APPENDIX C.1 SIN 132-45 CYBERSECURITY LABOR RATES AND DESCRIPTIONS

LABOR RATES

SIN 132-45 CyberSecurity Rate Template

GS-35F-110DA - SINs 132-45A, 132-45B, 132-45C, 132-45D

GS-35F-110DA - SINs 132-45A, 132-45B, 132-45C, 132-45D							
Labor Category	Minimum Education / Certification Level	Minimum Years of Experience	Contractor or Customer Facility or Both		GSA Price (Including IFF) Effective August 2018 - Dec 31, 2018	GSA Price (Including IFF) Effective Jan 2019 - Dec 31, 2019	GSA Price (Including IFF) Effective Jan 2020 - Dec 31, 2020
Security Analyst - Junior	Bachelors	1	Both		$86.82	$88.56	$90.33
Security Analyst - Intermediate	Bachelors	5	Both		$121.76	$124.20	$126.68
Security Analyst - Senior	Bachelors	7	Both		$159.13	$162.31	$165.56
Computer Network Defense (CND) Analyst – Junior	Bachelors	1	Both		$97.83	$99.79	$101.79
Computer Network Defense (CND) Analyst - Intermediate	Bachelors	5	Both		$132.77	$135.43	$138.14
Computer Network Defense (CND) Analyst - Senior	Bachelors	7	Both		$170.14	$173.54	$177.01
Security Architect - Junior	Bachelors	1	Both		$137.16	$139.91	$142.71
Security Architect - Intermediate	Bachelors	5	Both		$172.11	$175.55	$179.06
Security Architect - Senior	Bachelors	7	Both		$209.47	$213.66	$217.93
Information Assurance Analyst - Junior	Bachelors	1	Both		$116.90	$119.24	$121.63
Information Assurance Analyst - Intermediate	Bachelors	5	Both		$151.85	$154.88	$157.98

Information Assurance Analyst – Senior	Bachelors	7	Both		$184.03	$187.71	$191.46
Penetration Tester - Intermediate	Bachelors	3	Both		$144.19	$147.07	$150.01
Penetration Tester - Senior	Bachelors	6	Both		$161.56	$164.79	$168.09
Cybersecurity Engineer - Junior	Bachelors	1	Both		$91.01	$92.83	$94.69
Cybersecurity Engineer – Intermediate	Bachelors	5	Both		$125.95	$128.47	$131.04
Cybersecurity Engineer - Senior	Bachelors	7	Both		$163.32	$166.58	$169.92
Cybersecurity Technical Writer – Junior	Bachelors	1	Both		$82.63	$84.28	$85.97
Cybersecurity Technical Writer -Intermediate	Bachelors	5	Both		$117.57	$119.92	$122.32
CyberSecurity Assessment and Authorization (A&A) Analyst - Junior	Bachelors	1	Both		$107.23	$109.37	$111.56
CyberSecurity Assessment and Authorization (A&A) Analyst – Intermediate	Bachelors	5	Both		$142.17	$145.01	$147.91
CyberSecurity Assessment and Authorization (A&A) Analyst - Senior	Bachelors	7	Both		$179.54	$183.13	$186.79
Information Security Analyst (Data Protection) - Junior	Bachelors	1	Both		$142.82	$145.68	$148.59
Information Security Analyst (Data Protection) - Intermediate	Bachelors	5	Both		$177.76	$181.32	$184.94
Information Security Analyst (Data Protection) - Senior	Bachelors	7	Both		$215.13	$219.43	$223.82
Vulnerability Management Analyst – Junior	Bachelors	1	Both		$137.97	$140.73	$143.55

Vulnerability Management Analyst – Intermediate	Bachelors	5	Both		$172.91	$176.37	$179.90
Vulnerability Management Analyst – Senior	Bachelors	7	Both		$210.28	$214.48	$218.77
Cloud Computing Security Specialist (CCSS)-Subject Matter Expert (SME) – Staff	Bachelors	3	Both		$167.71	$171.06	$174.48
Cloud Computing Security Specialist (CCSS)-Subject Matter Expert (SME) – Intermediate	Bachelors	5	Both		$208.83	$213.01	$217.27
Cloud Computing Security Specialist (CCSS)-Subject Matter Expert (SME) – Senior	Bachelors	7	Both		$267.58	$272.94	$278.39
Operational Technology Security Engineer - Junior	Bachelors	1	Both		$129.66	$132.26	$134.90
Operational Technology Security Engineer - Intermediate	Bachelors	5	Both		$164.60	$167.90	$171.25
Operational Technology Security Engineer - Senior	Bachelors	7	Both		$201.97	$206.01	$210.13
			Jan 1, 2017 -Dec 31,2017	**Jan 1, 2018-Jun 30,2018**	**July 1, 2018-Dec 31,2018**	**Jan 1, 2019 -Dec 31,2019**	**Jan 1, 2020 -Dec 31,2020**
GSA Service Proposed (e.g. Labor Category or Job Title/Task)	Minimum Education / Certification Level	Minimum Years of Experience	Proposed GSA Price (Including IFF)	**Proposed GSA Price (Including IFF)**	**Proposed GSA Price (Including IFF)**	**Proposed GSA Price (Including IFF)**	**Proposed GSA Price (Including IFF)**
Architect I	Bachelors	1	$150.87	**$153.02**	**$153.02**	**$153.02**	**$153.02**

