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

Labor Category	Minimum Education / Certification Level	Minimum Years of Experience	Contractor or Customer Facility or Both	GSA Price (Including IFF) Effective Jan 2017 - Dec 31, 2017	GSA Price (Including IFF) Effective Jan 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 System Engineer Level 1	Bachelors	1	Both	$112.12	$115.60	$116.47	$120.27
Security System Engineer Level 2	Bachelors	5	Both	$146.01	$150.54	$151.68	$147.54
Security System Engineer Level 3	Bachelors	7	Both	$182.25	$187.91	$189.33	$184.17
Information Assurance Analyst Level 1	Bachelors	1	Both	$112.12	$115.60	$116.47	$113.30
Information Assurance Analyst Level 2	Bachelors	5	Both	$146.01	$150.54	$151.68	$147.54
Information Assurance Analyst Level 3	Bachelors	7	Both	$182.25	$187.91	$189.33	$184.17
Information Assurance Subject Matter Expert Level 4	Bachelors	10	Both	$221.89	$228.78	$230.51	$224.23
Information Assurance/ System Security Architect Level 1	Bachelors	1	Both	$112.12	$115.60	$116.47	$113.30
Information Assurance/ System Security Architect Level 2	Bachelors	5	Both	$146.01	$150.54	$151.68	$147.54
Information Assurance/ System Security Architect Level 3	Bachelors	7	Both	$182.25	$187.91	$189.33	$184.17
Training Specialist Level 1	Bachelors	1	Both	$119.42	$121.81	$122.73	$119.39
Specialized Technology Training Specialist Level 2	Bachelors	5	Both	$146.01	$150.54	$151.68	$147.54
Specialized Technology Training Specialist Level 3	Bachelors	7	Both	$182.25	$187.91	$189.33	$184.17
Cyber Warfare Specialist Level 1	Bachelors	5	Both	$155.56	$160.38	$161.59	$157.18
Cyber Warfare Specialist Level 2	Bachelors	7	Both	$194.16	$200.19	$201.71	$196.21
Subject Matter Expert Level 1	Bachelors	1	Both	$156.55	$159.69	$160.89	$156.51

Labor Category	Minimum Education / Certification Level	Minimum Years of Experience	Contractor or Customer Facility or Both	GSA Price (Including IFF) Effective Jan 2017 - Dec 31, 2017	GSA Price (Including IFF) Effective Jan 2018 - Dec 31, 2018	GSA Price (Including IFF) Effective Jan 2019 - Dec 31, 2019	GSA Price (Including IFF) Effective Jan 2020 - Dec 31, 2020
Subject Matter Expert Level 2	Bachelors	5	Both	$196.87	$200.81	$202.33	$196.82
Subject Matter Expert Level 3	Bachelors	7	Both	$254.48	$259.56	$261.53	$254.40
Architect I	Bachelors	1	Both	$150.87	$153.89	$156.96	$160.10
Architect II	Bachelors	3	Both	$181.29	$184.92	$188.62	$192.39
Architect III	Bachelors	5	Both	$211.72	$215.95	$220.27	$224.67
Architect IV	Bachelors	7	Both	$256.47	$261.60	$266.83	$272.17
Architect V	Bachelors	12	Both	$318.79	$325.17	$331.67	$338.31
Business Analyst I	Bachelors	1	Both	$120.70	$123.11	$125.57	$128.08
Business Analyst II	Bachelors	3	Both	$166.45	$169.78	$173.18	$176.64
Business Analyst III	Bachelors	5	Both	$212.21	$216.46	$220.79	$225.20
Business Analyst IV	Bachelors	7	Both	$256.47	$261.60	$266.83	$272.17
Business Analyst V	Bachelors	12	Both	$319.39	$325.78	$332.30	$338.94
Consultant I	Bachelors	1	Both	$207.85	$212.00	$216.24	$220.57
Consultant II	Bachelors	3	Both	$234.34	$239.03	$243.81	$248.69
Consultant III	Bachelors	5	Both	$256.47	$261.60	$266.83	$272.17
Consultant IV	Bachelors	7	Both	$296.70	$302.63	$308.69	$314.86
Consultant V	Bachelors	12	Both	$337.52	$344.27	$351.15	$358.17
Database Administrator I	Bachelors	1	Both	$120.70	$123.11	$125.57	$128.08
Database Administrator II	Bachelors	3	Both	$135.78	$138.50	$141.27	$144.09
Database Administrator III	Bachelors	5	Both	$150.87	$153.89	$156.96	$160.10
Database Administrator IV	Bachelors	7	Both	$216.43	$220.76	$225.18	$229.68
Database Administrator V	Bachelors	12	Both	$281.26	$286.89	$292.62	$298.48
Project Coordinator I	Bachelors	1	Both	$ 95.55	$ 97.46	$ 99.41	$101.40
Project Coordinator II	Bachelors	3	Both	$104.87	$106.97	$109.11	$111.29

