InfusionPoints
Securing Cloud Solutions

InfusionPoints Labor Categories 2026

Published by InfusionPoints, LLC 2026

Any comments relating to the material contained in this document may be submitted to InfusionPoints, LLC, by email to info@InfusionPoints.com

InfusionPoints - *Secure Business Solutions*, bridges the gap between security and business needs. We combine a unique blend of technology and business skills to help our clients with their critical security and privacy initiatives, while achieving high returns on their investments. We apply holistic, integrated methodologies for infusing security and privacy capabilities into their business solutions, by combining our frameworks with critical thinking and deep analytics to solve their most pressing security and privacy challenges. Our security and privacy solutions focus on the business needs -- from defining key security and privacy requirements, to developing enterprise security architectures, developing enterprise security and privacy roadmaps, and managing and implementing critical initiatives. We work with our clients to infuse security and privacy throughout every point in the business solutions' lifecycle to protect our clients' information and achieve their security and privacy objectives and goals. We are currently working in both commercial and Federal Government industries. We focus on the full life-cycle of a solution from the assessment – to the deployment, with capabilities in security and privacy strategy, program management, enterprise architecture, identity and access management and data protection. We are always focused on building secure business solutions.

How We Can Help

- Link business strategies with security and privacy solutions
- Bridge the gap between concepts and reality
- Leverage security and privacy investments to improve compliance, productivity, and efficiency
- Identify and mitigate security risks
- Develop, deploy and manage your IT security Infrastructure

InfusionPoints' Capabilities

Strategic Security and Privacy Capability

InfusionPoints' strategic security and privacy services meet business challenges head-on with an approach that balances short term objectives and long term goals to provide an enterprise security and privacy strategic roadmap. Using our proven security and privacy frameworks, our knowledgeable consultants, focus on providing security leadership from a business perspective by:

- Transforming security organizations
- Establishing security and privacy mission, vision, and objectives
- Formalizing governance and project management structures
- Assessing an organization's security environment
- Infusing security and privacy into business processes

Security Program Management Capability

InfusionPoints' Security Program Management team works for you, you have an independent trusted partner on your side to provide insight into current and future security technologies and management techniques. We leverage our InfusionPoints' Security Program Management framework and best practices to effectively and efficiently plan, design, develop, and implement your security programs by providing:

- Security Program Management Office
- Security Program Management Oversight
- Security Program Management Assessment

Enterprise Security Architecture Capability

Across a wide range of industries, InfusionPoints has made the mission of our clients "our mission," and we apply this in-depth understanding of client-specific objectives, resources, and constraints to build business and government enterprise security architectures ideally suited to support mission requirements.

Our consultants specialize in developing IT security and privacy architectures to protect sensitive consumer, employee, and partner information without losing sight of cost and efficiency. InfusionPoints' teams provide the entire range of technical and management skills to support multi-level security systems, electronic key management systems, Identity and Access Management, and Internet-based solutions designed to support global-scale implementations.

Identity and Access Management Capabilities

InfusionPoints’ consultants apply our proven Identity and Access Management (IdAM) framework to simplify identity and access infrastructures to increase security, privacy, compliancy, efficiencies, and reduce costs. IdAM infrastructures require seasoned professionals to plan, manage, and build your IdAM infrastructure that supports your digital identity lifecycle.

Our IdAM capabilities include:

- IdAM governance, architectures and program management
- Compliance and audit IdAM infrastructures
- Federated identity and access management
- Directory Services
- Strong Authentication
- Simplified Sign-On Authorization and Access Management
- User Management and Provisioning

Data Protection Capabilities

InfusionPoints’ information and data protection framework is a systematic, comprehensive approach to information security that makes business sense of information security by providing:

- Information and data security technology models
- Physical and logical data models
- Flat file and database encryption solutions
- Enterprise key management services
- Rights management services
- Network content filtering services

Network Security

InfusionPoints' project team identifies internal objectives, defines responsibilities, establishes project controls, procures selected hardware and software, plans the delivery of network services, and manages schedules and budgets to help ensure a successful network implementation for:

- Firewalls
- Virtual Private Networks
- Disaster Recovery solutions
- Network filtering services
- Intrusion Prevention/Detection
- Virus and Spam Filtering

Labor Categories

Program Manager

Description: The PMP Performs program and project management functions including: planning workload requirements to meet client requirements, preparing technical and price proposals, preparing invoicing, interviewing and hiring employees to meet client requirements, and providing professional consultation. Must understand business management and practices.