Architect II	Bachelors	3	$181.29	**$184.14**	**$184.14**	**$184.14**	**$184.14**
Architect III	Bachelors	5	$211.72	**$215.25**	**$215.25**	**$215.25**	**$215.25**
Architect IV	Bachelors	7	$256.47	**$260.14**	**$260.14**	**$260.14**	**$260.14**
Architect V	Bachelors	12	$318.79	**$323.96**	**$323.96**	**$323.96**	**$323.96**
Business Analyst I	Bachelors	1	$120.70	**$122.42**	**$122.42**	**$122.42**	**$122.42**
Business Analyst II	Bachelors	3	$166.45	**$168.83**	**$168.83**	**$168.83**	**$168.83**
Business Analyst III	Bachelors	5	$212.21	**$215.25**	**$215.25**	**$215.25**	**$215.25**
Business Analyst IV	Bachelors	7	$256.47	**$260.14**	**$260.14**	**$260.14**	**$260.14**
Business Analyst V	Bachelors	12	$319.39	**$323.96**	**$323.96**	**$323.96**	**$323.96**
Consultant I	Bachelors	1	$207.85	**$210.82**	**$210.04**	**$210.04**	**$210.04**
Consultant II	Bachelors	3	$234.34	**$237.69**	**$236.90**	**$236.90**	**$236.90**
Consultant III	Bachelors	5	$256.47	**$260.14**	**$259.35**	**$259.35**	**$259.35**
Consultant IV	Bachelors	7	$296.70	**$300.94**	**$294.26**	**$294.26**	**$294.26**
Consultant V	Bachelors	12	$337.52	**$342.35**	**$335.93**	**$335.93**	**$335.93**
Database Administrator I	Bachelors	1	$120.70	**$122.42**	**$122.42**	**$122.42**	**$122.42**

Database Administrator II	Bachelors	3	$135.78	**$137.72**	**$137.72**	**$137.72**	**$137.72**
Database Administrator III	Bachelors	5	$150.87	**$153.02**	**$153.02**	**$153.02**	**$153.02**
Database Administrator IV	Bachelors	7	$216.43	**$219.53**	**$219.53**	**$219.53**	**$219.53**
Database Administrator V	Bachelors	12	$281.26	**$285.28**	**$285.28**	**$285.28**	**$285.28**
Project Coordinator I	Bachelors	1	$95.55	**$96.92**	**$96.92**	**$96.92**	**$96.92**
Project Coordinator II	Bachelors	3	$104.87	**$106.37**	**$106.37**	**$106.37**	**$106.37**
Project Coordinator III	Bachelors	5	$115.66	**$117.31**	**$117.31**	**$117.31**	**$117.31**
Project Coordinator IV	Bachelors	7	$135.78	**$137.72**	**$137.72**	**$137.72**	**$137.72**
Project Manager I	Bachelors	1	$116.83	**$118.51**	**$118.51**	**$118.51**	**$118.51**
Project Manager II	Bachelors	3	$119.18	**$120.88**	**$120.88**	**$120.88**	**$120.88**
Project Manager III	Bachelors	5	$176.38	**$178.90**	**$178.90**	**$178.90**	**$178.90**
Project Manager IV	Bachelors	7	$226.30	**$229.53**	**$229.53**	**$229.53**	**$229.53**
Project Manager V	Bachelors	12	$319.39	**$323.95**	**$323.95**	**$323.95**	**$323.95**
Software Lab Services I	Bachelors	1	$241.21	**$244.66**	**$244.66**	**$244.66**	**$244.66**
Software Lab Services II	Bachelors	3	$258.37	**$262.06**	**$262.06**	**$262.06**	**$262.06**

