachelors	Associate degree +2 years relevant experience or 6 years relevant experience	Professional certifications such as (CompTIA Security + -CPTE - Certified Penetration Testing Engineer or CEH - Certified Ethical Hacker -Certified Information System Security Professional (CISSP), CISA, CISM, CRISC)
Masters (Advanced degree)	Bachelors +2 years relevant experience, or Associate + 4 years relevant experience	Masters Certificate or Professional license
Doctorate (Advanced degree)	Masters + 2 years relevant experience, or Bachelors + 4 years relevant experience	
* Successful completion of higher education which has not yet resulted in a degree may be counted as 1 year of experience for each year of college completed. * Skill Level minimum years of experience is defined as total years of experience		