Education and Years' Experience: Bachelor's degree, 7+ years

Senior Task Lead

Description: Senior task leader (STL) , experience in project and task management, responsible for ensuring successful task completion within the scheduled timeframe consistent with the established scope of work to include both the technical and financial solutions. Organizes, directs, and coordinates the planning and production of all activities associated with assigned tasks.

Education and Years' Experience: Master's Degree 8+ years

Project Coordinator

Description: Senior Task Lead (STL) leader, experience in project and task management, responsible for ensuring successful task completion within the scheduled timeframe consistent with the established scope of work to include both the technical and financial solutions. Organizes, directs, and coordinates the planning and production of all activities associated with assigned tasks.

Education and Years' Experience: Master's Degree 8+ years

Subject Matter Expert

Description: The Subject Matter Expert (SME) is primarily utilized on projects for their specific expertise, not in a managerial capacity, in support of the creation of comprehensive methods for describing current and/or future structure and behavior of an organization's processes, systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction

Education and Years' Experience: Master's Degree 10+ years

Functional Expert II

Description: Senior expert with extensive, enterprise-wide knowledge and experience in one or more designated functional and/or domain areas. Provides insight and advice concerning strategic direction and applicability of up to date, industry standard solutions. Is responsible for providing high level vision to program/project manager or senior client leadership to influence objectives of complex efforts.

Education and Years' Experience: Master's Degree 12+ years

Functional Expert I

Description: Mid level expert with enterprise-wide knowledge and experience in one or more designated functional and/or domain areas. Provides assistance on insight and advice concerning

strategic direction and applicability of up to date, industry standard solutions. Is responsible for assisting in providing high level vision to program/project manager or senior client leadership to influence objectives of complex efforts.

Education and Years' Experience: Bachelor's Degree 8+Years

Analyst II

Description: Expert with extensive knowledge and experience developing and applying analytic methodologies and principles. Leads the application of analytic techniques and helps define project objectives and strategic direction. Is responsible for providing leadership and vision to client and project teams around the methodology. Resolves complex problems, which require an in-depth knowledge of analytic methodologies and principles. Directs the activities of more junior Analysts or other staff as necessary on activities related to the application of analytical techniques and methodologies. Demonstrated managerial and supervisory skills.

Education and Years' Experience: Bachelor's Degree 1-5 years

Analyst I

Description: Possesses demonstrated knowledge and experience applying analytic methodologies and principles to address client needs. Applies analytic techniques in the evaluation of project objectives and contributes to the implementation of strategic direction. Performs analyst functions including data collection, interviewing, data modeling, project testing, and creation of performance measurements to support project objectives. Conducts activities in support of project team's objectives.

Education and Years' Experience: Bachelor's Degree 0-1 years

IT Consultant II

Description: Assists in providing support to plan, coordinate, and implement the organization's information security. Assists in providing support for facilitating and helping agencies identify their current security infrastructure and define future programs, design and implementation of security related to IT systems. Experience in several of the following areas is required; understanding of business security practices and procedures; knowledge of current security tools available; hardware/software security implementation; different communication protocols; encryption techniques/tools; familiarity with commercial products, and current Internet/EC technology.

Education and Years' Experience: Bachelor's Degree 6-10 years

IT Consultant I

Description: Assists in providing support to plan, coordinate, and implement the organization's information security. Assists in providing support for facilitating and helping agencies identify their current security infrastructure and define future programs, design and implementation of IT systems. Experience in several of the following areas is required; understanding of business practices and procedures; knowledge of current tools available; hardware/software implementation; different communication protocols; familiarity with commercial products, and current Internet/EC technology.