Software Lab Services III	Bachelors	5	$275.53	**$279.47**	**$279.47**	**$279.47**	**$279.47**
Software Lab Services IV	Bachelors	7	$301.28	**$305.59**	**$305.59**	**$305.59**	**$305.59**
Software Lab Services V	Bachelors	12	$337.50	**$342.34**	**$342.34**	**$342.34**	**$342.34**
Systems Administrator - Client, Enterprise and Data Center Technologies I	Bachelors	1	$121.69	**$123.42**	**$123.42**	**$123.42**	**$123.42**
Systems Administrator - Client, Enterprise and Data Center Technologies II	Bachelors	3	$135.27	**$137.20**	**$137.20**	**$137.20**	**$137.20**
Systems Administrator - Client, Enterprise and Data Center Technologies III	Bachelors	5	$148.85	**$150.98**	**$150.98**	**$150.98**	**$150.98**
Systems Administrator - Client, Enterprise and Data Center Technologies IV	Bachelors	7	$169.97	**$172.40**	**$172.40**	**$172.40**	**$172.40**
Systems Administrator - Client, Enterprise and Data Center Technologies V	Bachelors	12	$203.92	**$206.86**	**$206.86**	**$206.86**	**$206.86**
Technical Systems and Solutions Specialist I	Bachelors	1	$120.70	**$122.42**	**$122.42**	**$122.42**	**$122.42**
Technical Systems and Solutions Specialist II	Bachelors	3	$166.45	**$168.83**	**$168.83**	**$168.83**	**$168.83**
Technical Systems and Solutions Specialist III	Bachelors	5	$212.21	**$215.25**	**$215.25**	**$215.25**	**$215.25**
Technical Systems and Solutions Specialist IV	Bachelors	7	$234.54	**$237.90**	**$237.90**	**$237.90**	**$237.90**
Technical Systems and Solutions Specialist V	Bachelors	12	$262.20	**$265.95**	**$265.95**	**$265.95**	**$265.95**
IT Analyst - Solutions I	Bachelors	1	$110.63	**$112.22**	**$112.22**	**$112.22**	**$112.22**
IT Analyst - Solutions II	Bachelors	3	$123.20	**$124.97**	**$124.97**	**$124.97**	**$124.97**

IT Analyst - Solutions III	Bachelors	5	$135.78	**$137.72**	**$137.72**	**$137.72**	**$137.72**
IT Analyst - Solutions IV	Bachelors	7	$150.87	**$153.02**	**$153.02**	**$153.02**	**$153.02**
IT Analyst - Solutions V	Bachelors	12	$182.30	**$184.91**	**$184.91**	**$184.91**	**$184.91**

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.

Provides expert support, analysis and research into exceptionally complex cyber security problems, and processes relating to the subject matter. Serves as technical expert on project teams providing technical direction, interpretation and alternatives.
Applies extensive technical expertise in the field of cybersecurity, and has full knowledge of other related disciplines. Guides the successful completion of major programs and may function in a project leadership role. Develops technical solutions to complex problems that require the regular use of ingenuity and creativity. Expertise isin a particular area of Information Technology (e.g., Product SME, Information Systems Architecture, Telecommunications Systems Design, Architecture, Implementation, Information Systems Integration, Software Development Methodologies, Security Engineering, Security Compliance, Cognitive Security, Analytics, Privacy, Communications and Network SystemsManagement), or a specific functional area (e.g., finance, logistics, and operations research).

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

Project Manager

- Provides direction to the teams to include cybersecurity staff
- Provides overall strategic management, defines the program scope and objectives, manages project's scope, schedule, budget, and risk.
- Develops project management plans, project documentation, work breakdown structures, project schedules, integrated master schedules, financial reports, and risk management documentation

- Plans, organizes, monitors, and oversees IT projects, business strategies, and technology development.
- Manages cross functional teams
- Understands needs of business users as well as development and service support areas.
- Defines program and project goals, plans and reports.
- Responsible for all aspects of the development and implementation of assigned projects.

Project Coordinator

- Advises project team and cybersecurity staff on processes
- Develops project schedule and supports deliverables
- Analyzes impact change requests have on the schedule
- Analyzes progress reported against work schedules
- Organizes and facilitates sessions regarding the project management of the project

Consultant

- Leads or participate in cybersecurity consulting projects that deliver customer-focused results aligned with strategic and operational goals of the Client.
- Obtains and shares internal and external learning and knowledge, problem solving, strategy, methodologies, tool and processes.
- Facilitates identification, review and analysis of cybersecurity strategic issues and advises regarding development and implementation of strategy for the client's environment.
- May assist in developing, leading and conducting education classes
- Provides guidance in analyzing, investigating, and resolving issues.
- Analyzes trends and issues and provides recommendations.
- Responsible for development, implementation, and maintenance of guidelines, policies, procedures, and processes.
- Provides vision and guidance for area of responsibility
- Provides consultation and vision on process tools, methods, product lines, technology, implementation, support, process design, client initiatives, and business activities.
- May be required to oversee technical implementation and execution of strategic plans.
- Research and provide information on technical trends, evaluate and implement exiting applications and/or customized solutions.
- Has expertise and operates across one or more industries and variety of services such as information technology, e-business, cloud, security, and latest business transformation solutions.
- Adhere to project development and documentation standards

- Provides assistance and responsible for aspects of the development and implementation process, including tasks associated with program office support.