Labor Category	Minimum Education / Certification Level	Minimum Years of Experience	Contractor or Customer Facility or Both	GSA Price (Including IFF) Effective Jan 2017 - Dec 31, 2017	GSA Price (Including IFF) Effective Jan 2018 - Dec 31, 2018	GSA Price (Including IFF) Effective Jan 2019 - Dec 31, 2019	GSA Price (Including IFF) Effective Jan 2020 - Dec 31, 2020
Project Coordinator III	Bachelors	5	Both	$115.66	$117.97	$120.33	$122.74
Project Coordinator IV	Bachelors	7	Both	$135.78	$138.49	$141.26	$144.09
Project Manager I	Bachelors	1	Both	$116.83	$119.17	$121.55	$123.99
Project Manager II	Bachelors	3	Both	$119.18	$121.56	$123.99	$126.47
Project Manager III	Bachelors	5	Both	$176.38	$179.91	$183.51	$187.18
Project Manager IV	Bachelors	7	Both	$226.30	$230.82	$235.44	$240.15
Project Manager V	Bachelors	12	Both	$319.39	$325.78	$332.30	$338.94
Software Lab Services I	Bachelors	1	Both	$241.21	$246.03	$250.95	$255.97
Software Lab Services II	Bachelors	3	Both	$258.37	$263.53	$268.80	$274.18
Software Lab Services III	Bachelors	5	Both	$275.53	$281.04	$286.67	$292.40
Software Lab Services IV	Bachelors	7	Both	$301.28	$307.31	$313.45	$319.72
Software Lab Services V	Bachelors	12	Both	$337.50	$344.25	$351.14	$358.16
Systems Administrator - Client, Enterprise and Data Center Technologies I	Bachelors	1	Both	$121.69	$124.13	$126.61	$129.14
Systems Administrator - Client, Enterprise and Data Center Technologies II	Bachelors	3	Both	$135.27	$137.98	$140.74	$143.55
Systems Administrator - Client, Enterprise and Data Center Technologies III	Bachelors	5	Both	$148.85	$151.83	$154.87	$157.97
Systems Administrator - Client, Enterprise and Data Center Technologies IV	Bachelors	7	Both	$169.97	$173.37	$176.84	$180.37
Systems Administrator - Client, Enterprise and Data Center Technologies V	Bachelors	12	Both	$203.92	$208.00	$212.16	$216.40
Technical Systems and Solutions Specialist I	Bachelors	1	Both	$120.70	$123.11	$125.57	$128.08
Technical Systems and Solutions Specialist II	Bachelors	3	Both	$166.45	$169.78	$173.18	$176.64
Technical Systems and Solutions Specialist III	Bachelors	5	Both	$212.21	$216.46	$220.79	$225.20
Technical Systems and Solutions Specialist IV	Bachelors	7	Both	$234.54	$239.23	$244.01	$248.89

Labor Category	Minimum Education / Certification Level	Minimum Years of Experience	Contractor or Customer Facility or Both	GSA Price (Including IFF) Effective Jan 2017 - Dec 31, 2017	GSA Price (Including IFF) Effective Jan 2018 - Dec 31, 2018	GSA Price (Including IFF) Effective Jan 2019 - Dec 31, 2019	GSA Price (Including IFF) Effective Jan 2020 - Dec 31, 2020
Technical Systems and Solutions Specialist V	Bachelors	12	Both	$262.20	$267.44	$272.79	$278.24
IT Analyst - Solutions I	Bachelors	1	Both	$110.63	$112.84	$115.10	$117.40
IT Analyst - Solutions II	Bachelors	3	Both	$123.20	$125.67	$128.18	$130.74
IT Analyst - Solutions III	Bachelors	5	Both	$135.78	$138.49	$141.26	$144.09
IT Analyst - Solutions IV	Bachelors	7	Both	$150.87	$153.89	$156.96	$160.10
IT Analyst - Solutions V	Bachelors	12	Both	$182.30	$185.95	$189.67	$193.46

DESCRIPTIONS

Security System Engineer Level 1

- 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.