Education and Years' Experience: Associate Degree 3-7 years

Systems Engineer II

Description: Knowledge and proven experience in one or more of the following areas: operating systems and their applications in a networked (heterogeneous and homogenous) or stand-alone environment; system benchmarks and performance tuning; network protocols; network-based applications; systems planning, implementation and management for medium and large multi-user environments; system security issues and applications; network management software and platforms; various computer architectures and vendor lines; data storage technologies and their application in the IT environment; and various computer languages and software development methodologies. Designs complex network systems from requirements. Implements networks from plans. Reviews systems requirements. Analyzes, troubleshoots and develop solutions. Works independently at the highest technical level formulating creative solutions to diverse and highly complex technical or scientific assignments.

Education and Years' Experience: Bachelor's Degree 6-10 years

Systems Engineer I

Description: Knowledge and practical experience in one or more of the following areas: operating systems and their applications in a networked (heterogeneous and homogenous) or stand-alone environment; systems administration and configuration of at least two operating systems; and various computer languages and software development methodologies. Designs network systems from requirements. Implements networks from plans. Reviews systems requirements. Analyzes, troubleshoots and develops solutions.

Education and Years' Experience: Bachelor's Degree 3-7 years

Systems Analyst II

Description: Analyzes business procedures and problems to understand data and automation needed to support those processes. Guide users in formulating requirements, advise alternative approaches, and conducts evaluation studies. Develops and writes technical reports, findings, and recommendations related to the above.

Education and Years' Experience: Bachelor's Degree 1-5 years

Systems Analyst I

Description: Analyzes business procedures and problems to understand data and automation needed to support those processes. Guide users in formulating requirements, advise alternative approaches, and conducts evaluation studies. Develops and writes technical reports, findings, and recommendations related to the above.

Education and Years' Experience: Associate Degree 0-1 years

Network Engineer II

Description: Knowledge and practical experience in one or more of the following areas: site-specific computer hardware, applications software, operations systems software, and telecommunications devices. Considerable knowledge of networks and telecommunications procedures. Determines probable causes of malfunctions and hardware, applications and operating systems software and telecommunications. Troubleshoots users' problems by analyzing information provided by users. Corrects complex software and telecommunications malfunctions. Develops recommendations for

efficient hardware and software installation and configurations. Writes procedures for computer and/or network operations to provide users with guidelines in efficient utilization of the network. Registers new users on the network and establishes users' functional security profiles to allow network availability to all users. Assists users in the area of quality assurance.

Education and Years' Experience: Associate Degree 6-10 years

Network Engineer I

Description: Knowledge and practical experience in one or more of the following areas: site-specific computer hardware, applications software, operations systems software, and telecommunications devices. Knowledge of networks and telecommunications procedures. Determines probable causes of moderately complex-to-complex malfunctions and hardware, applications and operating systems software, and telecommunications. Troubleshoots users' problems by analyzing information provided by users. Develops recommendations for efficient hardware and software and software installation and configurations. Documents procedures for computer and/or network operations to provide users with guidelines in efficient utilization of the network.

Education and Years' Experience: High School Diploma 3-7 years

Quality Assurance Specialist

Description: Reports to PM in staff role (independent/objective). Coordinates with other managers on quality issues. Attends program reviews. Develops, implements, reviews quality assurance program for compliance with Government standards. Prepares/revises program QA plan/procedures. Performs formal QA of services provided. Monitors work efforts/deliverables for quality.

Education and Years' Experience: Bachelor's Degree 3-7 years

Configuration Management Analyst

Description: Develops and documents configuration management processes and procedures to meet the scope and complexity of systems. Maintains the CM environment and performs change control and configuration audits consistent with industry standards. Controls the change process so that only approved and validated changes are incorporated and promoted from Dev to QA to Prod. Implements version control process for hardware and software systems. Provides guidance on the selection and use of configuration management tools to store, track, and manage configuration artifacts. Creates build scripts and promotes those scripts within the software build process. Ensures that the development, test and production environments are identical in configuration to avoid inconsistencies with in environments. Directs and provides guidance to junior staff on configuration management related tasks.