Architect

- Responsible for guiding the design and implementation of secure solutions and services across our business and IT support areas. Driving the successful configuration and implementation of security solutions to reduce risk to an acceptable level.
- Responsible for overall system design or the component design of a large system or solution.
- Responsibility includes detailed documentation of technical requirements and design documents.
- Works with the development team for the development of applications or systems
- Facilitates and guides requirements gathering, analysis, development of hypotheses/conclusions
- Performs analysis of business models, logical specifications and/or user requirements to design client solutions.
- Has expert knowledge of application design and usability principles, issues, and techniques.
- Architects focused on solution architecture organizes the development effort of a system solution. Responsible for the overall vision that underlies the projected solution and transform the vision through the execution of the solution. Shapes, designs and plan specific service line in product areas.
- May include roles such as Application Architect, Portfolio Architect, Network Architect, Systems
- Architect, Mainframe Architect, Enterprise/Infrastructure Architect, Solutions Architect.

Business Analyst

- Acts as liaison between business areas and IT and cybersecurity business units
- Participates in research to evaluate business requirements and recommends solutions or assist in problem resolution.
- Works with client to plan and initiate the project
- Performs research, collection and collation of data from studies.
- Performs assessments and projections as part of analysis process.

Technical Systems and Solutions Specialist

- Track security violations and identify trends or exposures that could be addressed by additional training, technical measures, or use of application tools to enhance security. May lead or execute simulated attacks or security violations to assess the organization's data security measures.
- Works on client's key operations and business solutions. Analyzes, designs, and develops client's information systems and program specifications; involved in creation of

specification/requirements, and maintenance/ design/build /test phases of systems and applications. May also be asked to provide technical support and analysis of infrastructure projects and production environment; develop upgrade/improvement recommendation; monitor, plan, and measure impact of new products and services.

- Codes, test and debugs applications and programs. May participate in the application design of systems, including use of analytical techniques. Develops program specifications and detail design documents. Assists in testing, training, and preparation of operations. Works on systems business intelligence or decision support systems supporting client's key operations.

Roles may include: System Analyst, Programmer, Developer, Designer, Tester:

Database Administrator

- Based on skill level, the administrator can be staffed to do one, or a combination of the following: 1) installs, upgrades, resolves (patches, updates) to applications, 2) Implements the database design, that may include setup (creating tables, columns, data types, constraints), improving availability and response times, 3) Creates databases logical design which involves data architecture design, data modeling, and schema definition, 4) performs industry research for data and DB technologies and related software, tools, standards and training. 5) Supports remediation of Plan of Action and Milestones (POA&M). 6) Perform database maintenance on IDS/IPS and other security management consoles

System Administrator

- Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
- Provides technical support and analysis of infrastructure project and production environment; develops upgrade/improvement recommendation; monitors, plans, measures, and tests new products and services
- Works on client technologies including operating support systems
- Works on enterprise technologies, software configurations management and distribution, storage area networks
- Work on data center technologies such as network (LAN,WAN, router) management, server management, mainframe operating system.

Software Lab Services Specialist

- Collaborates closely with product development and product support, 2) Leading edge skill on the current versions of software products and on products in development/test, 3) Skills may include performance tuning, infrastructure logical designs, scaling, installation, integration, training, testing, migration. 4) Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level 5) Verify that application software/network/system security postures are implemented as stated, document deviations,

and recommend required actions to correct those deviations 6) Troubleshoot prototype design and process issues throughout the product design, development, and post-launch phases

IT Analyst Solutions

- Create, analyze, coordinate, and document complex IT and cybersecurity projects, products processes and provide recommendations based on analysis for optimal solutions.
- Create/update reports, and propose action and/or implementation plans and present to leadership to assist in decision-making and drive the work to conclusion.
- Provide IT process and/or product subject matter expertise, conduct research, gather requirements, and conduct analysis and/or coordination activities related to IT processes, projects and/or services.
- Display a technical aptitude and the ability to coordinate, design, and manage IT processes and work.

Substitution Table

Degree	Experience Equivalence	Other Equivalence
Bachelors	Associate degree +2 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		