Security System Engineer Level 2

- 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 general supervision of a security manager, uses experience and judgment as well as existing policies and regulations to provide network environment (NE) and advanced level computing environment support to include perimeter controls, internal network monitoring, sensor implementation and analysis. Supports Security Operations Center (SOC).
- Conducts and/or supports authorized penetration testing on enterprise network assets.

Security System Engineer Level 3

- 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 limited supervision, supports Security Operations Center (SOC), advanced computing, network, or enclave environments, applies extensive knowledge of a wide range of IA concepts, practices and procedures to ensure the secure integration and operation of all systems.
- By working independently or leading and directing others, solves IA problems quickly and completely.
- Conducts and/or supports authorized penetration testing on enterprise network assets.

Information Assurance (IA) Analyst Level 1

- Under general technical supervision, performs operational information assurance activities in a computing, network, or enclave environment. In accordance with the Federal Information Security Management Act (FISMA) and NIST guidelines, monitors multi-level security networks to identify potential security violations, incidents, attacks, and malicious behavior.
- As appropriate, takes appropriate action to report incident to higher authority as required by regulation, policy, or law and implement required IA security measures to assist in the mitigation of incident impact.
- Conducts analyses and documents intrusion detection incidents and data. Performs routine IA administrative tasks IAW applicable instructions and pre-established guidelines.
- Performs routine preventive and corrective maintenance, test and monitors network activities.
- Assists with the installing, day to day technical supporting, testing, and troubleshooting of IA systems in accordance with established policy, procedures, test plans and guidance.
- Supports the documentation, validation, and accreditation processes of IT systems.

Information Assurance (IA) Analyst Level 2:

Under general technical supervision, performs network monitoring, analysis and reporting in accordance with the Federal Information Security Management Act (FISMA) and NIST guidelines.

These skills and their associated duties may include the following:

- Intrusion: Examines potential security violations, incidents, malicious activity and attacks to determine if policy has been breached, assesses the impact, and preserves artifacts. Enters and tracks events and incidents. Supports incident escalation and assesses probable damages, identifies damage control and remediation, and assists in developing courses of action.

Supervises the installation, monitoring, testing, troubleshooting, and administration of IA hardware and software systems. Recommends, schedules, and performs IA system repairs, systems administration, and maintenance. Analyzes patterns of non compliance or attacks and recommends appropriate actions to minimize security risks and insider threat.

- Configures, optimizes, and tests network devices. Diagnoses and resolves IA problems in response to reported incidents.
- Enhances rule sets to identify or block sources or potential sources of malicious traffic.
- Supports the design and execution of exercise scenarios.
- Participates in IA risk assessments during the Assessment and Authorization (formerly known as C&A) process. Prepares, reviews, and evaluates documentation of compliance.
- Prepares recommendations for the DAA. Reviews IA and IA enabled software, hardware, and firmware for compliance with appropriate security configuration guidelines, policies, and procedures.
- Reviews AI security plans. Identifies alternative functional IA security strategies to address organizational security concerns. Reviews security safeguards to determine that security concerns identified in approved policies, plans, and doctrine have been fully addressed.
- Develops and implements programs to ensure that systems, network, and data users are aware of, understand, and follow IA policies and procedures.

Information Assurance (IA) Analyst Level 3:

- Provides the leadership, management, and supervisory IA skills. These skills and their associated duties may include the following: Intrusion: Ensures the rigorous application of IA policies, principles, and practices in the delivery of all information technology (IT) and IA services.
- Leads and directs team personnel too quickly, efficiently and effectively to solve complex IA problems.
- Identifies IA requirements as part of the IT acquisition development process and assists in the formulation of IA /IT budgets. Plans, integrates, and schedules the installation of new or modified hardware, operating systems, and software applications.
- Supervises the assessment and implementation of identified computer and network environment fixes such as system patches and fixes associated with specific technical vulnerabilities as part of the Information Assurance Vulnerability Management program.
- Guides the implementation of appropriate operational structures and processes to ensure an effective IA security program including boundary defense, incident detection and response.
- Evaluates functional operation and performance in light of test results and make recommendations regarding Assessment and Authorization (formerly known as C&A). Monitors and evaluates the effectiveness of IA security procedures and safeguards.
- Evaluates security violations to determine necessary initial and long term corrective action.