Education and Years' Experience: Bachelor's Degree 1-5 years

Technical Writer

Description: Supporting the contractor staff, prepares draft and final-form technical documents, which will become Task Order deliverable items. Is expected to be familiar with telecommunications/data terminology and capable of typing at least forty (40) wpm. Is expected to be capable of typing technical narrative and data. Will be responsible for spelling, grammar, and proper format, and for proofreading finished documents. Is expected to use various word processing equipment with various software applications.

Education and Years' Experience: High School Diploma 1-5 years

Cloud Architect

Description: Designs cloud infrastructure, virtual private cloud, virtual private network, relational database services, auto scaling, and compute resources to meet customers' requirements. Provides expertise in high availability, contingency planning, and automated provisioning. Responsible for cloud management and monitoring. Designs solutions for various deployment models (Private, Public, Community and Hybrid) and service models including Infrastructure as a Service (IaaS), Platform as a service (PaaS), Software as a Service (SaaS) and emerging cloud services to optimize the essential characteristics of cloud computing. Advices on storage and security solutions to securely store data in multi-tenancy environments. Collaborates with enterprise architecture team and other stakeholders to determine enterprise tools, technologies and processes. Establishes corporate cloud computing architecture policies and standards in compliance with appropriate security levels and governance in accordance with best practices prescribes by the National Institute of Standards and Technology (NIST), Federal Information Security Management Act (FISMA), Federal Information Processing Standard (FIPS), Office of Management and Budget (OMB) and Federal Risk and Authorization Management Program (FedRAMP). Responsible for delivering an end-to-end cloud architecture solution across all domains.

Education and Years' Experience: Bachelor's Degree 8+ years

Cloud Engineer II

Description: Provides direction on designing cloud infrastructure capable of supporting a number of applications in the cloud with an emphasis on scalability, automation, performance and availability. Oversees the installation, provisioning, configuration, operation and maintenance of required hardware and software related to cloud computing infrastructure components. Provides guidance and sets standards on migrating internal and external organizational projects to a cloud computing environment including migration of existing data centers to a cloud computing environment. Provides expertise on cloud implementations and researches emerging trends and technologies related to cloud engineering. Implements prescribed solutions for various deployment models (Private, Public, Community and Hybrid) and delivery models including Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS). Collaborates with security analysists, architects and engineers to define and implement the best solutions for the technical infrastructure layer in a cloud environment.

Education and Years' Experience: Bachelor's Degree 6-10 years

Cloud Engineer I

Description: Provides direction on designing cloud infrastructure capable of supporting a number of applications in the cloud with an emphasis on scalability, automation, performance and availability. Oversees the installation, provisioning, configuration, operation and maintenance of required hardware and software related to cloud computing infrastructure components. Provides guidance and sets standards on migrating internal and external organizational projects to a cloud computing environment including migration of existing data centers to a cloud computing environment. Provides expertise on cloud implementations and researches emerging trends and technologies related to cloud engineering. Implements prescribed solutions for various deployment models (Private, Public, Community and Hybrid) and delivery models including Infrastructure as a Service (IaaS), Platform as a

service (PaaS), and Software as a Service (SaaS). Collaborates with security analysists, architects and engineers to define and implement the best solutions for the technical infrastructure layer in a cloud environment.

Education and Years' Experience: Bachelor's Degree 3-7 years

Cloud Analyst II

Description: Responsible for configuring cloud environments that are scalable and reliable. Performs tasks including installation, configuration, and maintenance under the direction of the cloud engineering team. Collaborates with engineering, development and quality assurance teams to develop guidelines on automated monitoring and alerting protocols. Works with other infrastructure and engineering teams to identify emerging trends and technologies related to cloud engineering. Prepares and updates documentation relating to organizational standards and procedures pertaining to the cloud. Monitors and troubleshoots any cloud operational issues. Maintain logs and records related to the cloud environment.

Education and Years' Experience: Bachelor's Degree 1-5 years

Cloud Analyst I

Description: Responsible for configuring cloud environments that are scalable and reliable. Performs tasks including installation, configuration, and maintenance under the direction of the cloud engineering team. Collaborates with engineering, development and quality assurance teams to develop guidelines on automated monitoring and alerting protocols. Works with other infrastructure and engineering teams to identify emerging trends and technologies related to cloud engineering. Prepares and updates documentation relating to organizational standards and procedures pertaining to the cloud. Monitors and troubleshoots any cloud operational issues. Maintain logs and records related to the cloud environment.

Education and Years' Experience: Bachelor's Degree 0-1 years

Information Assurance Associate

Description: Provide mission applications focused expertise for the I user. Assist with installation and configuration of new software applications. Produce and/or contribute to IT knowledge articles. Conduct Operating System Security Assessments, Wireless Assessments, Database Assessments, Web Application Assessments, Penetration Testing, Network Mapping, Vulnerability Scanning, and Phishing Assessments. Provide report on how to implement Web services securely and that traditional network security tools and techniques are used to limit access to the Web Service to only those networks and systems that should have legitimate access.

Education and Years' Experience: Master's Degree 8+ years

Information Assurance Specialist II

Description: Analyzes and defines telecommunications security requirements. Designs, develops, engineers, implements operations and maintains the security systems. Gathers and organizes technical information about an organization's mission goals and needs, existing security products and ongoing programs related to security issues. Performs risk analyses to include risk assessment.

Education and Years' Experience: Bachelor's Degree 6-10 years

Information Assurance Specialist I

Description: Analyzes and defines telecommunications security requirements. Designs, develops, engineers, implements operations and maintains the security systems. Gathers and organizes technical information about an organization's mission goals and needs, existing security products and ongoing programs related to security issues. Performs risk analyses to include risk assessment.

Education and Years' Experience: Bachelor's Degree 3-7 years

Information Assurance (IA) Analyst II

Description: Individual will provide security architecture, policy and design guidance for business systems and networks. Individual will also provide Information Security Certification and Accreditation Support for applications, systems and networks in accordance with appropriate customer policies and processes.

Education and Years' Experience: Associates Degree 1-5 years

Information Assurance (IA) Analyst I

Description: Individual will provide security architecture, policy and design guidance for business systems and networks. Individual will also provide Information Security Certification and Accreditation Support for applications, systems and networks in accordance with appropriate customer policies and processes.

Education and Years' Experience: Associate Degree 0-1 years

Cybersecurity Architect

Description: Establishes system security information requirements using the analysis from information engineer(s) in the development of enterprise-wide or large scale information systems. Designs architecture to include the security for software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces. Senior level supervisor provides daily supervision and direction to staff.

Education and Years' Experience: Bachelor's Degree 8+

Cybersecurity Engineer II

Description: Provides knowledge in design, architecture, development and administration. Monitor existing cyber systems for structural integrity for future risk. Oversee the development and installation of new hardware and software so as to mitigate potential threats. Install and configure operating systems and other software and routinely test installed software for glitch detection and other issues. Create scalable, automated solutions for our customer base. Establish multi-platform versions of the software package and network mapping. Write penetration tests for existing and created code to ensure compatibility and stability. Evaluate, recommend, and implement automated test tools and strategies intended to help with incident response. Design, implement, and conduct test and evaluation procedures to ensure system requirements are met and to identify specific vulnerabilities. Evaluate cyber hardware and software and resolve LAN/MAN/WAN network related problems.

Education and Years' Experience: Bachelor's Degree 6-10 years

Cybersecurity Engineer I

Description: Provides knowledge in design, architecture, development and administration. Monitor existing cyber systems for structural integrity for future risk. Oversee the development and installation of new hardware and software so as to mitigate potential threats. Install and configure operating systems and other software and routinely test installed software for glitch detection and other issues. Create scalable, automated solutions for our customer base. Establish multi-platform versions of the software package and network mapping. Write penetration tests for existing and created code to ensure compatibility and stability. Evaluate, recommend, and implement automated test tools and strategies intended to help with incident response. Design, implement, and conduct test and evaluation procedures to ensure system requirements are met and to identify specific vulnerabilities. Evaluate cyber hardware and software and resolve LAN/MAN/WAN network related problems.