- Assesses impact, determines probably damage and suggest methods of damage control, conducts computer forensics, and follow-on analysis to build historical and predictive capabilities for IA incidents.
- Develops IA related customer support policies, procedures, and standards. Designs perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc., enhances rule sets to detect or block sources of malicious traffic, and establishes a protective net of layered defenses to prevent, detect, and eradicate threats. Specialist: Ensures that protection and detection capabilities are acquired or developed using the security engineering approach clients' IA architecture. Has a working knowledge of Government provided IA tools.
- Has a working knowledge of policy, guidance and evaluation criteria of the agency Critical Infrastructure Program. Prepares and/or oversees the preparation of IA certification and accreditation documentation. Analyzes, develops, evaluates, and integrates IA policies.
- Assists in the gathering and preservation of evidence used in the prosecution of computer crimes. Identifies the IT security program implications of new technologies or technology upgrades.
- Conducts IA cost benefit, economic and risk analysis in the IT acquisition decision making process. Interprets security requirements relative to the capabilities of new information technologies. Interprets patterns of non compliance to determine their impacts on levels of risk and/or overall effectiveness of IA programs.
- Analyzes identified security strategies and recommends the best approaches and/or practices.
- Monitors and evaluates the effectiveness of IA security procedures and safeguards to ensure they provide the intended level of protection.

Information Assurance Subject Matter Expert Level 4:

- SME in all functional and technical requirements associated with Information Assurance.
- Applies extensive knowledge of a variety of the IA field's concepts, strategies, practices, and procedures to ensure the secure integration and operations of all computer systems.
- Works independently to evaluate and solve complex IA related problems quickly and completely. Supports, monitors, tests, and troubleshoots hardware and software IA problems pertaining to the enclave environment.
- Prepares and/or oversees the preparation of IA certification and accreditation documentation.
- Develops system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands for complex network and enclave systems.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
- Coordinates with senior representatives within the customer organizations to establish and define programs, resources and risks. Applies expertise to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures. Provides guidance and direction to other professionals and serves in a consulting and/or advisory capacity.

Information Assurance/System Security Architect Level 1

- 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. Participates in risk assessment during the Assessment and Authorization (formerly known as C&A) process.
- Designs, develops, implements, and integrates information assurance architecture, system, or system component for use within data center, network, and enclave environments. Participates in information systems risk assessments and designs security countermeasures to mitigate identified risks.
- Ensures that the architecture and design of information systems (IS) are functional and secure. As necessary, designs and develops IA or IA enabled products, interface specifications, and approaches to secure the environment. Entry level position that applies knowledge of existing IA policy, procedures, and structures to design, develop, and implement systems, components, or architectures.
- Ensures that the implementation of security designs properly mitigate identified threats.
- Documents system security design features and provides input to implementation plans and standard operating procedures.

Information Assurance/System Security Architect Level 2

- 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.
- Participates in risk assessment during the Certification and Accreditation process.
- Designs, develops, implements, and integrates information assurance architecture, system, or system component for use within data center, network, and enclave environments.
- Participates in information systems risk assessments and designs security countermeasures to mitigate identified risks.
- Ensures that the architecture and design of information systems (IS) are functional and secure. As necessary, designs and develops IA or IA enabled products, interface specifications, and approaches to secure the environment.
- Assesses threats to the environment and provides input on the adequacy of security designs and architectures.
- Reports to senior IA architect, IA manager, or DAA for most operations with separate reporting to other senior management for network operational requirements, as necessary.
- Utilizes experience and judgment to plan and accomplish goals.

Information Assurance/System Security Architect Level 3

- 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.

- Participates in risk assessment during the Certification and Accreditation process.
- Designs, develops, implements, and integrates information assurance architecture, system, or system component for use within data center, network, and enclave environments.
- Participates in information systems risk assessments and designs security countermeasures to mitigate identified risks. Ensures that the architecture and design of information systems (IS) are functional and secure. As necessary, designs and develops IA or IA enabled products, interface specifications, and approaches to secure the environment.
- Utilizes experience and judgment to plan and accomplish enclave security related goals. Supports system or network designs that encompass multiple data center or networks to include those with differing data protection/classification requirements.
- Reports to DAA for IA issues with separate reporting to other senior management for network operational requirements, as necessary.