Education and Years' Experience: Associate Degree 3-7 years

Cybersecurity Administrator

Description: Provide mission applications focused expertise for the I user. Assist with installation and configuration of new software applications. Produce and/or contribute to IT knowledge articles. Conduct Operating System Security Assessments, Wireless Assessments, Database Assessments, Web Application Assessments, Penetration Testing, Network Mapping, Vulnerability Scanning, and Phishing Assessments. Provide report on how to implement Web services securely and that traditional network security tools and techniques are used to limit access to the Web Service to only those networks and systems that should have legitimate access.

Education and Years' Experience: Associate Degree 1-5 years

Penetration Tester II

Description: Conducts security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Executes tests by following the steps and procedures in a test plan and documents results in standardized format suitable for future analysis. Supports in coordination of technical tests, network scans, vulnerability scans, etc. that support the evaluation of security controls. Conducts reconnaissance data gathering and vulnerability research. Supports the creation of risk/vulnerability reporting. Leverages COTS or open source tools to conduct assessments, analyzes results, identifies exploitable vulnerabilities, and verifies vulnerabilities. Prepares and reviews assessment documents, validates and communicates key findings to stakeholders.

Education and Years' Experience: Associate Degree 3-7 years

Penetration Tester I

Description: Conducts security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Executes tests by following the steps and procedures in a test plan and documents results in standardized format suitable for future analysis. Supports in coordination of technical tests, network scans, vulnerability scans, etc. that support the evaluation of security controls. Conducts reconnaissance data gathering and vulnerability research. Supports the creation of risk/vulnerability reporting. Leverages COTS or open source tools to conduct assessments,

analyzes results, identifies exploitable vulnerabilities, and verifies vulnerabilities. Prepares and reviews assessment documents, validates and communicates key findings to stakeholders.

Education and Years' Experience: Associate Degree 1-5 years

Vulnerability Specialist

Description: Creates, reviews, and edits security risk evaluation documentation, procedures, and processes for computer networks, enterprises, applications, and weapon systems. Conducts security controls reviews for systems under assessment. Deploys security controls and/or configuration to mitigate or address cybersecurity risk factors. Conducts vulnerability assessment of systems using COTS, GOTS or opensource tools in support of continuous monitoring of the security posture. Conducts cybersecurity risk management and information assurance in accordance with Department of Defense (DoD) Risk Management Framework (RMF) guidelines, to include testing and auditing of DoD networks, development of policy/procedure for Access and Authorization (A&A) and system operation, ultimately leading to Authorization to Operate (ATO). Audits system policies and procedures using COTS, GOTS, and open-source auditing tools. Develops plans of action and milestones to remediate cybersecurity risks and/or configuration issues. Produces, prepares, and reviews relevant documentation and validates/communicates key findings to stakeholders.

Education and Years' Experience: Associate Degree 3-7 years

Vulnerability Analyst

Description: Creates, reviews, and edits security risk evaluation documentation, procedures, and processes for computer networks, enterprises, applications, and weapon systems. Conducts security controls reviews for systems under assessment. Deploys security controls and/or configuration to mitigate or address cybersecurity risk factors. Conducts vulnerability assessment of systems using COTS, GOTS or opensource tools in support of continuous monitoring of the security posture. Conducts cybersecurity risk management and information assurance in accordance with Department of Defense (DoD) Risk Management Framework (RMF) guidelines, to include testing and auditing of DoD networks, development of policy/procedure for Access and Authorization (A&A) and system operation, ultimately leading to Authorization to Operate (ATO). Audits system policies and procedures using COTS, GOTS, and open-source auditing tools. Develops plans of action and milestones to remediate cybersecurity risks and/or configuration issues. Produces, prepares, and reviews relevant documentation and validates/communicates key findings to stakeholders.

Education and Years' Experience: Associate Degree 1-5 years

Cyber Incident Response Associate

Description: Performs real-time proactive event investigation on various security enforcement systems, such as SIEM, Anti-virus, Internet content filtering/reporting, malware prevention, Firewalls, IDS & IPS, Web security, antispam, etc. Contributes to generating response to crisis or urgent situations to mitigate immediate or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Handles and responds to cyber security incidents through coordination with stakeholders such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement, and privacy offices. Intakes incident reporting, conducts ticket updates, and notifies stakeholders of cyber security incidents and forensic investigations in relation to computer security incidents and escalates when necessary. Coordinates response to computer security incidents. Recommends courses of action on

each incident and creates, manages, and records all actions taken and serve as initial POC for Events of Interest reported both internally and externally. Establishes/implements alarm/alert/incident escalation process and tracks, follows-up, and resolves incidents.