Training Specialist Level 1

- Responsible for instruction of Cyber and security related training.
- Collects training data for organization and FISMA requirements.
- Conducts/ support the research necessary to develop and revise training courses and prepares appropriate training catalogs.
- Develops all instructor materials (course outline, background material, and training aids).
- Develops all student materials (course manuals, workbooks, handouts, completion certificates, and course critique forms).
- Trains personnel by conducting formal classroom courses, workshops, seminars and/or computer based/computer aided training. Works under general supervision.

Specialized Technology Training Specialist Level 3:

- Responsible for instruction of Cyber and security related training.
- Conducts the research necessary to design advanced level specialized technology (e.g. IA, IPv6, Secure Virtualization) training programs to include network engineering, IT systems design, and IT systems implementation.
- Trains junior IT personnel by conducting formal classroom courses, workshops, seminars and/or computer-based/computer-aided training. Integrates COTS hardware and software with GOTS hardware and software to produce unique system-level training courses. Provides daily supervision and direction to staff.

Specialized Technology Training Specialist Level 2

- Responsible for instruction of Cyber and security related training.
- Conducts the research necessary to design advanced level specialized technology (e.g. IA, IPv6, Secure Virtualization) training programs to include network engineering, IT systems design, and IT systems implementation.

- Trains entry-level IT personnel by conducting formal classroom courses, workshops, seminars and/or computer-based/computer-aided training. Integrates COTS hardware and software with GOTS hardware and software to produce unique system level training courses.

Cyber Warfare Specialist Level 2:

- The Senior Cyber Warfare Engineer will provide technical direction within a team of technical and engineering personnel who will conduct / manage innovative solutions associated with Cyber Warfare. Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.
- Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. They shall provide technical leadership and have a strong understanding of information assurance, cyber warfare, and managing special access or compartmentalized security programs.
- They will lead technical teams researching new concepts for developing situational awareness or vulnerability tools supporting US government cyber warfare interest. This may include identification, exploitation, and/or remediation of infrastructure and system vulnerabilities; offensive and/or self defending networks; effects-based capabilities for exploiting or defending infrastructure and/or systems; and reverse engineering of systems exploitations to include computer forensics, and analysis of binaries, assembly language, source code and/or malicious logic code. High level security clearances may be required.

Cyber Warfare Specialist Level 1:

- The Cyber Warfare Specialist will provide technical and engineering support in the exploitation and/or remediation of infrastructure and computer systems.
- Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.
- Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. The specialist shall have an understanding in information assurance with expertise in computer and telecommunication network systems and cyber warfare.
- They will assist in researching new concepts for developing situational awareness and vulnerability tools to support US Government cyber warfare efforts. They will assist the Government with the identification, exploitation, and/or remediation of infrastructure and system vulnerabilities; developing and implementing offensive and/or self defending networks; developing and defending effects-based capabilities; and reverse engineering of systems exploitations to include computer forensics, and analysis of binaries, assembly language, source code and/or malicious logic code. High level security clearances may also be required.

Subject Matter Expert Level 1

- Under broad direction, provides expert support, analysis and research into especially Complex cyber security problems, and processes relating to the subject matter. Serves as technical expert on high-level project teams providing technical direction, interpretation and

alternatives. Possesses a complete understanding and wide experience in the application of technical principles, theories, and concepts in the field of cybersecurity.

- Provides technical solutions to a wide range of difficult problems. Expertise is in 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 Systems Management), or a specific functional area (e.g., finance, logistics, and operations research).

Subject Matter Expert Level 2

- With minimal direction, provides expert support, analysis and research into exceptionally complex cyber security problems, and processes relating to the subject matter. Serves as technical expert on executive-level 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 is in 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 Systems Management), or a specific functional area (e.g., finance, logistics, and operations research).

Subject Matter Expert Level 3

- Provides expert support, analysis and research into exceptionally complex cyber security problems, and processes relating to the subject matter.
- Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives.
- Applies advanced technical principles, theories, and concepts.
- Contributes to the development of new principles and concepts.
- Expertise is in 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 Systems Management), or a specific functional area (e.g., finance, logistics, and operations research).

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