Education and Years' Experience: Associate Degree 7+ years

Security Operations Specialist

Description: Performs real-time proactive event investigation on various security enforcement systems, such as SIEM, Anti-virus, Internet content filtering/reporting, malware prevention, Firewalls, IDS & IPS, Web security, antispam, etc. to collect, aggregate, correlate, and fuse network security and performance data to detect potential and actual intrusions. Actively monitor cyber security threats and risks. Support defensive cyber operations and follow standard operating procedures for detecting, classifying, and reporting incidents.

Education and Years' Experience: Associate Degree 3-7 years

Security Operations Analyst

Description: Performs real-time proactive event investigation on various security enforcement systems, such as SIEM, Anti-virus, Internet content filtering/reporting, malware prevention, Firewalls, IDS & IPS, Web security, antispam, etc. to collect, aggregate, correlate, and fuse network security and performance data to detect potential and actual intrusions. Actively monitor cyber security threats and risks. Support defensive cyber operations and follow standard operating procedures for detecting, classifying, and reporting incidents.

Education and Years' Experience: Associate degree 1-5 years

Acceptable Substitute

Description: Due to the availability or limitation of education, occasionally substitution of experience as referenced below for a professional labor type with additional years of experience will be provided to the Federal Agency when responding to their IT requirements and it is solely the acquiring agency's determination, if the substitution is considered acceptable prior to an award.

- An Associate Degree may be substituted for 3 years of required relevant IT experience with a High School Diploma
- A Bachelor's Degree may be substituted with Associate Degree + 1 years additional relevant IT experience
- A Bachelor's Degree may be substituted for 4 years of required relevant IT experience with a High School Diploma
- A Master's Degree may be substituted with Bachelor's Degree + 2 years additional relevant IT experience
- A Master's Degree may be substituted for 2 years of required relevant IT experience with a Bachelor's Degree A Ph.D. may be substituted with Master's Degree + 4 years additional relevant IT experience
- A Ph.D. may be substituted with 6 years relevant IT experience with a Bachelor's Degree

Service Proposed (eg Job Title/Task)*	Commercial Price List (CPL) OR Market Prices*
Program Manager	$270.00
Senior Task Lead	$180.00
Project Coordinator	$114.00
Subject Matter Expert	$300.00
Functional Expert II	$250.00
Functional Expert I	$174.00
Analyst II	$126.00
Analyst I	$90.00
IT Consultant II	$186.00
IT Consultant I	$162.00
Systems Engineer II	$192.00
Systems Engineer I	$168.00
Systems Analyst II	$144.00
Systems Analyst I	$120.00
Network Engineer II	$156.00
Network Engineer I	$108.00
Quality Assurance Specialist	$108.00
Configuration Management Analyst	$96.00
Technical Writer	$78.00
Cloud Architect	$288.00
Cloud Engineer II	$246.00
Cloud Engineer I	$198.00
Cloud Analyst II	$138.00
Cloud Analyst I	$102.00
Information Assurance Associate	$210.00
Information Assurance Specialist II	$174.00
Information Assurance Specialist I	$132.00
Information Assurance (Ia) Analyst II	$120.00
Information Assurance (Ia) Analyst I	$96.00
Cybersecurity Architect	$216.00
Cybersecurity Engineer II	$198.00
Cybersecurity Engineer I	$180.00
Cybersecurity Administrator	$132.00
Penetration Tester II	$150.00
Penetration Tester I	$120.00
Vulnerability Specialist	$138.00
Vulnerability Analyst	$114.00
Cyber Incident Response Associate	$225.00
Security Operations Specialist	$126.00
Security Operations Analyst	$90.00
Acceptable Substitute	$0.00